กองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะ
Broadcasting and Telecommunications Research and Development Fund for Public Interest

รายงานฉบับสมบูรณ์
(Final Report)

โครงการพัฒนาระบบต้นแบบเพื่อสนับสนุนงานป้องกันและปราบปรามมิจฉาชีพออนไลน์ที่ไม่ระบุตัวตน (ระยะที่ 1)

กรณีศึกษา เขตพื้นที่กองบังคับการตำรวจนครบาล 8

เสนอ
กองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์
และกิจการโทรคมนาคมเพื่อประโยชน์สาธารณะ (กทปส.)

มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร

สารบัญ

สารบัญ

สารบัญรูปภาพ

สารบัญรูปภาพ

สารบัญรูปภาพ

สารบัญรูปภาพ

สารบัญรูปภาพ

สารบัญรูปภาพ

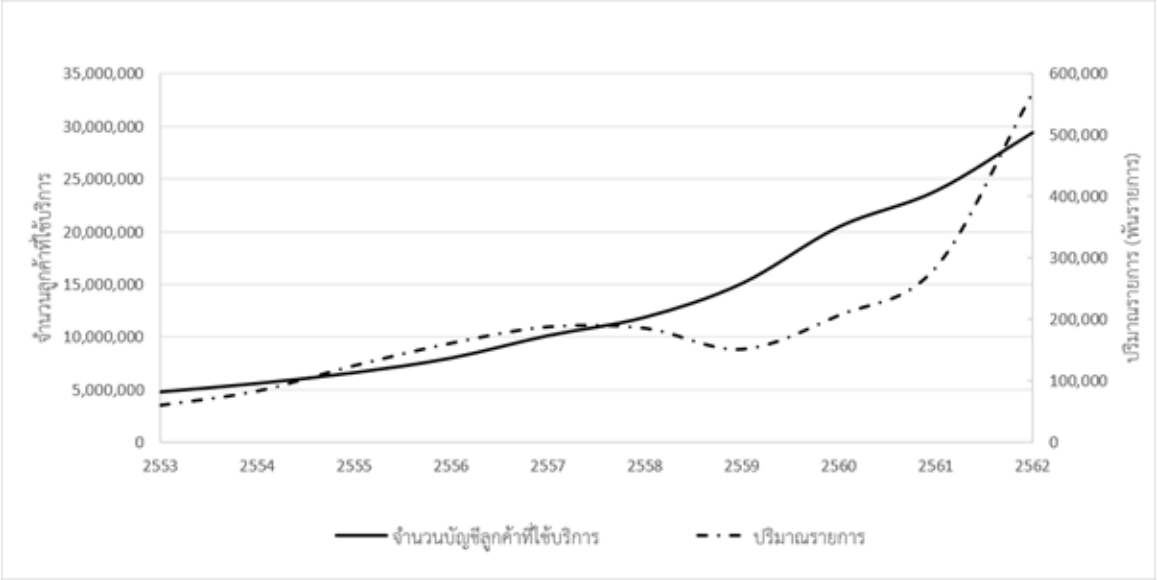
สารบัญรูปภาพ

สารบัญตาราง

บทที่ 1
บทนำ

1.1 หลักการและเหตุผล

ด้วยความก้าวหน้าของเทคโนโลยีการสื่อสารและเทคโนโลยีอินเทอร์เน็ต ผู้ใช้บริการธนาคารไม่จำเป็นต้องเดินทางไปยังธนาคารพาณิชย์ในเวลาทำการปกติเพื่อโอนเงินระหว่างบัญชีของบุคคลหนึ่งไปยังอีกบุคคลหนึ่ง ชำระค่าบริการต่าง ๆ หรือตรวจสอบยอดเงินอีกต่อไป เพราะผู้ใช้บริการสามารถเข้าถึงบริการเหล่านั้นผ่านเครือข่ายอินเทอร์เน็ตหรือผ่านแอปพลิเคชันของธนาคารที่ติดตั้งบนโทรศัพท์เคลื่อนที่แบบสมาร์ตโฟนจากจุดใดและเวลาใดก็ได้ ทำให้ธุรกรรมออนไลน์ในประเทศไทยเติบโตขึ้นเป็นอย่างมาก และยังมีแนวโน้มเติบโตขึ้นอย่างต่อเนื่องด้วย จากข้อมูลสถิติของธนาคารแห่งประเทศไทย ตั้งแต่ปี 2553 เป็นต้นมา ธุรกรรมการชำระเงินผ่านบริการ Mobile Banking ได้รับความนิยมเพิ่มขึ้นอย่างต่อเนื่อง ดังรูปที่ 1-1 (ธนาคารแห่งประเทศไทย, 2564)



รูปที่ 1-1 ธุรกรรมการชำระเงินผ่าน Mobile Banking

ธุรกรรมออนไลน์ช่วยให้ทุกคนสามารถเป็นผู้ซื้อและผู้ขายได้ง่าย ผ่านการติดต่อสื่อสารกันผ่านสื่อสังคมออนไลน์ต่าง ๆ หรือผ่านแพลตฟอร์มซื้อขายสินค้าออนไลน์ต่าง ๆ นอกจากการซื้อขายสินค้าออนไลน์ทั่วไปแล้ว ยังมีการสั่งซื้อสินค้าแบบจ่ายเงินล่วงหน้าหรือพรีออร์เดอร์ (Pre-order) การสมัครขอเงินกู้ดอกเบี้ยต่ำ และการทำธุรกรรมอื่น ๆ ทั้งนี้ได้มีรายงานของเฟซบุ๊กระบุว่า พ.ศ. 2562 ประเทศไทยกลายเป็นประเทศอันดับ 1 ในด้านการรับรู้และการใช้แชตออนไลน์เพื่อการซื้อสินค้าผ่านแพลตฟอร์มซื้อขายสินค้าออนไลน์ ซึ่งสอดคล้องกับการเปิดเผยของทาง VISA ที่ระบุว่า ประเทศไทยเป็นอันดับหนึ่งในด้านที่ผู้บริโภคใช้จ่ายผ่านโทรศัพท์เคลื่อนที่ในช่วงกลางปี พ.ศ. 2562 และรายงานเมื่อเดือนมกราคม พ.ศ. 2562 (Datareportal, 2020; Gimme, 2562; Nalisa, 2562) ผนวกกับสถานการณ์การระบาดของเชื้อไวรัสโคโรน่าสายพันธุ์ใหม่ (COVID-19) จึงมีผลทำให้ธุรกรรมออนไลน์ ซึ่งครอบคลุมถึงการสั่งซื้อสินค้าต่าง

ๆ ทั้งแบบแบบโอนเงินชำระค่าสินค้าปกติและแบบจ่ายเงินล่วงหน้า ไม่เว้นแม้แต่อาหาร ผ่านสื่อสังคมออนไลน์และแอปพลิเคชันต่าง ๆ เติบโตขึ้นเป็นอย่างมาก

โดยมีรายงานจากศูนย์วิจัยธนาคารออมสิน ระบุว่า ก่อนการแพร่ระบาดของไวรัสโคโรน่าสายพันธุ์ใหม่ (อ้างอิงข้อมูล ณ เดือน ก.พ. 2563 ที่ผ่านมา) มีการทำธุรกรรม 529.9 ล้านรายการ เติบโตขึ้น 68.5% และมีมูลค่าธุรกรรมการชำระเงินผ่าน Mobile Banking 2.3 ล้านล้านบาท เติบโตขึ้น 35.3% เมื่อเทียบกับเดือน ก.พ. 2562 ซึ่งข้อมูลนี้สอดคล้องกับข้อมูลของ สำนักงาน กสทช. ที่เปรียบเทียบการใช้งานแพลตฟอร์มออนไลน์ของคนไทย ระหว่างเดือนมกราคมถึงเดือนกุมภาพันธ์ 2563 พบว่า แพลตฟอร์มซื้อขายสินค้าออนไลน์ มียอดการเข้าใช้บริการเพิ่มขึ้นสูงมาก เช่น Shopee เพิ่มขึ้นประมาณ 479 % และ Lazada เพิ่มขึ้นประมาณ 122 % (Katchwattana, 2563; สพธอ., 2564ก) ซึ่งสะท้อนให้เห็นว่า คนไทยมีพฤติกรรมในการซื้อขายสินค้าออนไลน์มากขึ้น เพราะสะดวกทั้งผู้ซื้อและผู้ขาย ทั้งนี้ได้เคยมีคาดการณ์ในรายงานของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ว่า ในปี 2562 ประเทศไทยมีมูลค่า e-Commerce แบบ B2B (ย่อมาจาก Business to Business ซึ่งหมายถึงการค้าขายออนไลน์ระหว่างภาคเอกชนกับภาคเอกชนหรือระหว่างองค์กรธุรกิจ) และ B2C (ย่อมาจาก Business to Consumer ซึ่งหมายถึงการค้าขายออนไลน์ระหว่างภาคเอกชนกับภาคประชาชน) เพิ่ม 6.11% เป็น 1.91 ล้านล้านบาท และ 1.49 ล้านล้านบาท (สพธอ., 2564ข) จึงอนุมานได้ว่า มูลค่า e-Commerce แบบ C2C (ย่อมาจาก Consumer to Consumer ซึ่งหมายถึงการค้าขายออนไลน์ระหว่างภประชาชนกับภาคประชาชน) ก็น่าจะมีแนวแนวโน้มเติบโตเพิ่มขึ้นเช่นเดียวกัน

ถึงแม้ว่าความก้าวหน้าทางเทคโนโลยีสารสนเทศและการสื่อสารโทรคมนาคมจะช่วยเพิ่มความสะดวกสบายให้กับผู้ใช้บริการ แต่ก็แฝงไปด้วยภัยคุกคามจากผู้ไม่ประสงค์ดีที่อาศัยช่องโหว่ ทั้งจากคน ระบบ และกระบวนการ ตลอดจนข้อกฎหมายที่ยังมีจุดอ่อน และยังต้องการการพัฒนาให้เท่าทันเทคโนโลยีที่พัฒนาไปอย่างรวดเร็ว ทำให้ผู้ใช้บริการเกิดความเสียหาย กลายเป็นช่องทางให้มิจฉาชีพแอบแฝงเข้ามาหาผลประโยชน์ด้วยกลโกงรูปแบบต่าง ๆ โดยใช้การเปลี่ยนเลขหมายโทรศัพท์มือถือที่เป็นแบบเติมเงินไปเรื่อย ๆ และใช้เครือข่ายอินเทอร์เน็ตสาธารณะเป็นเครื่องมือหลักในการกระทำความผิดเพื่อหลอกเหยื่อซึ่งอาจเป็นผู้ซื้อหรือผู้ขายที่ไม่ได้ทำการตรวจสอบตัวตนจริงของบุคคลที่ทำธุรกรรมด้วยอย่างละเอียดถี่ถ้วน

ด้วยพันธกิจของสำนักงาน กสทช. โดยสำนักบริหารและจัดการเลขหมายโทรคมนาคม (จท.) ภายใต้สายงานกิจการโทรคมนาคม สำนักงาน กสทช. ในการกำกับ ควบคุมดูแลผู้ให้บริการคลื่นความถี่ จัดสรรและการกำกับการใช้เลขหมายโทรศัพท์ และได้มีการพัฒนาระบบลงทะเบียนยืนยันตัวตนของผู้ใช้บริการโทรศัพท์เคลื่อนที่ และพัฒนาระบบยืนยันตัวตนแบบอัตลักษณ์ สำหรับผู้ใช้บริการโทรศัพท์เคลื่อนที่แบบเติมเงิน ตั้งแต่ปี พ.ศ. 2556 จนถึงปัจจุบันซึ่งเป็นแนวทางสำคัญในการตรวจสอบข้อมูลของผู้ใช้บริการโทรศัพท์เคลื่อนที่ อย่างไรก็ดี ถึงแม้ว่าแนวทางดังกล่าวจะสามารถตรวจสอบและป้องกันการนำเลขหมายโทรศัพท์ไปใช้ในทางมิชอบแล้ว แต่ก็ยังไม่สามารถนำมาป้องกันและปราบปรามมิจฉาชีพออนไลน์ที่เป็นรายย่อยได้อย่างเป็นรูปธรรม

เนื่องด้วยปัจจุบันการทำธุรกรรมออนไลน์มีแนวโน้มเติบโตขึ้นเรื่อย ๆ ทำให้มิจฉาชีพใช้ช่องโหว่ดังกล่าวในการ กระทำความผิดทางออนไลน์ด้วยปัจจัยหลักคือ การที่ผู้เสียหายไม่สามารถที่จะหาหลักฐานหรือดำเนินการเอาผิดได้โดยง่าย อาทิเช่น การสั่งซื้อของออนไลน์แล้วไม่นำส่งของ สั่งสินค้าแบบจ่ายเงินล่วงหน้า (Pre-order) แล้วไม่ส่งของ การตอบรับการสมัครขอเงินกู้ดอกเบี้ยต่ำและการเสียค่าธรรมเนียม

เอกสารซึ่งไม่มีการยื่นกู้เงินจริง การซื้อขายของระหว่างบุคคลกับบุคลที่ไม่ได้ผ่านเว็บไซต์ที่ตรวจสอบความมีตัวตน ตามเว็บประกาศขาย หรือทางสื่อสังคมออนไลน์ Facebook , Instagram หรือ LINE การแฮกเข้าบัญชี Facebook หรือ LINE ของบุคคลอื่น และหลอกให้บุคคลอื่นโอนเงิน หรือ การทำธุรกรรมอื่น ๆ ทางออนไลน์ ซึ่งมิจฉาชีพออนไลน์มักจะมีกลโกงแอบแฝงอยู่ในรูปแบบต่าง ๆ เหล่านี้ จนทำให้ผู้ซื้อและผู้ขายไม่ได้มีการตรวจสอบตัวตนจริงของบุคคลที่ทำธุรกรรมอย่างละเอียดถี่ถ้วน ซึ่งแม้ในความเป็นจริงทางผู้เสียหายจะมีหลักฐานเบื้องต้นเช่นชื่อบัญชีธนาคาร สลิปการโอนเงินไปยังมิจฉาชีพ หรือตัวแทนของมิจฉาชีพ และเบอร์โทรศัพท์มือถือที่ใช้ติดต่อกัน แต่ก็ไม่สามารถดำเนินคดีเอาผิดได้โดยง่ายเนื่องจากการเปลี่ยนเลขหมายโทรศัพท์มือถือที่เป็นแบบเติมเงินไปเรื่อย ๆ และเป็นคดีความที่มีมูลค่าความเสียหายน้อย ทำให้ผู้เสียหายไม่อยากเสียเวลาในการแจ้งความดำเนินคดี ทั้งที่มิจฉาชีพเหล่านี้ได้กระทำความผิดในรูปแบบเดียวกันกับผู้เสียหายเป็นจำนวนมาก และมีมูลค่ารวมเป็นจำนวนมากแต่ก็ไม่ถูกดำเนินคดี

สำนักงาน กสทช. จึงได้มีประกาศรับคัดเลือกผู้ขอรับการส่งเสริมสนับสนุนจากเงินกองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะ เพื่อดำเนินโครงการจัดทำแนวทางพัฒนาระบบต้นแบบเพื่อสนับสนุนงานป้องกันและปราบปรามมิจฉาชีพออนไลน์ที่ไม่สามารถระบุตัวตน และศึกษาระบบการติดตาม ป้องกัน ต่อต้านการกระทำความผิดทางธุรกรรมการเงินผ่านช่องทางออนไลน์ หรือการทุจริตทางการเงินจากทั้งในและต่างประเทศเพื่อพัฒนาเป็นต้นแบบในการติดตามหาผู้กระทำความผิดมาดำเนินคดี และเป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 (ราชกิจจานุเบกษา, 2560) ซึ่งเป็นโครงการที่สอดคล้องกับความสนใจและความเชี่ยวชาญของคณะผู้วิจัย จึงเป็นที่มาของการยื่นข้อเสนอขอรับการส่งเสริมสนับสนุนจากเงินกองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะเพื่อดำเนินโครงการนี้ โดยคณะผู้วิจัยได้พิจารณาหาความร่วมมือกับหน่วยงานที่เกี่ยวข้อง และได้รับการตอบรับจากผู้กำกับการสืบสวนตำรวจภูธรจังหวัดนครนายก ซึ่งดูแลรับผิดชอบเขตพื้นที่จังหวัดนครนายก ซึ่งถือเป็นจังหวัดที่มีความเหมาะสมทางด้านสภาพเศรษฐกิจโดยรวม นอกจากนี้ยังใกล้กรุงเทพมหานครแม้จะไม่ใช่จังหวัดปริมณฑล

1.2 วัตถุประสงค์

1.2.1 เพื่อจัดทำแนวทาง หลักเกณฑ์ และระเบียบปฏิบัติ ในการรวบรวมพยานหลักฐานและดำเนินคดีธุรกรรมออนไลน์ของมิจฉาชีพรายย่อย เพื่อให้พนักงานสอบสวนรวบรวมพยานหลักฐานเพื่อดำเนินคดี และลงโทษผู้กระทำความผิด

1.2.2 เพื่อศึกษา และพัฒนาแนวทางการแลกเปลี่ยนข้อมูลพื้นฐานและข้อมูลที่สำคัญกับหน่วยงานที่เกี่ยวข้อง และพัฒนาระบบฐานข้อมูลมิจฉาชีพออนไลน์ในการตรวจสอบสำหรับพนักงานสอบสวน

1.2.3 เพื่อศึกษา ออกแบบและพัฒนาระบบต้นแบบสำหรับป้องกันและปราบปรามมิจฉาชีพแบบออนไลน์สำหรับพนักงานสอบสวนและประชาชน

1.2.4 จัดทำแผนสำหรับการจัดตั้งทีมงานที่เกี่ยวกับอาชญากรรมคอมพิวเตอร์โดยเฉพาะ เพื่อให้มีเจ้าหน้าที่ที่มีความรู้ ความชำนาญเฉพาะในการปราบปราม และดำเนินคดี

1.3 ขอบเขตการดำเนินงาน

ผู้ขอรับการส่งเสริมและสนับสนุนจากเงินกองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะที่ได้รับการคัดเลือก (ผู้รับทุน) จะต้องนำเงินที่ได้รับการส่งเสริมและสนับสนุน ไปดำเนินการโครงการจัดทำแนวทงพัฒนาระบบต้นแบบเพื่อสนับสนุนงานป้องกันและปราบปรามมิจฉาชีพออนไลน์ที่ไม่สามารถระบุตัวตน โดยมีภาระหน้าที่รับผิดชอบตามขอบเขตการดำเนินงาน รายละเอียด ดังต่อไปนี้

1.3.1 บูรณาการความร่วมมือ จัดทำความร่วมมือกับหน่วยงานที่เกี่ยวข้อง ได้แก่ สำนักงานตำรวจแห่งชาติ ธนาคาร เป็นต้น

1.3.2 ศึกษาและทบทวนวรรณกรมระบบการติดตาม ป้องกัน ต่อต้านการกระทำความผิดทางธุรกรรมทางการเงินผ่านช่องทางออนไลน์ หรีการทุจริตทางการเงิน จากทั้งในประเทศ และต่างประเทศ

1.3.3 ศึกษา รวบรวมข้อมูล ผู้เสียหายที่เป็นผู้ซื้อและผู้ขาย ที่มีมูลค่าความเสียหายต่อรายไม่เกิน 50,000 บาท ที่ทำธุรกรรมทางออนไลน์และธุรกรรมทางการเงินผ่านธนาคารกับบุคคลที่ไม่สามารถระบุตัวตนได้ ในเขตพื้นที่ศึกษา ย้อนหลังไม่น้อยกว่า 6 เดือน และในอนาคตสามารถพัฒนาระบบเพื่อรองรับยอดมูลค่าความเสียหายที่เพิ่มขึ้นได้โดยครอบคลุมรูปแบบการกระทำความผิด อย่างน้อย ดังนี้

1.3.3.1 ซื้อสินค้าผ่านออนไลน์ การซื้อขายตามเว็บประกาศขาย แล้วไม่ได้รับสินค้าตามกำหนด ผ่านทางสื่อสังคมออนไลน์ Facebook Instagram LINE หรือ การทำธุรกรรมอื่น ๆ ทางออนไลน์

1.3.3.2 ขายสินค้าผ่านออนไลน์ถูกกว่าท้องตลาด แล้วไม่มีสินค้าส่งจริง

1.3.3.3 ล่อลวงให้โอนเงินค่าสินค้าล่วงหน้า (Pre-order)

1.3.3.4 ล่อลวงให้โอนงินค่าทำสัญญาปล่อยเงินกู้นอกระบบดอกเบี้ยต่ำ อนุมัติง่าย ไม่ต้องตรวจสอบเครดิตบูโร

1.3.3.5 หลอกให้โอนเงินโดยการใช้การสวมรอบบัญชีอีเมล์ หรือ Social Media

1.3.3.6 แอบอ้างเป็นบุคคลต่าง ๆ หลอกว่าจะโอนเงินหรือส่งของให้ผ่านทางสื่อสังคมออนไลน์ Facebook, Instagram หรือ LINE

1.3.4 ศึกษา รวบรวมข้อมูล วิเคราะห์ปัจจัยภายใน และภายนอกที่เกี่ยวข้องกับธุรกรรมของคดีต่าง ๆ รวมทั้งปัจจัยที่เป็นช่องโหวในการกระทำความผิดของมิจฉาชีพ และช่องโหว่ที่ทำให้ผู้เสียหายขาดการตรวจสอบตัวตนก่อนการทำธุรกรรมทางออนไลน์ พร้อมทั้งมีจัดให้มีการประชุมเชิงปฏิบัติการโดยเชิญผู้เสียหาย พนักงานสอบสวน อัยการ และผู้เชี่ยวชาญในสายงานที่เกี่ยวข้อง ในเขตพื้นที่ศึกษา จำนวนไม่น้อยกว่า ๒๐ คนมาร่วมประชุมไม่น้อยกว่า ๒ ครั้ง

1.3.5 จัดทำสรุปผลการศึษา และผลการวิเคราะห์เป็นไปได้ในการพัฒนาระบบต้นแบบป้องกันและปราบปรามมิจฉชีพออนไลน์ที่ไสมารถระบุตัวตน ในเขตพื้นที่ศึกษา พร้อมแนวทาง การจัดทำหลักเกณฑ์ และระเบียบปฏิบัติในการรวบรวมพยานหลักฐานและดำเนินคดีที่สามารถทำได้ในปัจจุบันและแนวทางที่ควรจะดำเนินการในอนาคต

1.3.6 กำหนดแนวทางการแลกเปลี่ยนข้อมูลพื้นฐานและข้อมูลที่สำคัญในขั้นตอนรวบรวมพยานหลักฐาน เพื่อที่จะใช้ประกอบสำนวนเพื่อดำเนินคดีในชั้นศาล และประกอบการแจ้งอายัดบัญชีธนาคาร

1.3.7 งานออกแบบ และพัฒนาระบบแลกเปลี่ยนข้อมูล และระบบฐานข้อมูลมิจฉาชีพแบบออนไลน์ เพื่อใช้ติดตามคดี และเป็นข้อมูลประวัติผู้กระทำความผิด ในเขตพื้นที่ศึกษา อาทิเช่น เว็บบริการ

ทะเบียนราษฎร์ในการตรวจสอบชื่อที่อยู่ของผู้ถูกกล่าวหา เว็บบริการของโอเปอร์เรเตอร์เพื่อตรวจสอบเลขหมายต่าง ๆ กับเลขบัตรประชาชน เป็นต้น

1.3.8 งานศึกษา วิเคราะห์ และออกแบบระบบป้องกันและปราบปรามมิจฉาชีพแบบออนไลน์เพื่อรองรับการทำงานของพนักงานสอบสวน และผู้เสียหาย โดยมีระบบงานหลัก ดังนี้

1.3.8.1 ระบบยืนยันตัวตนระหว่างผู้ซื้อและผู้ขายก่อนทำธุรกรรมออนไลน์

1.3.8.2 ระบบตรวจสอบและค้นหลักฐานข้อมูลผู้กระทำความผิด ดำเนินคดี และผู้ถูกกล่าวหา

1.3.8.3 ระบบแจ้งความดำเนิดดีออนไลน์ ธุกรรมออนไลน์ที่ไม่สามารถระบุตัวตนผู้ถูกกล่าวหา

1.3.9 งานพัฒนาระบบยืนยันตัวตนของผู้ขายที่ต้องการจะรับโอนเงินก่อนส่งสินค้าหรือบริการเพื่อเป็นต้นแบบแนวทางปฏิบัติของผู้ขายที่ประกอบอาชีพสุจริต โดยต้องมีแนวทางการตรวจสอบอย่างน้อย ดังนี้

1.3.9.1 ระบบยืนยันตัวตนด้วยเลขหมายโทรศัพท์ และเลขบัตรประชาชนที่ใช้ลงทะเบียนซื้อซิมกับผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่

1.3.9.2 ระบบยืนยันตัวตนด้วยการตรวจสอบอัตลักษณ์บัตรประชาชนและรูปใบหน้าอัตโนมัติ

1.3.9.3 ระบบเชื่อมโยงข้อมูลการยืนยันตัวตนกับระบบงานอื่นตามที่ สำนักงาน กสทช. กำหนด

1.3.10 งานพัฒนาระบบตรวจสอบ สืบค้นข้อมูลของผู้ขาย และผู้ซื้อ ผ่านเว็บไซต์ เพื่อให้ประชาชนสามารถตรวจสอบประวัติของผู้ที่จะดำเนินธุรกรรมด้วยเบื้องต้นก่อนการตัดสินใจ สำหรับประชาชนในเขตพื้นที่ศึกษา โดยจะแสดงข้อมูลเฉพาะส่วนที่สามารถเปิดเผยได้ และไม่เปิดเผยข้อมูลชื่อหรือเลขหมายโทรศัพท์ของผู้กระทำความผิดต่อสาธารณะ และต้องเป็นไปตามกฎหมายเท่านั้น

1.3.11 งานพัฒนาระบบแจ้งความคดีธุรกรรมออนไลน์ที่ไม่สามารถระบุตัวตนผู้ถูกกล่าวหาได้ชัดเจน สำหรับประชาชนสามารถบันทึกข้อมูลหลักฐานทางอิเล็กทรอนิกส์ต่างๆ ประกอบสำนวนการดำเนินคดี เพื่อให้เจ้าหน้าที่ที่เกี่ยวข้องสามารถข้ามาตรวจสอบพยานหลักฐานของผู้แจ้งความในเบื้องต้นก่อนตัดสินใจรับแจ้งความ และสามารถตรวจสอบประวัติผู้ถูกกล่าวหาเพื่อพิจารณาแนวทางในการดำเนินคดีต่อไป

1.3.12 งานพัฒนาระบบแสดงผลรายงานสถิติต่าง ๆ สำหรับผู้บริหาร และพนักงานที่เกี่ยวข้อง พร้อมทั้งแจ้งเตือนผลความก้าวหน้าของคดีที่ต้องการติดตามเป็นพิเศษ

1.3.13 งานจัดหาบริการเครื่องคอมพิวเตอร์แม่ข่ายแบบคลาวด์ (Cloud Web Server) และเครื่องคอมพิวเตอร์แม่ข่ายสำหรับจัดเก็บฐานข้อมูล (Cloud Database Server) พร้อมอุปกรณ์ที่เกี่ยวข้องสำหรับโครงการที่มีขนาดความสามารถเหมาะสมกับระบบที่พัฒนาขึ้น เป็นระยะเวลาอย่างน้อย ๑๒ เดือน

1.3.14 จัดฝึกอบม และจัดตั้งทีมงานที่เกี่ยวกับอาชญากรรมคอมพิวเตอร์โดยเฉพาะ เพื่อให้มีเจ้าหน้าที่ที่มีความรู้ความชำนาญเฉพาะในการปราบปราม และดำเนินคดี โดยมีรายละเอียดอย่างน้อยดังนี้

1.3.14.1 จัดทำคู่มือการใช้งาน (User Manual) คู่มือการบำรุงรักษา (System Administrator Manual) โดยจะต้องครอบคลุมการใช้งานตามที่ได้ออกแบบ

1.3.14.2 จัดฝึกอบม และถ่ายทอดความรู้ให้กับเจ้าหน้าที่ดูแลระบบ และพัฒนาระบบที่เกี่ยวข้อง

1.3.14.3 จัดตั้งทีมงานที่สนับสนุนทางเทคนิคเพื่อรองรับการให้บริการพนักงานสอบสวน พร้อมเบอร์คอลเซ็นตอร์ จำนวน 2 อัตรา วันเวลาราชการ ตั้งแต่เวลา 09.00 น. ถึง 18.00 น.

1.4 ผลที่คาดว่าจะได้รับ

1.4.1 มีแนวทาง หลักเกณฑ์ และระเบียบปฏิบัติในการรวบรวมพยานหลักฐานในการดำเนินคดีธุรกรรมรายย่อยของผู้เสียหายในเขตพื้นที่ศึกษา

1.4.2 มีระบบต้นแบบในการป้องกันและปราบปรามคดีธุรกรรมออนไลน์ที่ไม่สามารถระบุตัวตนผู้ถูกกล่าวหาได้ในเขตพื้นที่ศึกษา

1.4.3 มีศูนย์คอลเซ็นเตอร์ที่ช่วยให้พนักงานสอบสวนสามารถโทรปรึกษาวิธีใช้งานและช่วยให้พนักงานสอบสวนปฏิบัติงานได้ง่ายขึ้น

1.4.4 เพิ่มประสิทธิภาพในการช่วยเหลือประชาชนตามภารกิจของเจ้าหน้าที่ตำรวจของพื้นที่ศึกษาให้มีประสิทธิภาพมากยิ่งขึ้น

1.4.5 ลดความซ้ำซ้อนของการทำงาน และระยะเวลาในการทำสำนวนของคดีได้รวมเร็วยิ่งขึ้น

ตารางที่ 1-1 การส่งมอบงานในแต่ละงวด

ผลงานที่ต้องส่งมอบ	เนื้อหาของรายงาน	ระยะเวลาที่ต้องส่งมอบผลงาน	จำนวนที่ส่งมอบ
1) รายงานฉบับที่ 1 รายงานผลการศึกษาเบื้องต้น (Inception Report)	แผนการดำเนินโครงการโดยละเอียด ไดแก รูปแบบ/วิธีการดำเนินงาน ขั้นตอนและระยะเวลาการดำเนินงาน โดยแผนการดำเนินงานจะตองมีความชัดเจนสมบูรณและนำไปปฏิบัติไดจริง และผลการดำเนินงานตามขอบเขตงานขอ 4.1 – 4.2	45 วัน	เอกสารสิ่งพิมพและแฟ้มข้อมูลอิเล็กทรอนิกส์ (.doc และ .pdf) จำนวน 6 ชุด
2) รายงานฉบับที่ 2 รายงานความก้าวหน้าฉบับที่ 1	รายงานผลการศึกษาเบื้องตน (Inception Report) และผลการดำเนินงานตามขอบเขตงานขอ 4.3 – 4.6	120 วัน	เอกสารสิ่งพิมพและแฟ้มข้อมูลอิเล็กทรอนิกส์ (.doc และ .pdf) จำนวน 6 ชุด
3) รายงานฉบับที่ 3 รายงานความก้าวหน้าฉบับที่ 2	รายงานความก้าวหนาฉบับที่ 1 และผลการดำเนินงานตามขอบเขตงานขอ 4.7 – 4.11	250 วัน	เอกสารสิ่งพิมพและแฟ้มข้อมูลอิเล็กทรอนิกส์ (.doc และ .pdf) จำนวน 6 ชุด
4) รายงานฉบับที่ 4 รายงานฉบับสมบูรณ์ (Final Report)	(1) รายงานสรุปผลการการดำเนินงานตามแผนทั้งหมด (2) รายงานการพัฒนาระบบทั้งหมด (3) สรุปผลการพัฒนา ทดสอบและฝกอบรมเกี่ยวกับการบริหารจัดการ ดูแลรักษา ออกแบบ พัฒนาและเขาใชงานระบบที่เสนอทั้งหมดพรอมทั้งสงมอบเอกสารการพัฒนา (4) รายงานผลการทดสอบระบบและเอกสารรายงานอื่น ๆ ที่เกี่ยวของ (5) บทสรุปผูบริหาร ฉบับภาษาไทย พิมพ 4 สี (6) เนื้อหารายงานความกาวหนาฉบับที่ 2	360 วัน	เอกสารสิ่งพิมพและแฟ้มข้อมูลอิเล็กทรอนิกส์ (.doc และ .pdf) จำนวน 6 ชุด

1.5 แผนงานและตารางการดำเนินโครงการ

คณะผู้วิจัยจะนำเงินที่ได้รับการส่งเสริมและสนับสนุน ไปดำเนินโครงการพัฒนาระบบต้นแบบเพื่อสนับสนุนงานป้องกันและปราบปรามมิจฉาชีพออนไลน์ (ระยะที่ 1) : กรณีศึกษา เขตพื้นที่ตำรวจภูธรจังหวัดนครนายก โดยมีภาระหน้าที่รับผิดชอบตามขอบเขตการดำเนินงาน ซึ่งแบ่งเป็นกิจกรรมต่าง ๆ ดังนี้

1.4.1 กิจกรรมหลักที่ 1 ดำเนินการศึกษาศึกษาและทบทวนวรรณกรรมระบบการติดตาม ป้องกันต่อต้านการกระทำความผิดทางธุรกรรมทางการเงินผ่านช่องทางออนไลน์ หรือการทุจริตทางการเงิน จากทั้งในประเทศ และต่างประเทศ

1.4.2 กิจกรรมหลักที่ 2 ดำเนินการศึกษา และรวบรวมข้อมูล จากผู้เสียหาย ฝ่ายกฎหมาย และฝ่ายต่าง ๆ ที่เกี่ยวข้อง

- กิจกรรมรองที่ 2.1 ดำเนินการศึกษา และรวบรวมข้อมูลผู้เสียหายที่เป็นผู้ซื้อและผู้ขาย ที่มีมูลค่าความเสียหายต่อรายไม่เกิน 50,000 บาท ที่ทำธุรกรรมทางออนไลน์และธุรกรรมทางการเงินผ่านธนาคารกับบุคคลที่ไม่สามารถระบุตัวตนได้ ในเขตพื้นที่ศึกษาตำรวจภูธรจังหวัดนครนายก ย้อนหลังไม่น้อยกว่า 6 เดือน โดยครอบคลุมรูปแบบการกระทำผิดต่อไปนี้
    1) การซื้อขายตามเว็บประกาศขายผ่านทางสื่อสังคมออนไลน์ต่าง ๆ เช่น เฟซบุ๊ก อินสตราแกรม ไลน์ หรือการทำธุรกรรมอื่น ๆ ทางออนไลน์ แล้วไม่ได้รับสินค้าตามกำหนด
    2) การขายสินค้าผ่านออนไลน์ถูกกว่าท้องตลาด แล้วไม่มีสินค้าส่งจริง
    3) การล่อลวงให้โอนเงินค่าสินค้าล่วงหน้าหรือพรีออร์เดอร์
    4) การล่อลวงให้โอนเงินค่าทำสัญญาปล่อยเงินกู้นอกระบบดอกเบี้ยต่ำ อนุมัติง่าย ไม่ต้องตรวจสอบเครดิตบูโร
    5) การหลอกให้โอนเงินโดยการใช้การสวมรอยบัญชีอีเมล์ หรือสื่อสังคมออนไลน์
    6) การแอบอ้างเป็นบุคคลต่าง ๆ หลอกว่าจะโอนเงินหรือส่งของให้ผ่านทางสื่อสังคมออนไลน์
- กิจกรรมรองที่ 2.2 ดำเนินการศึกษา รวบรวมข้อมูล วิเคราะห์ปัจจัยภายใน และภายนอกที่เกี่ยวข้องกับธุรกรรมของคดีต่าง ๆ รวมทั้งปัจจัยที่เป็นช่องโหว่ในการกระทำความผิดของมิจฉาชีพ และช่องโหว่ที่ทำให้ผู้เสียหายขาดการตรวจสอบตัวตนก่อนการทำธุรกรรมทางออนไลน์
- กิจกรรมรองที่ 2.3 ดำเนินการจัดประชุม

14.3 กิจกรรมหลักที่ 3 ดำเนินการออกแบบและพัฒนาระบบต้นแบบ

- กิจกรรมรองที่ 3.1 ดำเนินการออกแบบระบบยืนยันตัวตน
- กิจกรรมรองที่ 3.2 ดำเนินการออกแบบและพัฒนาระบบตรวจสอบข้อมูลผู้ซื้อผู้ขาย
- กิจกรรมรองที่ 3.3 ดำเนินการออกแบบระบบเชื่อมโยงข้อมูลกับระบบสำนักงานตำรวจแห่งชาติ
- กิจกรรมรองที่ 3.4 ดำเนินการออกแบบระบบเชื่อมโยงข้อมูลกับระบบสำนักงาน กสทช.
- กิจกรรมรองที่ 3.5 ดำเนินการออกแบบระบบแจ้งความอิเล็กทรอนิกส์ผ่านตู้คีออส

- กิจกรรมรองที่ 3.6 ดำเนินการออกแบบระบบรายงาน
- กิจกรรมรองที่ 3.7 ดำเนินการพัฒนาระบบยืนยันตัวตน
- กิจกรรมรองที่ 3.8 ดำเนินการพัฒนาระบบตรวจสอบข้อมูลผู้ซื้อผู้ขาย
- กิจกรรมรองที่ 3.9 ดำเนินการพัฒนาระบบเชื่อมโยงข้อมูลกับระบบสำนักงานตำรวจแห่งชาติ
- กิจกรรมรองที่ 3.10 ดำเนินการพัฒนาระบบเชื่อมโยงข้อมูลกับระบบสำนักงาน กสทช.
- กิจกรรมรองที่ 3.11 ดำเนินการพัฒนาระบบแจ้งความอิเล็กทรอนิกส์ผ่านตู้คีออส
- กิจกรรมรองที่ 3.12 ดำเนินการพัฒนาระบบรายงาน

14.4 กิจกรรมหลักที่ 4 ดำเนินการจัดทำคูมือการใชงาน และคูมือสำหรับผู้ดูแลระบบ

- กิจกรรมรองที่ 4.1 ดำเนินการจัดทำคู่มือการใช้งาน
- กิจกรรมรองที่ 4.2 ดำเนินการจัดทำคู่มือสำหรับผู้ดูแลระบบ

14.5 กิจกรรมหลักที่ 5 ดำเนินการจัดอบรมการใช้งานและการดูแลระบบ

- กิจกรรมรองที่ 5.1 ดำเนินการจัดอบรมการใช้งานให้กับเจ้าหน้าที่
- กิจกรรมรองที่ 5.2 ดำเนินการจัดอบรมการดูแลระบบให้กับเจ้าหน้าที่
- กิจกรรมรองที่ 5.3 ดำเนินการจัดตั้งทีมงานสนับสนุนทางเทคนิคเพื่อรองรับการให้บริการพนักงานสอบสวนพร้อมเลขหมายคอลเซ็นเตอร์ จำนวน 2 อัตรา

14.6 กิจกรรมหลักที่ 6 ดำเนินการประชาสัมพันธ์

- กิจกรรมรองที่ 6.1 ดำเนินการผลิตวีดิทัศน์ประชาสัมพันธ์เชิญชวนให้ผู้ซื้อและผู้ขายสินค้าออนไลน์เข้าลงทะเบียนในระบบ ผ่านสื่อสังคมออนไลน์ และสื่อหนังสือพิมพ์หรือวิทยุ อย่างน้อย 1 แห่ง
- กิจกรรมรองที่ 6.2 ดำเนินการผลิตวีดิทัศน์หรือสื่ออินโฟกราฟิค เพื่อใช้ประชาสัมพันธ์โครงการและเพื่อเผยแพร่ผ่านสื่อสังคมออนไลน์ และจัดให้มีการเผยแพร่ผ่านสื่อหนังสือพิมพ์หรือวิทยุ อย่างน้อย 1 แห่ง

14.7 กิจกรรมหลักที่ 7 ดำเนินการจัดทำรายงาน

- กิจกรรมรองที่ 7.1 ดำเนินการจัดทำรายงานผลการศึกษาเบื้องต้น
- กิจกรรมรองที่ 7.2 ดำเนินการจัดทำรายงานความก้าวหน้าฉบับที่ 1
- กิจกรรมรองที่ 7.3 ดำเนินการจัดทำรายงานความก้าวหน้าฉบับที่ 2
- กิจกรรมรองที่ 7.4 ดำเนินการจัดทำรายงานความก้าวหน้าฉบับสมบูรณ์
    - กิจกรรมย่อยที่ 7.4.1 รายงานสรุปผลการการดำเนินงานตามแผน
    - กิจกรรมย่อยที่ 7.4.2 รายงานการพัฒนาระบบ
    - กิจกรรมย่อยที่ 7.4.3 สรุปผลการพัฒนา ทดสอบและฝึกอบรมเกี่ยวกับการบริหารจัดการ การดูแลรักษา การออกแบบ การพัฒนาและการเข้าใช้งานระบบ
    - กิจกรรมย่อยที่ 7.4.4 รายงานผลการทดสอบระบบและรายงานอื่น ๆ ที่เกี่ยวข้อง
    - กิจกรรมย่อยที่ 7.4.5 บทสรุปผู้บริหาร ฉบับภาษาไทย พิมพ์ 4 สี

ตารางที่ 1-2 แผนการดำเนินงาน

การดำเนินงาน	ช่วงเวลาที่ดำเนินงาน											
	1	2	3	4	5	6	7	8	9	10	11	12
กิจกรรมหลักที่ 1 ดำเนินการศึกษาศึกษาและทบทวนวรรณกรรมระบบการติดตาม ป้องกันต่อต้านการกระทำความผิดทางธุรกรรมทางการเงินผ่านช่องทางออนไลน์ หรือการทุจริตทางการเงิน จากทั้งในประเทศ และต่างประเทศ												
กิจกรรมหลักที่ 2 ดำเนินการศึกษา และรวบรวมข้อมูล จากผู้เสียหาย ฝ่ายกฎหมาย และฝ่ายต่าง ๆ ที่เกี่ยวข้อง												
• กิจกรรมรองที่ 2.1 ดำเนินการศึกษา และรวบรวมข้อมูลผู้เสียหายที่เป็นผู้ซื้อและผู้ขาย ที่มีมูลค่าความเสียหายต่อรายไม่เกิน 50,000 บาท ที่ทำธุรกรรมทางออนไลน์และธุรกรรมทางการเงินผ่านธนาคารกับบุคคลที่ไม่สามารถระบุตัวตนได้ ในเขตพื้นที่ศึกษาตำรวจภูธรจังหวัดนครนายก ย้อนหลังไม่น้อยกว่า 6 เดือน												
• กิจกรรมรองที่ 2.2 ดำเนินการศึกษา รวบรวมข้อมูล วิเคราะห์ปัจจัยภายใน และภายนอกที่เกี่ยวข้องกับธุรกรรมของคดีต่าง ๆ รวมทั้งปัจจัยที่เป็นช่องโหว่ในการกระทำความผิดของมิจฉาชีพ และช่องโหว่ที่ทำให้ผู้เสียหายขาดการตรวจสอบตัวตนก่อนการทำธุรกรรมทางออนไลน์												
• กิจกรรมรองที่ 2.3 ดำเนินการจัดประชุม												
o กิจกรรมย่อยที่ 2.3.1 ประชุมเปิดโครงการอย่างเป็นทางการและประชุมเชิงปฏิบัติการสนทนากลุ่ม ครั้งที่ 1 (มีการประชุม 2 กลุ่ม)												
o กิจกรรมย่อยที่ 2.3.2 ประชุมเชิงปฏิบัติการสนทนากลุ่ม ครั้งที่ 2 พร้อมนำเสนอแนวทาง หลักเกณฑ์และระเบียบปฏิบัติในการรวบรวมพยานหลักฐานและดำเนินคดีที่สามารถทำได้ในปัจจุบัน และแนวทางที่ควรจะดำเนินการในอนาคต												
o กิจกรรมย่อยที่ 2.3.3 ประชุมแถลงผลการดำเนินโครงการ												
กิจกรรมหลักที่ 3 ดำเนินการออกแบบและพัฒนาระบบต้นแบบ												
• กิจกรรมรองที่ 3.1 ดำเนินการออกแบบระบบยืนยันตัวตน												
• กิจกรรมรองที่ 3.2 ดำเนินการออกแบบระบบตรวจสอบข้อมูลผู้ซื้อผู้ขาย												
• กิจกรรมรองที่ 3.3 ดำเนินการออกแบบระบบเชื่อมโยงข้อมูลกับระบบสำนักงานตำรวจแห่งชาติ												
• กิจกรรมรองที่ 3.4 ดำเนินการออกแบบระบบเชื่อมโยงข้อมูลกับระบบสำนักงาน กสทช.												
• กิจกรรมรองที่ 3.5 ดำเนินการออกแบบระบบแจ้งความอิเล็กทรอนิกส์ผ่านตู้คีออส												
• กิจกรรมรองที่ 3.6 ดำเนินการออกแบบระบบรายงาน												
• กิจกรรมรองที่ 3.7 ดำเนินการพัฒนาระบบยืนยันตัวตน												
• กิจกรรมรองที่ 3.8 ดำเนินการพัฒนาระบบตรวจสอบข้อมูลผู้ซื้อผู้ขาย												
• กิจกรรมรองที่ 3.9 ดำเนินการพัฒนาระบบเชื่อมโยงข้อมูลกับระบบสำนักงานตำรวจแห่งชาติ												
• กิจกรรมรองที่ 3.10 ดำเนินการพัฒนาระบบเชื่อมโยงข้อมูลกับระบบสำนักงาน กสทช.												
• กิจกรรมรองที่ 3.11 ดำเนินการพัฒนาระบบแจ้งความอิเล็กทรอนิกส์ผ่านตู้คีออส												
• กิจกรรมรองที่ 3.12 ดำเนินการพัฒนาระบบรายงาน												
กิจกรรมหลักที่ 4 ดำเนินการจัดทำคู่มือการใช้งาน และคู่มือสำหรับผู้ดูแลระบบ												
• กิจกรรมรองที่ 4.1 ดำเนินการจัดทำคู่มือการใช้งาน												

การดำเนินงาน	ช่วงเวลาที่ดำเนินงาน											
	1	2	3	4	5	6	7	8	9	10	11	12
● กิจกรรมรองที่ 4.2 ดำเนินการจัดทำคู่มือสำหรับผู้ดูแลระบบ												
กิจกรรมหลักที่ 5 ดำเนินการจัดอบรมการใช้งานและการดูแลระบบ												
● กิจกรรมรองที่ 5.1 ดำเนินการจัดอบรมการใช้งานให้กับเจ้าหน้าที่												
● กิจกรรมรองที่ 5.2 ดำเนินการจัดอบรมการดูแลระบบให้กับเจ้าหน้าที่												
● กิจกรรมรองที่ 5.3 ดำเนินการจัดตั้งทีมงานสนับสนุนทางเทคนิคเพื่อรองรับการให้บริการ พนักงานสอบสวนพร้อมเลขหมายคอลเซ็นเตอร์ จำนวน 2 อัตรา												
กิจกรรมหลักที่ 6 ดำเนินการประชาสัมพันธ์												
● กิจกรรมรองที่ 6.1 ดำเนินการผลิตวิดีทัศน์ประชาสัมพันธ์เชิญชวนให้ผู้ซื้อและผู้ขายสินค้าออนไลน์เข้าลงทะเบียนในระบบ ผ่านสื่อสังคมออนไลน์ และสื่อหนังสือพิมพ์หรือวิทยุ												
● กิจกรรมรองที่ 6.2 ดำเนินการผลิตวิดีทัศน์หรือสื่ออินโฟกราฟิก เพื่อใช้ประชาสัมพันธ์โครงการและเพื่อเผยแพร่ผ่านสื่อสังคมออนไลน์ และจัดให้มีการเผยแพร่ผ่านสื่อหนังสือพิมพ์หรือวิทยุ												
กิจกรรมหลักที่ 7 ดำเนินการจัดทำรายงาน												
● กิจกรรมรองที่ 7.1 ดำเนินการจัดทำรายงานผลการศึกษาเบื้องต้น												
● กิจกรรมรองที่ 7.2 ดำเนินการจัดทำรายงานความก้าวหน้าฉบับที่ 1												
● กิจกรรมรองที่ 7.3 ดำเนินการจัดทำรายงานความก้าวหน้าฉบับที่ 2												
● กิจกรรมรองที่ 7.4 ดำเนินการจัดทำรายงานความก้าวหน้าฉบับสมบูรณ์												
o กิจกรรมย่อยที่ 7.4.1 รายงานสรุปผลการการดำเนินงานตามแผน												
o กิจกรรมย่อยที่ 7.4.2 รายงานการพัฒนาระบบ												
o กิจกรรมย่อยที่ 7.4.3 สรุปผลการพัฒนา ทดสอบและฝึกอบรมเกี่ยวกับการบริหารจัดการ การดูแลรักษา การออกแบบ การพัฒนาและการเข้าใช้งานระบบ												
o กิจกรรมย่อยที่ 7.4.4 รายงานผลการทดสอบระบบและรายงานอื่น ๆ ที่เกี่ยวข้อง												
o กิจกรรมย่อยที่ 7.4.5 บทสรุปผู้บริหาร ฉบับภาษาไทย พิมพ์ ๔ สี												
o กิจกรรมย่อยที่ 7.4.6 จัดทำรายงานที่งานพัฒนาระบบแสดงผลรายงานสถิติต่าง ๆ สำหรับผู้บริหาร และพนักงานที่เกี่ยวข้อง (ครอบคลุมรายงานผลความก้าวหน้าของคดีที่ต้องการติดตามเป็นพิเศษ)												

บรรณานุกรม

ธนาคารแห่งประเทศไทย. (2564). การชำระเงินผ่านระบบการชำระเงินและช่องทางต่าง ๆ. Retrieved May 9, 2021, From https://www.bot.or.th/App/BTWS_STAT/statistics/ReportPage.aspx?reportID=681&language=th

ราชกิจจานุเบกษา. (2560). พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐. Retrieved May 9, 2021, From http://www.ratchakitcha.soc.go.th/DATA/PDF/2560/A/010/24.PDF

สพธอ. (2564ก). ETDA แนะพลิกวิกฤตให้เป็นโอกาส ขายของออนไลน์อยู่บ้านนั่งนับเงิน ช่วงโควิด-19. Retrieved May 3, 2021, From https://www.etda.or.th/th/newsevents/pr-

news/eCommerce/ETDA-แนะพลกวกฤตใหเปนโอกาส-ขายของออนไลนอยบานนงนบเงน.aspx?feed=590fb9ad-c550-4bc5-9a56-459ad4891d74

สพธอ. (2564ข). รายงานผลการสำรวจมูลค่าพาณิชย์อิเล็กทรอนิกส์ในประเทศไทย ปี 2561 (ฉบับปรับปรุง). Retrieved May 3, 2021, From https://www.etda.or.th/th/https/www-etda-or-th/th/newsevents/pr/Value-of-e-Commerce-Survey-in-Thailand-2019.aspx

Datareportal. (2020). DIGITAL 2020: THAILAND. Retrieved May 3, 2021, From https://datareportal.com/reports/digital-2020-thailand

Gimme. (2562). สัดส่วนผู้คนซื้อขายของผ่านทางมือถือ. Retrieved May 3, 2021, From https://droidsans.com/thailand-world-top-mobile-purchase/

Nalisa. (2562). เทรนด์ช้อปปิ้งผ่านแชทออนไลน์มากที่สุดในโลก. Retrieved May 3, 2021, From https://marketeeronline.co/archives/131754

Katchwattana, P. (2563). ยกระดับ Digital & Mobile Banking ทางรอด ‘ธุรกิจธนาคาร’ หลังวิกฤตโควิด. Retrieved May 3, 2021, From https://www.salika.co/2020/06/03/new-way-of-digital-mobile-banking-for-bank-fight-covid/

บทที่ 2
การทบทวนวรรณกรรม

2.1 แนวคิดสำหรับวิธีการหลอกลวงทางเทคโนโลยี

2.1.1 คำจัดกับความของคดีฉ้อโกง และบทลงโทษ

2.1.1.1 ความผิดฐานฉ้อโกง

การกระทำความผิดฐานฉ้อโกงนั้นก็คือการหลอกลวงคนอื่นด้วยการแสดงข้อความอันเป็นเท็จ หรือปกปิดความจริงที่ควรบอก ซึ่งเป็นการกระทำโดยทุจริต และการหลอกลวงทำให้ได้ทรัพย์สินไปจากผู้ถูกหลอกลวงหรือคนอื่นๆ หรือทำให้ผู้ถูกหลอกลวงหรือคนอื่นต้องทำ ถอนหรือทำลายเอกสารสิทธิ ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกพันบาท หรือทั้งจำทั้งปรับ ซึ่งในปัจจุบันส่วนมากจะเป็นความผิดฐานฉ้อโกงแบบนี้ ซึ่งการฉ้อโกงนั้นมีหลายลักษณะ เช่น การฉ้อโกงประชาชน การฉ้อโกงแรงงาน การหลอกกินอาหารและเครื่องดื่มฟรี เป็นต้น สามารถแบ่งได้ตามประมวลกฎหมายอาญา มาตรา 341 – 348 โดยมีรายละเอียดดังนี้

1) มาตรา 341 ผู้ใดโดยทุจริต หลอกลวงผู้อื่นด้วยการแสดงข้อความอันเป็นเท็จ หรือปกปิดข้อความจริงซึ่งควรบอกให้แจ้ง และโดยการหลอกลวงดังว่านั้นได้ไปซึ่งทรัพย์สินจากผู้ถูกหลอกลวงหรือบุคคลที่สาม หรือทำให้ผู้ถูกหลอกลวงหรือบุคคลที่สาม ทำ ถอน หรือทำลายเอกสารสิทธิ ผู้นั้นกระทำความผิดฐานฉ้อโกง ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ (สถาบันนิติธรรมาลัย, 2564)
2) มาตรา 342 ถ้าในการกระทำความผิดฐานฉ้อโกง ผู้กระทำ (๑) แสดงตนเป็นคนอื่น หรือ (๒) อาศัยความเบาปัญญาของผู้ถูกหลอกลวงซึ่งเป็นเด็ก หรืออาศัยความอ่อนแอแห่งจิตของผู้ถูกหลอกลวง ผู้กระทำต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ (สถาบันนิติธรรมาลัย, 2564)
3) มาตรา 343 ถ้าการกระทำความผิดตามมาตรา 341 ได้กระทำด้วยการแสดงข้อความอันเป็นเท็จต่อประชาชน หรือด้วยการปกปิดความจริงซึ่งควรบอกให้แจ้งแก่ประชาชน ผู้กระทำต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ (สถาบันนิติธรรมาลัย, 2564)
   ถ้าการกระทำความผิดดังกล่าวในวรรคแรก ต้องด้วยลักษณะดังกล่าวในมาตรา 342 อนุมาตราหนึ่งอนุมาตราใดด้วย ผู้กระทำต้องระวางโทษจำคุกตั้งแต่หกเดือนถึงเจ็ดปี และปรับตั้งแต่หนึ่งหมื่นบาทถึงหนึ่งแสนสี่หมื่นบาท (สถาบันนิติธรรมาลัย, 2564)
4) มาตรา 344 ผู้ใดโดยทุจริต หลอกลวงบุคคลตั้งแต่สิบคนขึ้นไปให้ประกอบการงานอย่างใด ๆ ให้แก่ตนหรือให้แก่บุคคลที่สาม โดยจะไม่ใช้ค่าแรงงานหรือค่าจ้างแก่บุคคลเหล่านั้น หรือโดยจะใช้ค่าแรงงานหรือค่าจ้างแก่บุคคลเหล่านั้นต่ำกว่าที่ตกลงกัน ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ (สถาบันนิติธรรมาลัย, 2564)

5) มาตรา 345 ผู้ใดสั่งซื้อและบริโภคอาหารหรือเครื่องดื่ม หรือเข้าอยู่ในโรงแรม โดยรู้ว่าตนไม่สามารถชำระเงินค่าอาหาร ค่าเครื่องดื่ม หรือค่าอยู่ในโรงแรมนั้น ต้องระวางโทษจำคุกไม่เกินสามเดือน หรือปรับไม่เกินห้าพันบาท หรือทั้งจำทั้งปรับ (สถาบันนิติธรรมาลัย, 2564)
6) มาตรา 346 ผู้ใดเพื่อเอาทรัพย์สินของผู้อื่นเป็นของตนหรือของบุคคลที่สาม ชักจูงผู้หนึ่งผู้ใดให้จำหน่ายโดยเสียเปรียบซึ่งทรัพย์สิน โดยอาศัยเหตุที่ผู้ถูกชักจูงมีจิตอ่อนแอ หรือเป็นเด็กเบาปัญญา และไม่สามารถเข้าใจตามควรซึ่งสาระสำคัญแห่งการกระทำของตน จนผู้ถูกชักจูงจำหน่ายซึ่งทรัพย์สินนั้น ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ (สถาบันนิติธรรมาลัย, 2564)
7) มาตรา 347 ผู้ใดเพื่อให้ตนเองหรือผู้อื่นได้รับประโยชน์จากการประกันวินาศภัย แกล้งทำให้เกิดเสียหายแก่ทรัพย์สินอันเป็นวัตถุที่เอาประกันภัย ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ (สถาบันนิติธรรมาลัย, 2564)
8) มาตรา 348 ความผิดในหมวดนี้ นอกจากความผิดตามมาตรา 343 เป็นความผิดอันยอมความได้ (สถาบันนิติธรรมาลัย, 2564)

ทั้งนี้ความผิดฐานฉ้อโกง ถือเป็นความผิดที่ยอมความกันได้ ซึ่งหมายถึงผู้เสียหายและผู้กระทำความผิด สามารถเจรจา คืนทรัพย์สิน หรือชำระค่าเสียหายเพื่อยุติคดี แต่ยกเว้น "ความผิดฐานฉ้อโกงประชาชน" ผู้เสียหายต้องดำเนินการแจ้งความ หรือฟ้องคดีภายในเวลา 3 เดือน นับตั้งแต่ทราบเรื่องและรู้ตัว ผู้กระทำผิด ไม่เช่นนั้น คดีจะขาดอายุความ

นอกจากความผิดฐานฉ้อโกง ตามประมวลกฎหมายอาญา มาตรา 341 – 348 แล้ว การกระทำความผิดในรูปแบบการฉ้อโกงออนไลน์ สามารถเชื่อมโยงไปยังความผิดอื่น ๆ ที่ถูกประกาศไว้ในพระราชบัญญัติอื่น ๆ ได้อีกด้วย เช่น

1) พ.ร.บ.คอมพิวเตอร์ - พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 (ราชกิจจานุเบกษา, 2560) โดยมีมาตราที่เกี่ยวข้องดังนี้

มาตรา 5 ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 6 ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 7 ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 8 ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และ

ข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 14 วรรคหนึ่ง (1) ซึ่งบัญญัติว่า "ผู้ใดกระทำความผิดโดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา ผู้นั้นต้องระวางโทษจำคุกไม่เกินห้าปีหรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ" และถ้าการกระทำความผิดข้างต้นมิได้กระทำต่อประชาชน แต่เป็นการกระทำต่อบุคคลใดบุคคลหนึ่ง ผู้กระทำ ผู้เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์ดังกล่าวต้องระวางโทษจำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 6 หมื่นบาท หรือทั้งจำทั้งปรับ และให้เป็นความผิดอันยอมความได้ตามมาตรา 14 วรรคท้าย

2) พ.ร.บ. คอมพิวเตอร์ - พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ได้ระบุทลงโทษในมาตรา 73 ว่า ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลของผู้ใช้บริการหรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ที่พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้ และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใดโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาทหรือทั้งจำทั้งปรับ (ประชาชาติธุรกิจ, 2563)
3) พ.ร.บ. เงินกู้ – พระราชกำหนดการกู้ยืมเงินที่เป็นการฉ้อโกงประชาชน พ.ศ. 2527 มาตรา 4 "ผู้ใดโฆษณาหรือประกาศให้ปรากฏต่อประชาชนหรือกระทำด้วยประการใด ๆ ให้ปรากฏแก่บุคคลตั้งแต่สิบคนขึ้นไปว่า ในการกู้ยืมเงินตนหรือบุคคลใดจะจ่ายหรืออาจจ่ายผลประโยชน์ตอบแทนให้ตามพฤติการณ์แห่งการกู้ยืมเงินในอัตราที่สูงกว่าอัตราดอกเบี้ยสูงสุดที่สถาบันการเงินตามกฎหมายว่าด้วยดอกเบี้ยเงินให้กู้ยืมของสถาบันการเงินจะพึงจ่ายได้ โดยที่ตนรู้หรือควรรู้อยู่แล้วว่าตนหรือบุคคลนั้นจะนำเงินจากผู้ให้กู้ยืมเงินรายนั้นหรือรายอื่นมาจ่ายหมุนเวียนให้แก่ผู้ให้กู้ยืมเงิน หรือโดยที่ตนรู้หรือควรรู้อยู่แล้วว่า ตนหรือบุคคลนั้นไม่สามารถประกอบกิจการใด ๆ โดยชอบด้วยกฎหมายที่จะให้ผลประโยชน์ตอบแทนพอเพียงที่จะนำมาจ่ายในอัตรานั้นได้ และในการนั้นเป็นเหตุให้ตนหรือบุคคลใดได้กู้ยืมเงินไป ผู้นั้นกระทำความผิดฐานกู้ยืมเงินที่เป็นการฉ้อโกงประชาชน (ปุณิกา และ ปริยานุช, 2560)
ผู้ใดไม่มีใบอนุญาตให้ประกอบธุรกิจเกี่ยวกับปัจจัยชำระเงินต่างประเทศตามกฎหมายว่าด้วยการควบคุมการแลกเปลี่ยนเงิน ดำเนินการ หรือให้พนักงาน ลูกจ้าง หรือบุคคลใดดำเนินการโฆษณา ประกาศหรือชักชวนประชาชนให้ลงทุนโดย
(1) ซื้อหรือขายเงินตราสกุลใดสกุลหนึ่งหรือหลายสกุล หรือ
(2) เก็งกำไรหรืออาจจะได้รับผลประโยชน์จากการเปลี่ยนแปลงของอัตราแลกเปลี่ยนเงิน ให้ถือว่าผู้นั้นกระทำความผิดฐานกู้ยืมเงินที่เป็นการฉ้อโกงประชาชนด้วย"
4) พ.ร.บ. แชร์ – พระราชบัญญัติการเล่นแชร์ พ.ศ. 2534 มาตรา 6 ห้ามมิให้บุคคลธรรมดาเป็นนายวงแชร์หรือจัดให้มีการเล่นแชร์ที่มีลักษณะอย่างหนึ่งอย่างใดดังต่อไปนี้ (ดี.พี. ลอว์ แอนด์ เซอร์วิส จำกัด, 2562)
(1) เป็นนายวงแชร์หรือจัดให้มีการเล่นแชร์มีจำนวนวงแชร์รวมกันมากกว่าสามวง
(2) มีจำนวนสมาชิกวงแชร์รวมกันทุกวงมากกว่าสามสิบคน

(3) มีทุนกองกลางต่อหนึ่งงวดรวมกันทุกวงเป็นมูลค่ามากกว่าจำนวนที่กำหนดไว้ในกฎกระทรวง

(4) นายวงแชร์หรือผู้จัดให้มีการเล่นแชร์นั้นได้รับประโยชน์ตอบแทนอย่างอื่นนอกจากสิทธิที่จะได้รับทุนกองกลาง ในการเข้าร่วมเล่นแชร์ในงวดหนึ่งงวดใดได้โดยไม่ต้องเสียดอกเบี้ย

เพื่อประโยชน์แห่งมาตรานี้ ให้ถือว่าผู้ที่สัญญาว่าจะใช้เงินหรือทรัพย์สินอื่นใดแทนนายวงแชร์หรือผู้จัดให้มีการเล่นแชร์ เป็นนายวงแชร์หรือผู้จัดให้มีการเล่นแชร์ด้วย

มาตรา 17 ผู้ใดฝ่าฝืนมาตรา 6 ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

5) พ.ร.บ. ลิขสิทธิ์ - พระราชบัญญัติลิขสิทธิ์ (ฉบับที่ 3) พ.ศ. 2558 มาตรา 31 ผู้ใดรู้อยู่แล้วหรือมีเหตุอันควรรู้ว่างานใดได้ทำขึ้นโดยละเมิดลิขสิทธิ์ของผู้อื่น กระทำอย่างใดอย่างหนึ่งแก่งานนั้นเพื่อหากำไร ให้ถือว่าผู้นั้นกระทำการละเมิดลิขสิทธิ์ ถ้าได้กระทำดังต่อไปนี้ (Wichianlaw, 2561)

(1) ขาย มีไว้เพื่อขาย เสนอขาย ให้เช่า เสนอให้เช่า ให้เช่าซื้อ หรือเสนอให้เช่าซื้อ

(2) เผยแพร่ต่อสาธารณชน

(3) แจกจ่ายในลักษณะที่อาจก่อให้เกิดความเสียหายแก่เจ้าของลิขสิทธิ์

(4) นำหรือสั่งเข้ามาในราชอาณาจักร

มาตรา 70 ผู้ใดกระทำการละเมิดลิขสิทธิ์ตามมาตรา 31 ต้องระวางโทษปรับตั้งแต่หนึ่งหมื่นบาทถึงหนึ่งแสนบาท

ถ้าการกระทำความผิดตามวรรคหนึ่งเป็นการกระทำเพื่อการค้า ผู้กระทำต้องระวางโทษจำคุกตั้งแต่สามเดือนถึงสองปี หรือปรับตั้งแต่ห้าหมื่นบาทถึงสี่แสนบาทหรือทั้งจำทั้งปรับ

2.1.1.2 คดีมโนสาเร่

คดีมโนสาเร่ หมายถึง คดีที่โจทก์ฟ้องเรียกเอาทรัพย์สินจำนวนไม่มาก หรือคดีฟ้องขับไล่ที่มีค่าเช่าหรืออาจให้เช่าได้ ราคาเล็กน้อย ถือเป็นคดีที่ไม่ยุ่งยาก ไม่ซับซ้อน การพิจารณาคดีจะเป็นไปโดยรวบรัดเพื่อความสะดวก รวดเร็ว ประหยัดและยุติธรรม

จากหลักกฎหมาย มาตรา 189 แห่งประมวลกฎหมายวิธีพิจารณาความแพ่ง บัญญัติไว้ว่า คดีมโนสาเร่ คือ (สำนักงานกฎหมายทนายความกอบเกียรติ, 2562)

(1) คดีที่มีคำขอให้ปลดเปลื้องทุกข์อันอาจคำนวณเป็นราคาเงินได้ไม่เกินสามแสนบาท

(2) คดีฟ้องขับไล่บุคคลใด ๆ ออกจากอสังหาริมทรัพย์อันมีค่าเช่าหรืออาจให้เช่าได้ในขณะยื่นคำฟ้องไม่เกินเดือนละสามหมื่นบาท

การพิจารณาคดีมโนสาเร่ ต่างจากคดีแพ่งสามัญ หลายประการ เช่น โจทก์สามารถยื่นฟ้องเป็นหนังสือหรือแถลงด้วยวาจาก็ได้ และเสียค่าขึ้นศาลมากที่สุดเพียงหนึ่งพันบาท เมื่อโจทก์ฟ้องแล้วศาลจะกำหนดวันนัดพิจารณาเพื่อให้จำเลยมาศาลเพื่อการไกล่เกลี่ย ให้การ และสืบพยานในวันเดียวกัน โดยจำเลยไม่ต้องยื่นคำให้การภายใน 15 วันอย่างคดีแพ่งสามัญ

สำหรับการสืบพยาน ตามมาตรา 193 จัตวา บัญญัติว่า ให้ศาลกำหนดวันนัดพิจารณาโดยเร็วและออกหมายเรียกไปยังจำเลย ในหมายนั้นให้จดแจ้งประเด็นแห่งคดีและจำนวนทุนทรัพย์หรือราคาที่เรียกร้อง และข้อความว่าให้จำเลยมาศาลเพื่อการไกล่เกลี่ย ให้การ และสืบพยานในวันเดียวกัน

และให้ศาลสั่งให้โจทก์มาศาลในวันนัดพิจารณานั้นด้วย (สำนักงานกฎหมายทนายความกอบเกียรติ, 2562)

2.1.2 ประเภทของการฉ้อโกง

ในปัจจุบันสภาพสังคมมีความสลับซับซ้อนมาก อาชญากรรมประเภทฉ้อโกงมีความสลับซับซ้อนมากขึ้นตามไปด้วย ถึงแม้ว่าการฉ้อโกงในบางรูปแบบอาจจะมีลักษณะคล้ายคลึงกันกับที่เคยปรากฏในอดีตเมื่อหลายสิบปีก่อน แต่ก็มีการสร้างเครือข่ายองค์กรอาชญากรรม หรือนำเทคโนโลยีสารสนเทศมาใช้ในการฉ้อโกง ซึ่งจะทำให้มีชาวบ้านที่ไม่รู้เท่าทัน ก็จะหลงเชื่อและตกเป็นผู้ถูกหลอกมากขึ้น ก่อความเสียหายอย่างมากทั้งแก่ตัวบุคคลชุมชนและประเทศชาติ

สำหรับรูปแบบการฉ้อโกงในยุคปัจจุบันสามารถประมวลได้ 8 รูปแบบ ดังต่อไปนี้

1) การฉ้อโกงโดยหลอกลวงให้ร่วมลงทุนในลักษณะแชร์ลูกโซ่
2) การฉ้อโกงโดยหลอกลวงให้ทำรายการที่ตู้เอทีเอ็ม
3) การฉ้อโกงโดยส่งอีเมลมาทำความรู้จักคุ้นเคยและหลอกลวงให้โอนเงินเข้าบัญชี
4) การฉ้อโกงโดยปลอมตัวและปลอมที่อยู่อีเมลมาหลอกลวงให้โอนเงินผิดบัญชี
5) การฉ้อโกงโดยอ้างการรักษาพยาบาลมาหลอกลวงเอาเงิน
6) การฉ้อโกงโดยอ้างการเรี่ยไรเงินไปช่วยเหลือทางราชการหรือผู้ด้อยโอกาส
7) การฉ้อโกงโดยใช้ศาสนาเป็นเครื่องมือในการหลอกลวง
8) การฉ้อโกงโดยอ้างว่าเป็นเจ้าหน้าที่ในกระบวนการยุติธรรมและหลอกลวงเอาเงิน

และสำหรับกรณีของการฉ้อโกง ที่เป็นการฉ้อโกงออนไลน์ ผ่านทาง Facebook, Line, Instagram เป็นต้น สามารถแบ่งออกเป็น 5 รูปแบบ ดังนี้

1) การหลอกลวงขายสินค้าในรูปแบบต่าง ๆ โดยมีเจตนาทุจริตที่จะไม่ขายสินค้าจริงๆ หรือไม่มีสินค้าอยู่จริง โดยนำภาพสินค้าของคนอื่นมาลงโพสต์เพื่อขายให้เหยื่อหลงเชื่อ
2) การหลอกลวงขายสินค้าที่ลงโพสต์ไว้ว่าเป็นของแท้แต่ส่งของเลียนแบบหรือของปลอม หรือของคนละประเภทกับที่โพสต์ขาย
3) การหลอกลวงว่าจะให้กู้ยืมเงินในอัตราดอกเบี้ยต่ำ โดยให้ผู้เสียหาย โอนเงินค่าธรรมเนียม หรือค่าดอกเบี้ยงวดแรก หรือค่ามัดจำ เป็นต้น
4) การหลอกลวงด้วยการตีสนิทเข้ามาจีบ (ส่วนใหญ่ใช้รูปโปรไฟล์ ชาวต่างชาติหน้าตาดีสวย เท่ห์) และหลอกว่าจะส่งของมาให้ จากนั้นจะมีผู้ร่วมขบวนการโทรมาติดต่อหลอกว่าเป็นพนักงานบริษัทขนส่งให้โอนค่าธรรมเนียมเพื่อดำเนินการนำพัสดุออกจากด่านศุลกากร โดยส่วนมากจะอ้างว่ามีเงินสดจำนวนมากอยู่ในพัสดุดังกล่าว
5) การหลอกลวงด้วยการแฮกข้อมูลสื่อสังคมออนไลน์ของผู้อื่น โดยที่เจ้าของข้อมูลไม่ได้อนุญาต และทำการหลอกลวงของยืมเงินจากผู้อื่นที่เกี่ยวข้องกับสื่อสังคมออนไลน์นั้น ๆ

2.1.3 ทฤษฎีป้องกันอาชญากรรม

การแก้ไขปัญหาอาชญากรรมที่จะทำให้บรรลุเป้าหมายหรือผลสำเร็จได้นั้น ตำรวจจะต้องรู้จักการกำหนดยุทธศาสตร์หรือกลยุทธ์ในการแก้ไขปัญหาให้ “ถูกจุดและตรงประเด็น” ซึ่งแนวทางการป้องกันอาชญากรรมเชิงรุก โดยใช้ทฤษฎีสามเหลี่ยมอาชญากรรม เพื่อเป็นแนวทางในการแก้ไขปัญหาอาชญากรรมในแต่ละพื้นที่ โดยเบื้องต้นตำรวจต้องมีข้อมูลที่จะใช้ในการวิเคราะห์สภาพปัญหาอาชญากรรมที่เกิดขึ้นในแต่ละพื้นที่ ข้อมูลนั้นอาจจะมาจากคดีที่เกิดขึ้นในพื้นที่ที่พนักงานสอบสวนได้รับ

คำร้องทุกข์ไว้แล้ว คดีที่เกิดขึ้นแต่ยังไม่ได้รับคำร้องทุกข์หรือข้อมูลข่าวสารที่ได้รับจากการร้องเรียนของประชาชน เป็นต้น เมื่อวิเคราะห์ข้อมูลดังกล่าวแล้ว จะทำให้ทราบถึงช่วงเวลา สถานที่ที่เกิดเหตุ พฤติกรรมของคนร้าย ตลอดจนสภาพปัญหาและสาเหตุของการเกิดอาชญากรรม อันจะนำไปใช้ประโยชน์ในการกำหนดกลยุทธ์การแก้ไขปัญหาอาชญากรรมต่อไป

ทฤษฎีสามเหลี่ยมอาชญากรรม (Crime Triangle Theory) ได้อธิบายถึงสาเหตุหรือองค์ประกอบของการเกิดอาชญากรรม ประกอบด้วยด้านต่าง ๆ ของสามเหลี่ยม 3 ด้าน ซึ่งประกอบด้วย

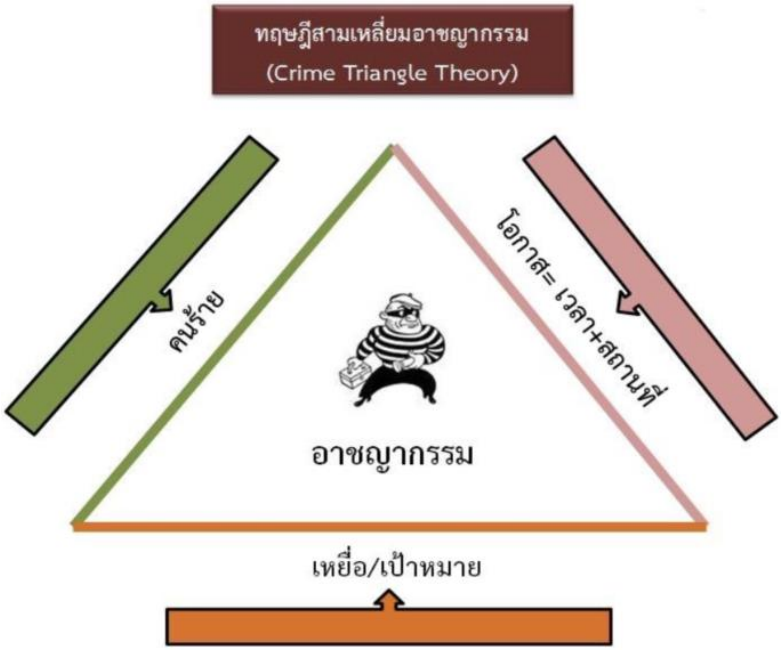
- ผู้กระทำผิด/คนร้าย หมายถึง ผู้ที่มีความต้องการจะก่อเหตุหรือลงมือกระทำความผิด
- เหยื่อ/เป้าหมาย หมายถึง บุคคล สถานที่ หรือวัตถุสิ่งของ ที่ผู้กระทำผิดหรือคนร้ายมุ่งหมายกระทำต่อเป้าหมายที่ต้องการ
- โอกาส หมายถึง ช่วงเวลา และสถานที่ที่เหมาะสมที่ผู้กระผิดหรือคนร้าย สามารถจะลงมือกระทำความผิดหรือก่ออาชญากรรม

เมื่อเหตุการณ์หรือสถานการณ์ครบองค์ประกอบทั้ง 3 ด้าน ดังกล่าวข้างต้น จะทำให้เกิดอาชญากรรมขึ้น ทฤษฎีดังกล่าวได้เสนอแนวคิดในการแก้ไขปัญหาอาชญากรรม หรือการป้องกันไม่ให้เกิดอาชญากรรม โดยต้องพยายามทำอย่างไรก็ตามที่จะให้องค์ประกอบของสามเหลี่ยมอาชญากรรมด้านใดด้านหนึ่งหายไป ก็จะทำให้อาชญากรรมไม่เกิดขึ้น แสดงได้ดังรูปที่ 2-1 (สุรพงษ์ ชัยจันทร์, 2561)

วิธีในการดำเนินการเพื่อทำให้องค์ประกอบการเกิดอาชญากรรม ด้านใดด้านหนึ่งหายไป มีดังนี้

2.1.3.1 ด้านผู้กระทำผิดหรือคนร้าย

ต้องพยายามลดหรือควบคุมจำนวนผู้กระทำความผิดหรือคนร้ายในพื้นที่ที่รับผิดชอบ โดยมุ่งเน้นใช้ทฤษฎีบังคับใช้กฎหมาย เช่น การเฝ้าระวังบุคคลพ้นโทษที่เข้ามาอยู่ในพื้นที่ การกำหนดมาตรการควบคุมแหล่งอบายมุขหรือสถานบริการที่จะเป็นแหล่งเพาะอาชญากรรม การระดมกวาดล้างอาชญากรรมอย่างสม่ำเสมอ การจับกุมผู้กระทำความผิดตามหมายจับ การสืบสวนหาข่าวเกี่ยวกับแหล่งซ่องสุมของผู้กระทำความผิดหรือคนร้าย มาตรการตีวงสุรา การปิดล้อมตรวจค้น การไประงับเหตุอย่างรวดเร็วของสายตรวจ เพื่อให้สามารถจับกุมผู้กระทำความผิดหรือคนร้ายได้อย่างทันท่วงที รวมทั้งการประสานงานกับหน่วยงานที่เกี่ยวข้อง เพื่อร่วมกันแก้ไขปัญหาอาชญากรรม ยาเสพติดให้โทษ และปัญหาการว่างงาน เป็นต้น



รูปที่ 2-1 ทฤษฎีสามเหลี่ยมอาชญากรรม

2.1.3.2 ด้านเหยื่อ/เป้าหมาย

ผู้เสียหายหรือเหยื่อ หรือประชาชนทั่วไปต้องรู้จักการป้องกันตนเอง ครอบครัว และชุมชนหรือสังคม ตำรวจจะต้องยื่นมือเข้าไปช่วยเหลือประชาชนในพื้นที่ โดยมีการประชาสัมพันธ์ให้ความรู้ข้อมูลข่าวสารที่เป็นประโยชน์ต่อประชาชนในการป้องกันอาชญากรรม หรือไม่ให้ตกเป็นเหยื่ออาชญากรรม เช่น การแต่งตัว การใส่เครื่องประดับหรือของที่มีค่า การหลอกลวงของคนร้ายในลักษณะต่าง ๆ โดยอาจจะจัดเป็นโครงการตำรวจเตือนภัย โครงการตรวจเยี่ยมประชาชน เป็นต้น

2.1.3.3 ด้านโอกาส

โอกาสที่ผู้กระทำความผิดหรือคนร้ายจะลงมือก่ออาชญากรรมนั้นจะต้องอาศัย เวลาและสถานที่ที่เหมาะสมในการก่อเหตุ ตำรวจต้องพยายามหาวิธีการเพื่อที่จะตัดช่องโอกาสของคนร้ายดังกล่าว โดยแยกออกเป็น

- เวลา ต้องพยายามตัดช่องโอกาสในเรื่องเวลาที่จะเกิดเหตุ โดยมุ่งเน้นการปรากฏตัวของเจ้าหน้าที่ตำรวจสายตรวจ การตั้งจุดตรวจค้น เป็นต้น
- สถานที่ สำหรับเรื่องการตัดช่องโอกาสในเรื่องสถานที่นั้น สามารถกระทำได้หลายวิธี และมีทฤษฎีที่เกี่ยวข้องมากมาย เช่น ทฤษฎีการควบคุมอาชญากรรมจากสภาพแวดล้อม เป็นวิธีการปรับสภาพแวดล้อมและใช้ประโยชน์สภาพแวดล้อม ในการลดโอกาสการก่ออาชญากรรม การจัดการพื้นที่ให้ปลอดภัย การเพิ่มประสิทธิภาพเครื่องมือเครื่องใช้ทางเทคโนโลยีใหม่ ๆ

2.2 แนวคิดการติดตาม สืบสวนสอบสวน จับกุมผู้ต้องหา

2.2.1 หลักการสืบสวน และความรับผิดชอบของพนักงานสืบสวน

2.2.1.1 ความหมายของการสืบสวน

ประมวลกฎหมายพิจารณาคดีความอาญา มาตรา 2(10) ได้ให้ความหมายการสืบสวน หมายถึง การรวบรวมพยานหลักฐาน ซึ่งพนักงานฝ่ายปกครองหรือตำรวจ ซึ่งได้ปฏิบัติตามอำนาจและหน้าที่เพื่อรักษาความสงบเรียบร้อยของประชาชน และเพื่อทราบรายละเอียดแห่งความผิด

2.2.1.2 ผู้มีอำนาจในการสืบสวน

ประมวลกฎหมายวิธีพิจารณาคดีความอาญา มาตรา 17 กำหนดไว้ว่า พนักงานฝ่ายปกครองหรือตำรวจ มีอำนาจในการสืบสวนคดีอาญาได้

ประมวลกฎหมายวิธีพิจารณาคดีความอาญามาตรา 2(16) กำหนดไว้ว่าพนักงานฝ่ายปกครองหรือตำรวจ หมายถึง เจ้าพนักงานซึ่งกฎหมายให้มีอำนาจและหน้าที่รักษาความสงบเรียบร้อยของประชาชน ให้รวมถึงพัศดี เจ้าพนักงานสรรพสามิต กรมศุลกากร กรมเจ้าท่า พนักงานตรวจคนเข้าเมือง และเจ้าพนักงานอื่นๆ ในเมื่อทำการอันเกี่ยวกับการจับกุมปราบปรามผู้กระทำผิดกฎหมาย ซึ่งตนมีหน้าที่ต้องจับกุมหรือปราบปราม

2.2.1.3 หลักเกณฑ์ในการสืบสวน

การสืบสวนนั้น เป็นการดำเนินงานขั้นต้นของพนักงานฝ่ายปกครองหรือตำรวจ ซึ่งได้ปฏิบัติตามอำนาจที่เพื่อจะบรรลุวัตถุประสงค์ในการรักษาความสงบเรียบร้อยของประชาชนและทราบรายละเอียดแห่งการกระทำผิด สำหรับหลักเกณฑ์การดำเนินการสืบสวนคดีอาญานั้น มิได้กาหนดไว้ในประมวลกฎหมายวิธีพิจารณาความอาญา เหมือนกับกรณีการสอบสวนและพิจารณาในศาล เนื่องจาก การสืบสวนเป็นการปฏิบัติเพื่อให้ได้มาซึ่งข้อเท็จจริงขั้นต้นของพนักงานฝ่ายปกครองหรือตำรวจ โดยมีเทคนิคในการสืบสวนหลายรูปแบบ จึงย่อมไม่อาจที่จะกาหนดหลักเกณฑ์วิธีการปฏิบัติโดยบัญญัติเป็นข้อผูกมัดตายตัวได้

การสืบสวน สามารถแบ่งออกได้เป็น 2 แบบ ดังนี้

1) การสืบสวนก่อนเกิดเหตุ (Preventive Investigation) คือการแสวงหาข้อเท็จจริงและข้อมูลเพื่อประโยชน์ในการป้องกันการกระทำผิด หรือหาทางระงับมิให้มีอาชญากรรมเกิดขึ้น โดยมีจุดมุ่งหมายคือการตัดโอกาสและช่องทางในการกระทำผิดของอาชญากร จึงเป็นการสืบสวนเหตุการณ์ทั่ว ๆ ไป ในขณะที่ยังไม่มีการกระทำผิดเกิดขึ้น เพื่อให้ทราบรายละเอียดของสภาพอันแท้จริงในพื้นที่ความรับผิดชอบของนักสืบ เช่น ความประพฤติของประชาชน รายชื่อและพฤติการณ์ของบรรดากลุ่มประกอบกิจการทุจริตผิดกฎหมาย พวกนักเลงอันธพาล และอาชญากรในท้องถิ่นทุกประเภท ตลอดจนศึกษาถึงลักษณะภูมิประเทศ ถนน ตรอก ซอย แม่น้ำ สถานที่สำคัญ หรืออาจรียกได้ว่า เป็นการสืบสวนหาข่าว
2) การสืบสวนหลังเกิดเหตุ (Primary Investigation) คือกระบวนการแสวงหาข้อเท็จจริงและหลักฐานเพื่อที่จะทราบรายละเอียดแห่งความผิด ในกรณีที่มีความผิดเกิดขึ้นแล้ว ลักษณะการสืบสวนหลังเกิดเหตุนั้น โดยจะเป็นการสืบสวนเมื่อมีการกระทำผิดเกิดขึ้นแล้วโดยมีวัตถุประสงค์ 3 ประการคือ

2.1 ในกรณีจับผู้กระทำผิดได้ การสืบสวนในลักษณะนี้เจ้าหน้าที่ตำรวจจะต้องสืบสวนหาพยานหลักฐาน ข้อเท็จจริง พยานบุคคล พยานเอกสาร พยานวัตถุ เพื่อที่จะนำมา พิสูจน์ความผิดของผู้ต้องหาในชั้นสอบสวน ตลอดจนชั้นพิจารณาคดีของศาล เพื่อที่จะสามารถลงโทษผู้กระทำผิดได้

2.2 ในกรณีรู้ตัวผู้กระทำผิด แต่ยังจับตัวไม่ได้ การสืบสวนในลักษณะนี้ นอกจากจะเป็นการสืบสวนเพื่อแสวงหาข้อเท็จจริงเกี่ยวกบรายละเอียดแล้ว ยังจะต้องสืบสวนหาตัวผู้กระทำผิดต่อไปอีก

2.3 ในกรณีไม่รู้ตัวผู้กระทำผิดและยังไม่ทราบรายละเอียดแห่งความผิดการสืบสวนในลักษณะนี้จะต้องเป็นการสืบสวนหาข้อเท็จจริงและหาหลักฐานเพื่อให้ได้รายละเอียดวาใครเป็นผู้กระทำผิด ทำที่ไหน เมื่อไร อย่างไร และสาเหตุการกระทำความผิดนั้น

2.2.1.4 วิธีการสืบสวน

การสืบสวนเป็นเรื่องของการแสวงหาข้อเท็จจริงและหลักฐานเพื่อที่จะรักษาความสงบเรียบร้อยของประชาชนและเพื่อที่จะทราบรายละเอียดแห่งการกระทำผิด ดังนั้นเพื่อให้ได้ข้อเท็จจริงและหลักฐานดังกล่าว มีวิธีการสืบสวนดังนี้

2.2.1.4.1 การสืบสวนในลักษณะสายลับ

กรรมวิธีทางการสืบสวนวิธีหนึ่งโดยใช้การปลอมแปลงและอ้างข้อแก้ตัวต่างๆ เพื่อทำให้บุคคลที่คาดว่าเป็นผู้ต้องสงสัยว่าเป็นอาชญากรเกิดความไว้วางใจ ชอบมั่วสุม อย่างไรก็ตาม

วิธีการสืบสวนในลักษณะสายลับนั้น เจ้าหน้าที่ฝ่ายสืบสวนจะต้องใช้ดุลยพินิจในการที่จะเชื่อถือข่าวสารจากสายลับเป็นกรณีพิเศษ เนื่องจากบุคคลที่เข้ามาเป็นสายลับนั้น จะต้องมีเหตุจูงใจให้เข้ามาเป็นสายลับ ดังนั้น ข่าวสารที่ได้มาจากสายลับอาจจะเป็นได้ทั้งข้อเท็จจริงหรือเท็จก็ได้ จึงสมควรที่เจ้าหน้าที่ต้องกรองข่าวเสียก่อน

2.2.1.4.2 การสืบสวนในลักษณะข่าวกรองตำรวจ

การสืบสวนในลักษณะข่าวกรองตำรวจนั้น เป็นวิธีการสืบสวนของเจ้าหน้าที่ตำรวจอีกวิธหนึ่ง ที่ดำเนินเพื่อแสวงหาข้อเท็จจริงและพยานหลักฐานจากการผลิตข่าวด้านอาชญากรรม โดยมี 5 วิธีคือ

1) การรวบรวม เป็นการรวบรวมข่าวสารจากแหล่งต่างๆ เช่น โรงพยาบาล สถานีตำรวจ เรือนจำ วิทยุ โทรทัศน์
2) การประเมินค่า เป็นการนำข่าวสารที่ได้จากแหล่งข่าวต่างๆ มาทำการประเมินว่าข่าวสารนั้นเชื่อถือได้หรือไม่
3) การวิเคราะห์ เป็นการนำข่าวที่ได้จากการประเมินค่าแล้วมาพิจารณาในรายละเอียดของข่าวที่เกี่ยวข้อง เพื่อหาข้อเท็จจริง
4) การสนธิกรรม เป็นการนำข่าวสารต่างๆ ที่ได้ผานกรรมวิธีข้างต้นมาประกอบกัน เพื่อกำหนดภาพของข่าวกรอง
5) การตีความ เป็นการดำเนิน 3 ขั้นคือการวิเคราะห์ การสนธิกรรม การอนุมานเพื่อหาความหมายที่แฝงอยู่รวมทั้งข้อยุติด้วย

2.2.1.4.3 การสืบสวนในลักษณะการเฝ้าตรวจ

การสืบสวนในลักษณะการออกตรวจนั้นหมายถึง การที่เจ้าหน้าที่ตำรวจสืบสวนออกตรวจพื้นที่โดยมีวิธีการคือการเฝ้าสังเกตบุคคล สิ่งของ หรือสถานที่ต่างๆ โดยปกปิดสถานะของตนเอง เช่น การสืบสวนหาพยานหลักฐานที่จะใช้ยืนยันผู้ต้องสงสัย, หาแหล่งที่อยู่ของคนร้าย หรือการค้นหาเบาะแสความเคลื่อนไหวของคนร้ายอันนำไปสู่การจับกุมผู้ต้องหา โดยทั่วไปหลักการสืบสวนในลักษณะออกตรวจมีอยู่ 3 วิธีคือ

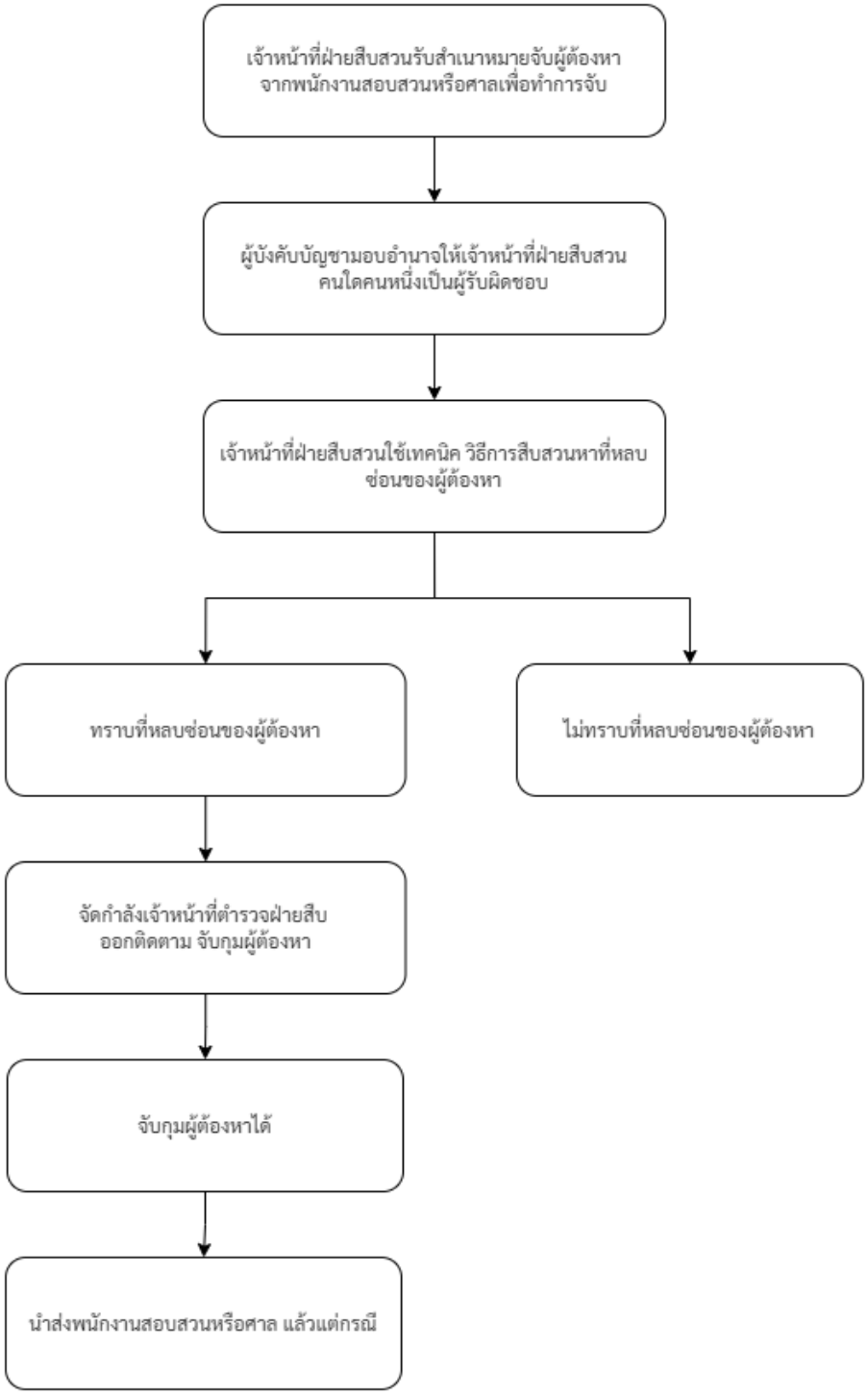
1) การออกตรวจแบบเคลื่อน เช่น การเดินเท้าสะกดรอย และการใช้ยานพาหนะ
2) การออกตรวจชนิดประจำที่ ได้แก่ การเฝ้าตรวจเคหะสถาน อาคารพาณิชย์ หรือสถานที่ต่างๆ โดยใช้รูปแบบสังเกตการณ์
3) การเฝ้าตรวจโดยใช้เครื่องมืออิเล็กทรอนิกส์ เป็นวิธีการสืบสวนโดยใช้เทคโนโลยีสมัยใหม่เข้ามาช่วยเหลือการปฏิบัติงานด้านสืบสวน เช่น การใช้เครื่องดักฟัง หรือกล้องโทรทัศน์วงจรปิด เป็นต้น

2.2.1.5 การบันทึกการสืบสวน

การบันทึกการสืบสวนคือหนังสือที่พนักงานฝ่ายปกครองหรือตำรวจจดไว้เป็นหลักฐานในการสืบสวน เป็นการจดข้อความเรื่องราว อันเป็นพยานหลักฐานต่างๆ ที่จะยืนยันหรือค้นคว้าหาข้อมูลข้อเท็จจริงแห่งคดี เช่น การตรวจสถานที่เกิดเหตุ บันทึกติดตามคนร้าย บันทึกการตรวจยึด เป็นต้น หากพนักงานสอบสวนเห็นว่าเป็นประโยชน์ต่อรูปคดีก็จะนำไปประกอบสำนวนกับการสอบสวนได้ ศาลจะรับฟังบันทึกการสอบสวนไว้เพื่อประกอบคดี บันทึกการสอบสวนมีความจำเป็นต่อเจ้าหน้าที่ฝ่ายสืบสวนเป็นอย่างมากในรายละเอียดของการบันทึกการสอบสวนนี้ อย่างน้อยเจ้าหน้าที่ตำรวจฝ่ายสืบสวนผู้รับผิดชอบจะต้องบันทึกให้ปรากฏข้อความดังต่อไปนี้

1) การสืบสวนได้ดำเนินมาเป็นระยะๆ เริ่มตั้งแต่ต้นจนจบการสืบสวน
2) วัน เวลา ตำบลที่เกิดเหตุ
3) ข้อมูล มูลเหตุ พฤติการณ์แห่งคดี จะต้องทำการสืบสวนให้ทราบถึงผู้กระทำผิด ผู้เสียหาย
4) พยานหลักฐานซึ่งได้แก่ พยานบุคคล พยานเอกสาร วัตถุพยาน
5) ให้ปรากฏข้อมูลถึงเหตุจูงใจ ที่ผู้สืบสวนสามารถได้พยานหลักฐานมา
6) เหตุผลแวดล้อมกรณีที่เกี่ยวเนื่องในเหตุการณ์นั้น ๆ โดยละเอียด
7) ถ้าผู้สืบสวนจับกุมผู้ต้องหาได้ ให้ลงวัน เวลา ตำบลที่จับ ตลอดจนท่าทีที่ส่อพิรุธของผู้ถูกจับด้วย
8) ถ้ายังไม่ได้ตัวผู้กระทำผิด แต่ผู้ที่สืบสวนไปมาจนทำให้เชื่อว่าใครเป็นผู้ต้องหา ให้สอบสวนที่อยู่อาศัยเวลานั้นและในอดีตด้วย ตำหนิรูปพรรณ ภรรยา บุตรเครือญาติที่เกี่ยวข้อง หรือแม้กระทั่งเพื่อนฝูง เพื่อเป็นประโยชน์ในการสืบสวนหาผู้กระทำผิด
9) เหตุผลอื่นๆ ที่เห็นวาเป็นธรรมกับคู่กรณี
10) ในกรณีจับผู้ต้องหาได้ รีบส่งผู้ต้องหาพร้อมบันทึกการสืบสวนที่ผู้บังคับบัญชาลงนามไปยังเจ้าพนักงานที่มีอำนาจสอบสวน บันทึกการสอบสวนที่ยังไม่ได้ผู้กระทำผิด หรือมีพฤติการณ์แสดงว่าจะก่อความไม่สงบขึ้นหรือเหตุการณ์อื่น ๆ จะในท้องที่ใด ต้อง

เสนอให้ผู้บังคับบัญชาทราบตามลำดับขั้นและถือเป็นหน้าที่ของผู้บังคับบัญชาจะต้องพิจารณา แล้วดำเนินการไปตามส่วนของแต่ละเหตุการณ์



รูปที่ 2-2 ขั้นตอนการสืบสวนจับกุมผู้ต้องหาตามหมายจับของเจ้าหน้าที่ฝ่ายสืบสวน

2.2.2 หลักการสอบสวน และความรับผิดชอบของพนักงานสอบสวน

2.2.2.1 ความหมายของการสอบสวน

ความหมายของการสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 2 (11) ได้กำหนดนิยามไววา “การสอบสวน หมายถึงการรวบรวมพยานหลักฐานและการดำเนินคดีการทั้งหลายอื่นตามบทบัญญัติแห่งประมวลกฎหมายนี้ ซึ่งพนักงานสอบสวนได้ทำไปเกี่ยวกับความผิดที่กล่าวมาเพื่อที่จะทราบขอเท็จจริงหรือพิสูจน์ความผิดเพื่อที่จะเอาตัวผู้กระทำความผิดมาฟองลงโทษ”

2.2.1.2 ผู้มีอำนาจในการสอบสวน

ตามประมวลกฎหมายวิธีพิจารณาความอาญา กำหนดให้ผู้เป็นพนักงานสอบสวนมี 2 ประเภท คือ

1) ในกรณีความผิดเกิดในราชอาณาจักร คือ เจ้าหน้าที่ตำรวจ หรือพนักงานฝ่ายปกครอง ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 18
2) ในกรณีความผิดเกิดนอกราชอาณาจักรตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 20 คือ
   (ก) อัยการสูงสุด หรือผู้รักษาการแทน หรือ
   (ข) พนักงานอัยการ กรณีอัยการสูงสุดเป็นผู้มอบหมายหน้าที่ให้เป็นผู้รับผิดชอบทำการสอบสวนแทน

2.2.1.3 หลักเกณฑ์ในการสอบสวน

สาระสำคัญของการสอบสวนมีดังนี้

1) เพื่อดำเนินการเกี่ยวกับความผิดที่กล่าวมา ได้แก่ การดำเนินตามขั้นตอนต่อไปนี้
   (1) การพิจารณาความผิด
   (2) การบันทึกปากคำผู้เสียหาย และพยาน
   (3) การบันทึกปากคำของผู้ตองหา
   (4) การรวบรวมพยานหลักฐานเป็นการดำเนินการสวนหนึ่งของพนักงานสอบสวนที่เกี่ยวข่องกับความผิดที่กล่าวหา
2) เพื่อที่จะทราบข่อเท็จจริงหรือพิสูจน์ความผิด การที่จะทราบขอเท็จจริงหรือเพื่อพิสูจน์ความผิด อาจกระทำได้โดยการพิจารณาจากพยานหลักฐานต่าง ๆ ที่พนักงานสอบสวนได้ดำเนินการตามที่ได้กล่าวตามข่อ1 ข้างตน ซึ่งได้แกพยานบุคคล พยานเอกสารวัตถุพยาน พยาน ผู้ชำนาญการและจากบันทึกคำใหการของผู้ต่องหา
3) เพื่อจะเอาตัวผู้กระทำความผิดมาฟองลงโทษ พนักงานสอบสวนมีวิธีการเอาตัวผู้กระทำความผิดมาลงโทษ มีดังนี้
   (1) โดยการออกหมายเรียกใหมาพบ พนักงานสอบสวน (ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 7 และ 133)

(2) โดยการออกหมายจับและดำเนินการออกประกาศจับตามระเบียบของราชการที่กำหนดไว (ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 6)

(3) โดยการรับตัวจากเจ้าพนักงาน หรือราษฎรผู้ทำการจับ (ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 89)

(4) โดยการเขาพบพนักงานสอบสวน (การมอบตัว)

(5) โดยพนักงานสอบสวนเป็นผู้จับและควบคุม ซึ่งในระหว่างสอบสวนปรากฏวา

(6) เป็นผู้กระทำความผิด (ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 136)

4) เพื่อใหพนักงานอัยการมีอำนาจฟองคดีตอศาล เพราะกฎหมายบัญญัติไววาห้ามมิให้พนักงานอัยการฟองคดีตอศาลโดยมิใหมีการสอบสวนในความผิดนั้นกอน

2.2.1.4 ขั้นตอนการสอบสวน

กระบวนการสืบสวนของเจ้าหน้าที่สอบสวน มีดังนี้

1) รับคำร้องทุกข์กล่าวโทษ - พนักงานสอบสวนเวร จะปฏิบัติหน้าที่เพื่อรับคำร้องทุกข์หรือคำกล่าวโทษ เมื่อดำเนินการแล้วจะลงบันทึกประจำวัน เป็นหลักฐานเอาไว้

2) แสวงหาและรวบรวมพยานหลักฐาน - ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 131 เพื่อที่ประสงค์ที่จะทราบข้อเท็จจริงและ พฤติการณ์ต่างๆ อันเดียวกันเรื่องที่ถูกกล่าวหา เพื่อจะรู้ตัวผู้กระทำความผิด และพิสูจน์ให้เห็นความผิดหรือความบริสุทธิ์ของผู้ต้องหา

3) พิจารณาพยานหลักฐานพร้อมปรับบทกฎหมาย - นำพยานหลักฐานที่ได้มาเพื่อพิจารณาการกระทำอันเป็นองค์ประกอบความผิดตามที่กฎหมายบัญญัติ ว่าเชื่อได้มาผู้ต้องหากระทำความผิดหรือไม่ จากนั้นได้จะเสนอสำนวนให้หัวหน้าพนักงานสอบสวนพิจารณา

4) ส่งสำนวนให้พนักงานอัยการ - ประมาลกฎหมายวิธีพิจารณาความอาญา มาตรา 140-144 พนักงานสอบสวนจะต้องทำความเห็นหลังจากรวบรวมหลักฐานแล้ว ว่า เห็นควรอย่างไร "เห็นควรสั่งฟ้อง" "เห็นควรสั่งไม่ฟ้อง" ในคดีที่ไม่ทราบตัวผู้กระทำความผิด ให้มีความเห็น "เห็นควรงดการสอบสวน"

2.2.1.5 การบันทึกการสอบสวน

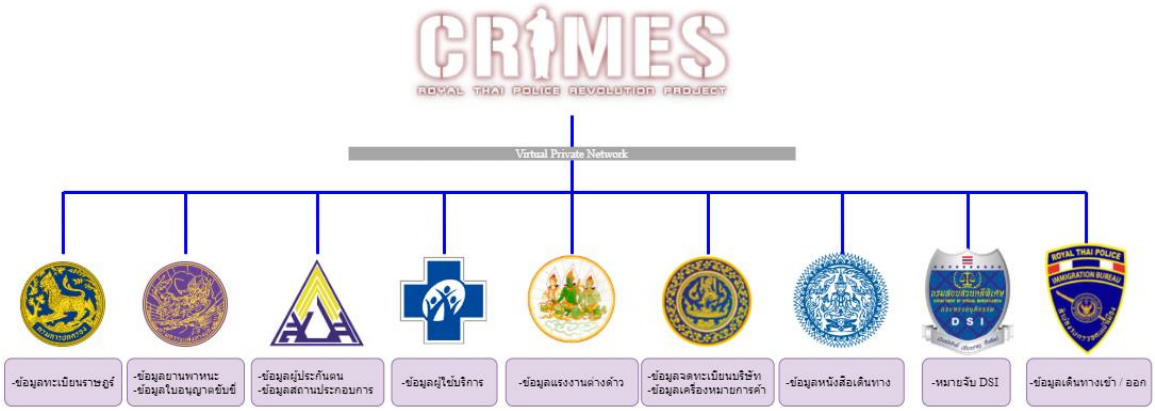
2.2.3 ระบบสารสนเทศข้อมูลอาชญากรรมสำนักงานตำรวจแห่งชาติ (CRIMES)

สำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานตำรวจแห่งชาติ ร่วมกับ บริษัทสงขลาฟินิชชิ่ง จำกัด พัฒนาระบบสารสนเทศข้อมูลอาชญากรรมสำนักงานตำรวจแห่งชาติ (CRIMES : Criminal Record and Information Management Enterprise Systems) เพื่อเพิ่มประสิทธิภาพให้กับสถานีตำรวจทั่วประเทศ และหน่วยงานตำรวจอื่นที่มีอำนาจหน้าที่สืบสวนสอบสวนคดีอาญา

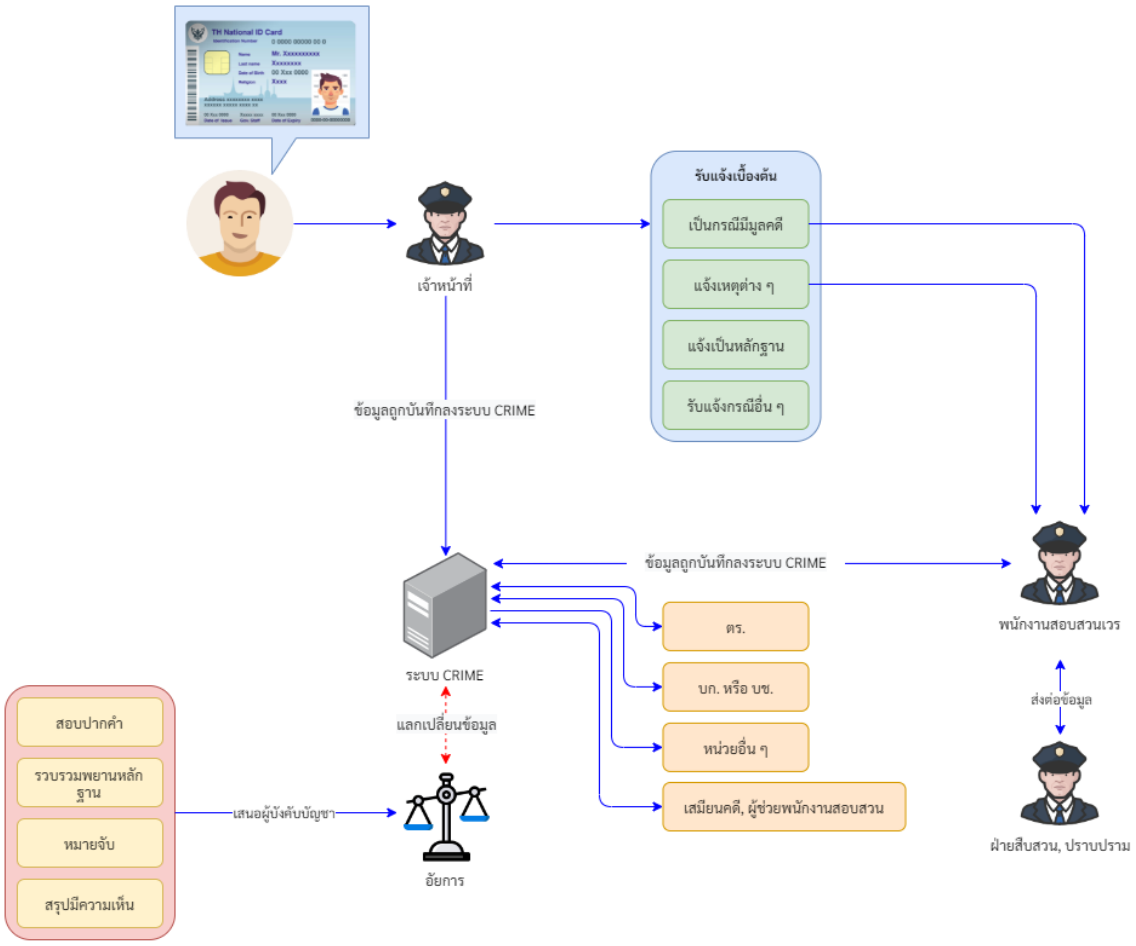
ระบบ CRIMES เป็นแหล่งรวบรวมข้อมูล ทั้งในด้านงานสอบสวน งานป้องกันปราบปราม งานจราจร รวมไปทั้งเป็นจุดศูนย์กลางสู่การเชื่อมต่อไปยังฐานข้อมูลของหน่วยงานอื่น ทั้งในส่วนของสำนักงานตำรวจแห่งชาติเอง หรือ หน่วยงานภายนอก เป็นเครื่องมือช่วยในการสืบสวน อำนวยความยุติธรรม ดำรงความถูกต้องของข้อมูล อำนวยความสะดวกให้กับเจ้าหน้าที่ผู้ปฏิบัติงานโดยเฉพาะงานระดับสถานีตำรวจ ลดขั้นตอนการบันทึกข้อมูลสนับสนุนงานต่าง ๆ ช่วยให้ประชาชนที่มาติดต่อได้รับการอำนวยความสะดวกและความยุติธรรมได้อย่างโปร่งใสและรวดเร็ว

สำหรับการทำงานของระบบ CRIMES เมื่อประชาชนมาแจ้งความร้องทุกข์ที่สถานีตำรวจ เจ้าหน้าที่ตำรวจเวรประชาสัมพันธ์ จะสอบถามและบันทึกข้อมูลเบื้องต้นในระบบคอมพิวเตอร์ เพื่อคัดกรองเรื่อง และแนะนำให้ผู้มาแจ้งความร้องทุกข์ ไปพบพนักงานสอบสวน ข้อมูลเบื้องต้นจะถูกส่งผ่านระบบคอมพิวเตอร์ ไปยังพนักงานสอบสวนเพื่อสืบค้นข้อมูล และบันทึกข้อมูลในชั้นการพิจารณาของพนักงานสอบสวน และข้อมูลจะถูกส่งผ่านระบบต่อไปยังฝ่ายสืบสวนป้องกันปราบปราม ซึ่งจะมีการเชื่อมโยงระบบกับหน่วยงานอื่นๆ ทั้งภายในและภายนอก เพื่อสนับสนุนการทำงานของตำรวจ ยกตัวอย่าง เช่น การเชื่อมต่อขอข้อมูลบุคคลจากทะเบียนราษฎร์ ทะเบียนประวัติอาชญากร ข้อมูลประกันสังคม และข้อมูลอื่นๆ เช่น ข้อมูลยานพาหนะ จากกรมการขนส่งฯ ข้อมูลทะเบียนปืนจากกรมการปกครอง เป็นต้น แสดงการเชื่อมโยงข้อมูลดังรูปที่ 2-3 (มนตรี สีทอง, 2564)

นอกจากนี้ CRIMES ยังถูกออกแบบไว้รองรับการทำงานของพนักงานสอบสวนด้วยระบบเทคโนโลยีสารสนเทศ และยังช่วยอำนวยความสะดวกให้พนักงานสอบสวน และผู้เกี่ยวข้องในการสืบค้นข้อมูลบริการ ข้อมูลอิเล็กทรอนิกส์ บริการแจ้งเตือนการทำงานของพนักงานสอบสวนและบริหารจัดการข้อมูลอย่างเป็นระบบ แสดงแผนภูมิการทำงานของระบบ CRIMES ดังรูปที่ 2-4



รูปที่ 2-3 การเชื่อมโยงกับหน่วยงานภายนอกของระบบ CRIMES



รูปที่ 2-4 ขั้นตอนการรับแจ้งความและบันทึกลงระบบ CRIMES

กลุ่มงานของระบบ CRIMES ประกอบไปด้วยระบบดังต่อไปนี้

1) ระบบบันทึกข้อมูล (Data Entry)
2) ระบบสืบค้นข้อมูล (Data Search)
3) ระบบบริการข้อมูลอิเล็กทรอนิกส์ (e-Data Service)
4) ระบบบริการแจ้งเตือน (Alarm & Alert Service)
5) ระบบบริหารจัดการข้อมูลและระบบ (Data & System Management)

สำหรับกลุ่มผู้ใช้งานระบบ CRIMES มีความหลากหลายโดยพยายามจัดให้สอดคล้องกับโครงสร้างการทำงานจริงของสถานีตำรวจและหน่วยบังคับบัญชา โดยกลุ่มผู้ใช้งานประกอบไปด้วย

1) เสมียนคดี
2) พนักงานสอบสวน
3) หัวหน้างานสอบสวน
4) หัวหน้าสถานี
5) หัวหน้าหน่วยงานสอบสวน
6) หัวหน้างานสืบสวนสอบสวนระดับจังหวัด

7) รองหัวหน้าหน่วยงานจังหวัด
8) รองหัวหน้าหน่วยงานจังหวัดที่มีอำนาจสอบสวน
9) หัวหน้าหน่วยงานจังหวัด
10) หัวหน้าหน่วยงานจังหวัดที่อำนาจอำนาจสอบสวน
11) รองหัวหน้าหน่วยงานระดับภาค
12) หัวหน้าหน่วยงานระดับภาค
13) ฝ่ายประมวลผลข้อมูล
14) ฝ่ายประวัติอาชญากร
15) เจ้าหน้าที่สืบค้นข้อมูล

ประโยชน์ของระบบ CRIMES นอกจากจะอำนวยความสะดวกและจัดการข้อมูลที่เกิดขึ้นตั้งแต่ประชาชนเข้ามาติดต่อจนกระทั่งการทำงานของเจ้าหน้าที่ในการติดตามความคืบหน้าของเรื่องนั้น ๆ โดยสามารถสรุปประโยชน์ของระบบ CRIMES ในด้านต่าง ๆ ได้ดังนี้

1) พัฒนาและเพิ่มประสิทธิภาพให้กับสถานีตำรวจ และหน่วยงานที่มีอำนาจหน้าที่สืบสวนสอบสวนคดีอาญา
2) ใช้ฐานข้อมูลกลางและทำงานแบบรวมศูนย์ ซึ่งง่ายต่อการบริหารจัดการข้อมูล
3) เชื่อมโยงข้อมูลระหว่างหน่วยงานที่มีอำนาจในการสืบสวน
4) สนับสนุนการแลกเปลี่ยนข้อมูลร่วมกับหน่วยงานต่าง ๆ ในกระบวนการยุติธรรม
5) สามารถนำข้อมูลด้านงานอาชญากรรม มาใช้วิเคราะห์ ประมวลผลเพื่อสนับสนุนงานด้านปฏิบัติการ ด้านบริหาร และด้านสถิติ
6) สามารถแบ่งปันการใช้ข้อมูลที่เกี่ยวข้องกับการสืบสวน สอบสวนเพื่อประโยชน์ร่วมกัน

2.3 ผลการศึกษา รวบรวมข้อมูลจากในประเทศและต่างประเทศ

2.3.1 ข่าวการถูกฉ้อโกงในประเทศไทย: กรณีตัวอย่าง

เมื่อเดือนตุลาคม 2562 มีผู้เสียหายเข้าแจ้งความ หลังถูกผู้ต้องหาที่รู้จักผ่านแอปพลิเคชันหนึ่งเข้ามาพูดคุยตีสนิท ก่อนถูกหลอกเอาทรัพย์สินไปจำนวนมาก โดยชายคนดังกล่าวอายุประมาณ 44 ปี รูปร่างสันทัดสูงประมาณ 160 เซนติเมตร เข้ามาพูดคุยผ่านทางแอปพลิเคชัน จนสนิทสนมจึงตกลงคบหาดูใจและเป็นแฟนกัน ชายคนดังกล่าวอ้างว่าเคยทำงานเป็นกุ๊กอยู่ต่างประเทศ ปัจจุบันเปิดร้านอาหารอยู่ที่จังหวัดนครราชสีมา อยากมีครอบครัว นอกจากนี้ ตนเห็นว่าชายคนดังกล่าวมีสวนเมล่อน จึงนำโฉนดบ้านที่ดินไปจำนองกับธนาคารเพื่อนำเงินมาลงทุนกัน โดยเมื่อได้เงินมาชายคนดังกล่าวพยายามออกอุบายขอยืมเงินไปจ่ายค่าทำธุรกิจต่าง ๆ นานา รวมแล้วประมาณ 45,000 บาท หลังจากนั้น ชายคนดังกล่าวเริ่มมีพิรุธบ่ายเบี่ยงไม่คืนเงิน และบอกว่าจะต้องรีบเข้าไปทำธุระที่กรุงเทพฯ โดยให้ไปพบที่สถานีรถไฟ จากนั้นก็ไม่สามารถติดต่อได้เลย (Sanook, 2562)

เมื่อเดือนมีนาคม 2563 น.ส.เอ (นามสมมุติ) ถูกผู้ต้องหาแอบอ้างเป็นแอดมินเพจจิตอาสาเพื่อเด็กและสังคมโทรศัพท์หลอก น.ส.เอ ให้ช่วยบริจาคเงินเพื่อไถ่ชีวิตโค กระบือ และบริจาคเงินช่วยเหลือผู้ป่วยโรคมะเร็งระยะสุดท้ายที่จังหวัดขอนแก่น น.ส.เอ หลงเชื่อจึงได้โอนเงินจำนวน 419,490 บาท ไปยังบัญชีเงินฝากของผู้ต้องหาทั้งสอง จากนั้น น.ส.เอ ได้ติดต่อไปยังแอดมินเพจจิตอาสาเพื่อเด็กและสังคมว่าได้โอนเงินบริจาคไปแล้ว แต่ทางแอดมินเพจดังกล่าวแจ้งว่าไม่ได้มีการรับบริจาคเงิน เพื่อช่วยเหลือผู้ป่วย

โรคมะเร็งระยะสุดท้ายที่จังหวัดขอนแก่น และไม่ได้รับบริจาคเงินเพื่อไถ่โคกระบือแต่อย่างใด (Sanook2, 2563)

เมื่อเดือนมีนาคม 2563 มีผู้เสียหายเข้าแจ้งความกับตำรวจ เนื่องจากโดนหลอกขายหน้ากากอนามัยผ่านเฟสบุ๊ก โดยผู้เสียเล่าว่า ได้รู้จักกับผู้ต้องหาผ่านทางเฟสบุ๊กมาร์เก็ต ประกาศขายหน้ากากอนามัย และได้ติดต่อพูดคุยซื้อขายหน้ากากอนามัยราคา 373,000 บาท จึงได้โอนเงินเข้าบัญชีธนาคารไทยพาณิชย์ ชื่อบัญชี น.ส.พรวิลัย ก่อนจะนัดรับของตอนเย็นวันที่ 12 มี.ค. แต่มีการเลื่อนนัด และถูกบ่ายเบี่ยงมาตลอด จนในที่สุดก็ไม่สามารถติดต่อผู้ต้องหาได้ (Mgronline, 2563)

เมื่อเดือนเมษายน 2563 ผู้ต้องหาได้เข้าไปสังเกตการณ์การประมูลนาฬิกายี่ห้อ Rolex รุ่น SUBMARINE ในเพจเฟสบุ๊ก ขายนาฬิกามือสอง หลังจากจบการประมูล ผู้ต้องหาได้หลอกลวงว่าเป็นเจ้าของทรัพย์และติดต่อไปยังผู้เสียหายเพื่อให้ผู้เสียหายโอนเงินให้ และในวันเดียวกันนี้เอง ผู้ต้องหาได้ก่อเหตุซ้ำ โดยเข้าไปสังเกตการณ์ในกลุ่มประมูลขายล้อแม็คและยางของรถยนต์กระบะ ยี่ห้อ อีซูซุ และแสร้งเป็นเจ้าของเพจและโทรศัพท์หาหลอกผู้เสียหายให้โอนเงินพร้อมส่งหลักฐานกลับไปยังเพจดังกล่าว (Sanook3, 2563)

เมื่อเดือนพฤษภาคม 2563 ผู้เสียหายเข้าแจ้งความ โดยเปิดเผยว่า พบ เฟสบุ๊ก ชื่อ "Beauty club คลับความงาม" โฆษณาขายอุปกรณ์ออกกำลังกาย แทรมโพลีน เครื่องเล่นสำหรับกระโดด เสริมพัฒนาการเด็ก จัดโปรโมชั่นพิเศษ จากราคา 3,999 บาท ลดเหลือ 999 บาท และจูงใจว่า หากซื้อวันนี้จะมีของแถมให้คือบ้านบอลและลูกบอล 100 ลูก มีจำนวนจำกัด ทำให้มีผู้สนใจรีบโอนเงินในเวลารวดเร็ว แต่พอถึงกำหนดกลับไม่มีใครได้รับสินค้า (Thaipbs, 2563)

เมื่อเดือนพฤษภาคม 2563 ได้มีการจับกุม 3 หนุ่มใต้แฮกเฟสบุ๊กหลอกยืมเงินเพื่อนเจ้าของบัญชี Fb หลงกลตกเป็นเหยื่อทั่วประเทศนับ 10,000 ราย รวมมูลค่าความเสียหายกว่า 14.7 ล้านบาท และจากการตรวจสอบประวัติพบว่ามีการเข้าแฮกเฟสบุ๊กของผู้อื่นจำนวน 289 ครั้ง จากการสอบสวนผู้ต้องหาที่ปลอมเฟสบุ๊กหลอกโอนเงินคือ นายเอกลักษณ์ โดยจะค้นหาเบอร์โทรศัพท์จาก google แล้วนำเบอร์โทรศัพท์ไปล็อกอินเข้าเฟสบุ๊ก ส่วนรหัสผ่านก็จะสุ่มเอาจากหมายเลขโทรศัพท์ เมื่อเข้าบัญชีเฟสบุ๊กของผู้เสียหายได้แล้วก็จะแชตไปขอยืมเงินจากเพื่อนสนิทในเฟสบุ๊กให้โอนเข้าบัญชีธนาคารที่จัดเตรียมไว้ จากนั้นก็จะถอนเงินสดออกจากบัญชีแล้วนำมาแบ่งกัน (Mgronline2, 2563)

เมื่อเดือนกรกฎาคม 2563 ผู้เสียหายได้เข้าแจ้งความ สภ.ถาวร อ.เฉลิมพระเกียรติ จังหวัดบุรีรัมย์ หลังถูกหลอกโอนเงินซื้อนมผงผ่านเฟสบุ๊ก แต่สุดท้ายกลับไม่ได้รับของและถูกเชิดเงินหนีไม่สามารถติดต่อได้ โดยเมื่อช่วงต้นเดือนกรกฎาคม ผู้เสียหาย เห็นผู้ใช้เฟสบุ๊กชื่อว่า “PAM PAM” ได้โพสต์ขายนมผงแบบจืด ซึ่งมีอยู่ประมาณ 11 กล่อง และเธอเห็นว่าผู้ที่โพสต์ขายเป็นแม่ลูกอ่อนเหมือนกัน จึงติดต่อไปสอบถามรายละเอียด และตกลงซื้อขายกัน โดยได้โอนเงินไปยังบัญชีของผู้ขาย แต่ผ่านไป 3 วันยังไม่ได้รับของ พอติดต่อไปยังเจ้าของเฟสบุ๊กก็ไม่สามารถติดต่อได้ และล่าสุดได้ปิดเฟสฯ หนีไป (Mgronline3, 2563)

เมื่อเดือนสิงหาคม 2563 หญิงวัย 62 ปี ถูกเร่งรัดทวงหนี้ค่าโทรศัพท์สุดท้ายกลายเป็นแก๊งค์มิจฉาชีพ มีคนอ้างเป็นทนายจับคนร้ายได้ฟ้องชนะได้เงินหลักล้านทำให้หลงเชื่อทยอยโอนเงินกว่า 4 แสนบาท ต้นเรื่องมาจาก ยาย ได้รับ SMS แจ้งมาให้ไปชำระหนี้ค่าโทรศัพท์ กว่า 20,000 บาท ก็ได้ไปชำระตามบัญชีที่แจ้งมา แต่ต่อมาทราบว่า SMS นั้นเป็นของแก๊งต้มตุ๋นหลอกให้โอนเงินไป จากนั้นไม่นานก็มีคนทักทางข้อความโทรศัพท์ อ้างตัวเป็นทนายบอกว่า จับแก๊งต้มตุ๋น แก๊งนี้ได้แล้ว แต่ยายต้องเสียเงินค่าทนาย เริ่มแรก 20,000 บาท ต่อมาบอกต้องขึ้นศาล ซึ่งในครั้งแรกเสียไป 30,000 บาท และเรียกร้องเพิ่ม

อีก 60,000 บาท ยายก็ยังเชื่อโอนเงินไปอีก 60,000 บาท ผ่านไปไม่นาน คนที่อ้างตัวเป็นทนายก็ติดต่อกลับมาแจ้งความคืบหน้าบอกว่า เรายังไม่ชนะคดี ต้องมีค่าดำเนินการอีก 90,000 บาท ยายก็ยังอยากสู้ต่อก็โอนไปอีก 90,000 บาท และยังมีการทยอยโอนไปเรื่อย ๆ รวมแล้วทั้งหมด 4 แสน 1 หมื่นบาท (PPTVOnline, 2563)

เมื่อเดือนตุลาคม 2563 ตำรวจได้เข้าจับกุมแก๊งชาวจีนที่ลักลอบทำงานในไทย 14 คน โดยผู้กระทำผิดเหล่านี้จะสมัครเล่นเกมด้วยการอ้างตัวว่า เป็นผู้เชี่ยวชาญและชักชวนผู้เล่นซื้อไอเทมเกมผ่านบัญชีชื่อตัวเอง โดยหลอกว่าจะสามารถซื้อได้ในราคาถูกกว่าปกติ รวมถึงการชักชวนพูดคุยเชิงสเน่ห์หา ทำให้ผู้เล่นจำนวนมากหลงเชื่อ โอนเงินให้ซื้อไอเทมเกมให้ และสูญเงินจำนวนมาก (Thaipbs, 2562)

เมื่อเดือนพฤศจิกายน 2563 มีการโพสท์เตือนภัยจากหญิงสาวรายหนึ่ง หลังมีมิจฉาชีพอ้างว่าตัวเองเป็นนักบินชาวอังกฤษ จะส่งของขวัญมาเซอร์ไพรส์ และให้จ่ายค่าส่งของให้ แต่ผู้เสียหายไหวตัวทันไปหาข้อมูลก็พบว่าเป็นมิจฉาชีพหลอกโอนเงินและชิ่งหนี โดยได้เปิดเผยว่า มีผู้ใช้เฟสบุ๊กชื่อว่า Sophia Antonio ทักเข้ามาหาตนว่า ผมชอบคุณ ตนเองก็ไม่ได้สนใจ และมิจฉาชีพก็ทักมาเรื่อย ๆ แล้วบอกว่าฉันชอบคุณนะ ผมอยากให้คุณมาอยู่ลอนดอนกับผม คุณรู้สึกยังไงกับผม ตนเองก็ตอบไปว่า โอเคฉันก็ชอบคุณนะ คุณหล่อ คุณดูดี อยากรู้จักกันให้มากกว่านี้ หลังจากนั้นไม่นานหญิงสาวรายนี้ก็จับพิรุธได้จากภาพถ่ายที่ได้รับ ทำให้รอดพ้นจากการตกเป็นเหยื่อของมิจฉาชีพรายนี้ (Sanook4, 2563)

เมื่อเดือนธันวาคม 2563 ตำรวจสามารถจับกุมผู้ต้องหาหลอกขายหน้ากากอนามัยได้ โดยผู้ต้องหารับสารภาพว่า ผู้ต้องหาโพสต์ขายหน้ากากอนามัยผ่านทางเฟสบุ๊ก ชื่อ Khun nune ในรายที่ถูกกว่าท้องตลาด โดยนำรูปจากอินเตอร์เน็ตมาโพสต์ขายเพื่อให้บุคคลทั่วไปหลงเชื่อและโอนเงินเข้าบัญชีเพื่อซื้อหน้ากากอนามัย แต่ไม่ได้มีสินค้าส่งให้กับลูกค้าตามที่ลงข้อมูลไว้ (Thairathonline, 2563)

เมื่อเดือนธันวาคม 2563 ผู้เสียหายได้รับการติดต่อจากผู้หญิงคนหนึ่ง โดยแสดงตัวว่าเธอเป็นเจ้าของโรงงานผลิตมูลไก่อัดเม็ดที่จังหวัดนครราชสีมา กำลังต้องการเปลือกมะพร้าวสับกว่า 3,700 กระสอบ และมูลไก่อัดเม็ดอีก 1,200 กระสอบ เพื่อนำไปผสมทำปุ๋ยอินทรีย์แจกจ่ายให้กับชาวบ้าน จึงอยากชักชวนผู้เสียหายให้มาร่วมทำธุรกิจด้วย ต่อมาผู้เสียหายก็ได้รับการติดต่อจากผู้หญิงอีกคนผ่านทางเพจเฟสบุ๊ก โดยหญิงคนดังกล่าวแจ้งว่า เพิ่งย้ายมาดำรงตำแหน่งเกษตรอำเภอ อยากให้ผู้เสียหายมารับงานเช่นเดียวกัน หญิงที่อ้างตัวเป็นเกษตรอำเภอ ระบุว่าทางอำเภอไม่สามารถออกบิลสั่งจ่ายในชื่อบุคคล 2 คนได้ จึงเสนอให้ ผู้เสียหายเป็นฝ่ายซื้อมูลไก่อัดเม็ดทั้งหมดจากโรงงานที่จังหวัดนครราชสีมา แล้วจึงนำเปลือกมะพร้าวสับ พร้อมมูลไก่อัดเม็ดทั้งหมด มาขายให้กับเกษตรอำเภออีกทอดหนึ่ง ผู้เสียหายจึงำโอนเงินมัดจำไปรวมทั้งหมด 70,000 บาท แต่แล้วก็ไม่สามารถติดต่อเจ้าของโรงงานมูลไก่อัดเม็ดได้อีกเลย รวมทั้งหญิงที่อ้างตัวเป็นเกษตรอำเภอเช่นเดียวกัน (Newsch7online, 2563)

เมื่อเดือนมีนาคม 2564 ผู้ต้องหาได้อ้างตัวเป็นผู้จัดการโรงแรมกักตัวทางเลือก หรือ Alternative state Quarantine หลอกให้ผู้เสียหายชาวแอฟริกาใต้ที่จะเดินทางเข้ามาในประเทศไทย โอนเงินค่าสถานที่กักตัว จนสูญเงินไปกว่า 35,000 บาท โดยผู้เสียหายเล่าว่า ได้ติดต่อจองโรงแรม ย่านสุขุมวิท เพื่อใช้เป็นสถานที่กักตัวผ่านทางเว็บไซต์ asq.wanderthai.com ต่อมามีคนร้ายอีเมลมาโดยอ้างว่าเป็นผู้จัดการโรงแรม และขอเก็บค่าธรรมเนียมเป็นเงิน 35,000 บาท ผู้เสียหายจึงโอนเงินเข้าบัญชีที่คนร้ายแจ้งมา กระทั่งมาทราบภายหลังว่าเป็นการแอบอ้าง ไม่ใช่การดำเนินการของทางโรงแรม และจากการตรวจสอบขยายผลพบว่า มีผู้เสียหายตกเป็นเหยื่อ 5-6 คน รวมความเสียหายกว่า 200,000 บาท (Newsch7online2, 2564)

เมื่อเดือนเมษายน 2564 ผู้เสียหายได้แชทผ่านเฟสบุ๊กกับผู้ต้องหาเพื่อติดต่อขายวัวสายพันธุ์บราซิล 2 ตัว ในราคา 37,000 บาท โดยอ้างว่าเป็นเจ้าของฟาร์มวัว หลังโอนเงินเรียบร้อย เจ้าของฟาร์มได้แจ้งว่า จะนำวัวไปส่งให้กับน้องสาวของผู้เสียหายที่อยู่ในพื้นที่ อ.โนนแดง แต่ผ่านไปหลายวัน ก็ยังไม่มีใครนำวัวมาส่ง จึงได้ทักแชตไปหาเจ้าของฟาร์มวัว แต่ก็ติดต่อไม่ได้ และพบว่าได้ทำการปิดเฟสบุ๊กหนีไปแล้ว (Newsch7online3, 2564)

เมื่อเดือนเมษายน 2564 ผู้ต้องหาได้ใช้เฟสบุ๊กเพื่อแฝงตัวไปในกลุ่มเพจขายของมือสอง ประเภทอะไหล่รถมือสอง, อุปกรณ์เครื่องมือช่างต่าง ๆ ก่อนจะหลอกขายสินค้าในราคาที่ถูกกว่าท้องตลาดให้กับลูกเพจหรือสมาชิกกลุ่ม โดยเมื่อผู้เสียหายโอนเงินให้แล้ว กลับไม่ส่งสินค้าในตามที่ตกลง และบล็อกเฟสบุ๊กติดต่อไม่ได้ โดยบัญชีธนาคารที่ผู้ต้องหาเคยใช้ในการรับเงินที่ได้จากการหลอกลวง มีจำนวนถึง 18 บัญชี ซึ่งส่วนใหญ่เป็นบัญชีธนาคารส่วนตัวของผู้ต้องหา และบัญชีธนาคารของบุคคลที่ผู้ต้องหารู้จัก ซึ่งผู้ต้องหาได้ขอยืมบัญชีธนาคารมาใช้ โดยให้ค่าตอบแทนในการยืมบัญชีธนาคารมาใช้ บัญชีธนาคารละ 500 - 1,000 บาท (KomChadLuek, 2564)

เมื่อเดือนเมษายน 2564 ผู้ต้องหาได้ใช้เฟสบุ๊กชื่อ "นายกัน คนเดิม" เข้าไปค้นหาชื่อนามสกุล หมายเลขโทรศัพท์ และหมายเลขบัญชีธนาคารพ่อค้าแม่ค้าขายของออนไลน์ จากนั้นได้ว่าจ้างให้ทำสำเนาบัตรประชาชนของพ่อค้าแม่ค้าสินค้าออนไลน์ แล้วทำรับรองสำเนาถูกต้อง เพื่อให้ออกซิมการ์ดโทรศัพท์ใหม่ที่ศูนย์บริการโทรศัพท์ หลังจากนั้นจะโทรศัพท์ไปที่ Call Center ของธนาคารเพื่อขอรีเซ็ทรหัสผ่านบัญชีธนาคารออนไลน์ของผู้เสียหาย แล้วทำการโอนเงินจากบัญชีผู้เสียหาย เข้ามายังบัญชีผู้ต้องหา โดยมีมูลค่าความเสียหายกว่า 1.5 ล้านบาท (Thairathonline2, 2564)

เมื่อเดือน เมษายน 2564 เจ้าหน้าที่ตำรวจได้เข้าจับกุม น.ส.แสงรวี ผู้ต้องหาเปิดเฟสบุ๊กหลอกขายของเล่นสนามเด็กเล่นราคาถูก มีผู้เสียหายจำนวนมาก ในหลายพื้นที่ทั่วประเทศ จากการตรวจสอบพบว่า มีหมายจับในการก่อเหตุในลักษณะเดียวกันจำนวน 4 หมายจับ ตั้งแต่เมื่อเดือนกันยายน 2563 โดยผู้ต้องหา เปิดเพจเฟสบุ๊กชื่อ “Annabee gold” ใช้ในการฉ้อโกง โดนจะโพสต์ประกาศหลอกขายสินค้าประเภทสนามเด็กเล่นเสริมพัฒนาการ ในราคาชุดละ 990 บาท ทำให้เกิดความสนใจเนื่องจากเป็นสินค้าที่ราคาถูก จึงทำให้ผู้เสียหายที่สนใจหลงเชื่อโอนเงินเข้าไปยังบัญชีธนาคารไทยพาณิชย์ ชื่อบัญชี น.ส.แสงรวี มโนธรรม เลขที่บัญชี 206-282829-2 เมื่อถึงกำหนดส่งสินค้าปรากฏว่าทางเพจไม่ได้ส่งสินค้าให้แต่อย่างใด ซึ่งพบว่ามีประชาชนผู้ที่ได้รับความเสียหายกว่า 200 ราย ดำเนินการแจ้งความร้องทุกข์กับสถานีตำรวจทั่วประเทศ (Policetv, 2564)

2.3.2 การทบทวนวรรณกรรมในประเทศที่เกี่ยวข้อง

จากการทบทวนวรรณกรรมในประเทศที่เกี่ยวข้อง ที่ได้จากการสืบค้นในฐานข้อมูล Thai Journals Online (ThaiJO) ซึ่งเป็นระบบฐานข้อมูลวารสารอิเล็กทรอนิกส์กลางของประเทศไทย ที่เป็นแหล่งรวมวารสารวิชาการที่ผลิตในประเทศไทยทุกสาขาวิชา ทั้งสาขาวิทยาศาสตร์/เทคโนโลยี และมนุษยศาสตร์และสังคมศาสตร์ ThaiJO ด้วยการค้นหาจากคำสำคัญ เช่น มิจฉาชีพออนไลน์ โกงออนไลน์ เป็นต้น ซึ่งพบบทความวิจัยที่น่าสนใจ ดังต่อไปนี้

กรกนก นิลดำและคณะ (2563) ได้ทำการวิจัยเรื่อง วิธีการกลโกง ช่องทางการสื่อสาร และประสบการณ์ในการถูกมิจฉาชีพออนไลน์หลอกลวงของผู้สูงอายุในจังหวัดเชียงราย เครื่องมือที่ใช้ในงานวิจัยในครั้งนี้คือใช้แบบสอบถาม กับกลุ่มผู้สูงอายุตั้งแต่ 50 ปี ขึ้นไป ในตำบลต่าง ๆ ของจังหวัด

เชียงราย โดยใช้กลุ่มตัวอย่างทั้งหมด 400 คน ผลการวิจัยพบว่า วิธีการกลโกงที่มิจฉาชีพออนไลน์ใช้หลอกลวงกลุ่มตัวอย่าง มีดังนี้ 1) การฉ้อโกงโดยหลอกลวงให้ร่วมลงทุนในลักษณะลูกโซ่ ร้อยละ 30.5 2) ฉ้อโกงโดยหลอกลวงให้ทำรายการที่ตู้เอทีเอ็มเพื่อให้โอนเงินไปให้ ร้อยละ 27.25 3) ฉ้อโกงโดยส่งอีเมล์มาทำความรู้จักคุ้นเคยและหลอกลวงให้โอนเงินเข้าบัญชีมิจฉาชีพ ร้อยละ 11.75 4) การฉ้อโกงโดยปลอมตัวและปลอมที่อยู่อีเมล์มาหลอกลวงให้โอนเข้าบัญชีมิจฉาชีพ ร้อยละ 8.25 5) การฉ้อโกงโดยอ้างการรักษาพยาบาลมาหลอกลวงเงิน ร้อยละ 6.25 6) การฉ้อโกงโดยอ้างการเรี่ยไรเงินไปช่วยเหลือทางราชการหรือผู้ด้อยโอกาส ร้อยละ 7.00 7) การฉ้อโกงโดยใช้ศาสนาเป็นเครื่องมือในการหลอกลวง ร้อยละ 3.75 8) การฉ้อโกงโดยอ้างอิงวาเป็นเจ้าหน้าที่ในกระบวนการยุติธรรมและหลอกลวงเอาเงิน ร้อยละ 5.25 โดยผู้สูงอายุส่วนใหญ่ถูกหลอกลวงผ่านช่องทาง เฟสบุ๊ก ร้อยละ 44 รองลงมาคือ แอพพลิเคชั่นไลน์ ร้อยละ 31.25 และน้อยที่สุดคือ อินสตาแกรม ร้อยละ 5.25 และซึ่งเมื่อผู้สูงอายุรู้ว่าตนเองถูกหลอกลวง ผู้สูงอายุส่วนใหญ่ใช้การโพสต์หรือประกาศลงสื่อออนไลน์เพื่อเปิดเผยตัวมิจฉาชีพ ร้อยละ 46.75 รองลงมาคือ แจ้งความกบพนักงานตำรวจ ร้อยละ 25.75 และน้อยที่สุดคือ การตามเอาเงินคืน ร้อยละ 6.50

สถาบันดำรงราชานุภาพ กระทรวงมหาดไทย (2561) ได้ศึกษารูปแบบหรือพฤติกรรมการหลอกลวงในประเด็นต่าง ๆ ปัจจุบัน ซึ่งจากการศึกษาพบว่ารูปแบบประเด็นในการหลอกลวงออนไลน์มีดังนี้ 1) การฉ้อโกงหลอกลวงให้ ร่วมลงทุนในลักษณะแชร์ ลูกโซ่ 2) การฉ้อโกงโดยหลอกลวงให้ทำรายการผ่านตู้เอทีเอ็ม 3) การฉ้อโกงโดยใช้ศาสนาเป็นเครื่องมือหลอกลวงชาวบ้าน 4) การถูกหลอกลวงจากตัวแทนประกันชีวิตหลอกให้ ทำประกันผ่านโทรศัพท์ 5) การถูกหลอกลวงจากการให้บริการหวยออนไลน์หลอกลวงผ่านเว็บไซต์ 6) การฉ้อโกงโดยอ้างว่าเป็นเจ้าหน้าที่ในกระบวนการยุติธรรมและหลอกลวงเอาเงินโดยอ้างว่าเพื่อช่วยเหลือทางคดีความ 7) การฉ้อโกงทาง เฟสบุ๊ก มาทำความรู้จักคุ้นเคยและหลอกลวงให้โอนเงินเข้าบัญชี 8) กลโกงการทุจริตจากการซื้อ–ขายที่ดิน การสวมรอยต่าง ๆ 9) การหลอกลวงฝากให้เข้ารับราชการ

พิรุฬห์รัตน์ ศรีแจ่ม และ ธันย์พันธ์ ใคร้วานิช (2561) ได้ทำการวิจัยเกี่ยวกับปัจจัยของกลโกงในการทำธุรกรรมทางการเงินในยุคดิจิทัล ซึ่งจากการวิจัยพบว่ารูปแบบกลโกงทุกธุรกรรมการเงิน มีดังนี้ 1) การถูกแอบอ้าง 2) การสั่งสินค้าแบบออนไลน์ 3) การหลอกให้รางวัล 4) การหลอกอาชีพเสริมออนไลน์ 5) การหลอกเรียกเก็บเงิน 6) การหลอกลวงให้บริจาค จากแบบสอบถามออนไลน์จำนวนทั้งหมดที่เก็บข้อมูลมานั้นมีจำนวน 745 ชุดนำข้อมูลที่ได้มารวบรวมเพื่อประกอบการวิเคราะห์และประมวลผลทดสอบความสัมพันธ์ของตัวแปรด้วยสถิติ Analysis of Variance (ANOVA) พบว่าผู้ตอบแบบสอบถามส่วนใหญ่เสียหายจากการถูกแอบอ้าง จำนวน 745 คน สูญเงินเฉลี่ย 731 บาท รองลงมาคือเสียหายจากการสั่งสินค้าจำนวน 744 คน สูญเงินเฉลี่ย 895 บาท ต่อมาคือเสียหายจากรางวัลจำนวน 743 คน สูญเงินเฉลี่ย 814 บาท เสียหายจากการหลอกอาชีพจำนวน 743 คน สูญเงินเฉลี่ย 1,154 บาท เสียหายจากการเรียกเก็บจำนวน 742 คน สูญเงินเฉลี่ย 165 บาท และน้อยที่สุดคือเสียหายจากการบริจาคจำนวน 107 คน สูญเงินเฉลี่ย 66 บาท รวมมีความเสียหายโดยรวมต่อการสำรวจครั้งนี้โดยเฉลี่ยคือ 14,666.98 บาท

ฐิติมา อินกล่ำ (2559) ได้ทำการวิจัยเรื่อง วาทกรรมทางการสื่อสารเพื่อการหลอกลวงทำธุรกรรมทางการเงินออนไลน์ ผ่านเครื่องอิเล็กทรอนิกส์ เครื่องมือที่ใช้ในการวิจัยครั้งนี้ใช้แบบสัมภาษณ์เชิงลึกในการเก็บรวบรวมข้อมูลการวิจัยศึกษาจากกลุ่มตัวอย่างที่ถูกหลอกลวงให้ทำธุรกรรมทางการเงินออนไลน์ผ่านเครื่องอิเล็กทรอนิกส์ ในเขตพื้นที่จังหวัดอุตรดิตถ์ จำนวน 16 คน จากการวิจัยพบว่า องค์ประกอบที่มีผลต่อการถูกหลอกลวงทำธุรกรรมทางการเงินออนไลน์ผ่านเครื่องอิเล็กทรอนิกส์ มีองค์ประกอบดังนี้ 1)

ปัจจัยด้านความน่าเชื่อถือของมิจฉาชีพ ซึ่งมิจฉาชีพมักเริ่มต้นการสนทนาด้วยการสร้างความน่าเชื่อถือ โดยส่วนใหญ่มักจะใช้วิธีการสร้างเรื่องราวหรือเหตุการณ์ให้น่าเชื่อและไว้วางใจ รองลงมาคือการอ้างอิงความเป็นบุคคลสำคัญ และการอ้างอิงระบบอิเล็กทรอนิกส์ 2) ปัจจัยด้านเนื้อหาและการพูดคุย ประกอบด้วยการใช้การพูดคุยในการสร้าง ความสนใจให้กับเหยื่อ โดยการสร้างความกลัว หรือการสร้างความหวัง จากนั้นจะพูดคุยไปในเชิงกระตุ้นความต้องการและตอบสนองความต้องการของเหยื่อในด้านผลประโยชน์ ด้านผลตอบแทนที่สูงกว่า ซึ่งมิจฉาชีพจะใช้การโน้มน้าวมากกว่าการข่มขู่ 3) ปัจจัยด้านผู้ถูกหลอกลวง บริบทหรือสิ่งแวดล้อมทางการสื่อสารของผู้รับสารเป็นปัจจัยสำคัญ เช่น บริบทด้านสถานการณ์หรือเงื่อนไขเวลา เป็นสิ่งที่กำหนดให้ผู้รับสารต้องรีบ ตัดสินใจการทำธุรกรรมทางการเงิน ด้านจิตวิทยา เช่น ความกลัว ความโลภ อำนาจทางกฎหมาย รวมถึงวัฒนธรรม สังคม เศรษฐกิจส่วนตัวของผู้รับสารหรือเหยื่อเป็นสิ่งสำคัญที่ส่งผลให้เหยื่อ หลงเชื่อกลอุบายของมิจฉาชีพ และเป็นสิ่งกำหนดพฤติกรรมในการตัดสินใจทำธุรกรรมทางการเงิน ออนไลน์ และ 4) เทคนิคการนำเสนอ โดยการใช้ขั้นตอนการโน้มน้าวใจ (motivated sequence) เพื่อหลอกลวงเหยื่อประกอบด้วย 5 ขั้นตอน คือ การสร้างความสนใจ การสร้างความต้องการหรือระบุปัญหา การตอบสนองความต้องการหรือทางออกของปัญหา การอธิบายให้เห็นภาพข้อดีหรือผลกระทบ และการลงมือปฏิบัติ

พิมลพรรณ บุญยะเสนา และ สุขุม พันธุ์ณรงค์ (2554) ได้ทำการวิจัยเรื่องการวิเคราะห์พฤติกรรมการใช้จ่ายเงินของเด็กและเยาวชนที่ติดเกม โดยจะส่งผลให้มีความเสี่ยงต่อการถูกล่อลวงจากแก๊งมิจฉาชีพ ดังนี้ 1) พฤติกรรมการเล่นเกมเนื่องจากต้องมีการทำธุรกรรมทางการเงินออนไลน์ 2) ปัญหาทางครอบครัว เนื่องจากเด็กติดเกมจะเกิดจากการมีปัญหากับครอบครัวจึงทำให้มีการปรึกษาครอบครัวน้อยลง 3) เทคโนโลยีและสื่อ ยั่วยุในด้านเกมที่มีข้อมูลส่วนใหญ่แนวโน้มไปทิศทางที่หลอกหลวง 4) การให้บริการของธุรกิจการร้านเกมร้านอินเทอร์เน็ตและตู้เกม ที่ไม่มีความปลอดภัยของข้อมูลของผู้ใช้บริการ 5) การคบเพื่อน กลุ่มเพื่อนมีส่วนสำคัญและมีอิทธิพลต่อการตัดสินใจของเด็กและเยาวชนสูงมาก 6) นิสัยส่วนตัวของเด็กและเยาวชน คือ เด็กและเยาวชนที่มีนิสัยอยากรู้ อยากลอง ชอบสิ่งท้าทาย จึงทำให้ตกเป็นเหยื่ออย่างง่ายดาย

สถาบันดำรงราชานุภาพ กระทรวงมหาดไทย (2561) ได้ศึกษารูปแบบหรือพฤติกรรมการหลอกลวงในประเด็นต่างๆ ปัจจุบัน ซึ่งจากการศึกษาพบว่ารูปแบบประเด็นในการหลอกลวงออนไลน์มีดังนี้ 1) การฉ้อโกงหลอกลวงให้ ร่วมลงทุนในลักษณะแชร์ ลูกโซ่ 2) การฉ้อโกงโดยหลอกลวงให้ทำรายการผ่านตู้เอทีเอ็ม 3) การฉ้อโกงโดยใช้ศาสนาเป็นเครื่องมือหลอกลวงชาวบ้าน 4) การถูกหลอกลวงจากตัวแทนประกันชีวิตหลอกให้ ทำประกันผ่านโทรศัพท์ 5) การถูกหลอกลวงจากการให้บริการหวยออนไลน์หลอกลวงผ่านเว็บไซต์ 6) การฉ้อโกงโดยอ้างว่าเป็นเจ้าหน้าที่ในกระบวนการยุติธรรมและหลอกลวงเอาเงินโดยอ้างว่าเพื่อช่วยเหลือทางคดีความ 7) การฉ้อโกงทาง Facebook มาทำความรู้จักคุ้นเคยและหลอกลวงให้โอนเงินเข้าบัญชี 8) กลโกงการทุจริตจากการซื้อ–ขายที่ดิน การสวมรอยต่างๆ 9) การหลอกลวงฝากให้เข้ารับราชการ

ณัฏฐกาญจน์ ศุกลรัตนเมธี และ นุชประภา โมกข์ศาสตร์ (2562) ได้ทำการวิจัยเกี่ยวกับการรู้เท่าทัน สื่อสังคมออนไลน์ของเยาวชนเพื่อการเป็นพลเมืองในสังคมประชาธิปไตย ผลการศึกษาพบว่าสามารถแบ่งตัวชี้วัดการรู้เท่าทันสื่อสังคมออนไลน์ของเยาวชนในสังคมประชาธิปไตยออกเป็นสองกลุ่ม ได้แก่ การรับข้อมูลเข้าและการส่งข้อมูลออกโดยตัวชี้วัดเกี่ยวกับ “การรับข้อมูลเข้า” ประกอบด้วยการมีทักษะในการเข้าถึงข้อมูล (Access) โดยสามารถเลือกรับข้อมูลข่าวสารและสื่อการเมืองจากแหล่งที่หลากหลาย;

ทักษะในการวิเคราะห์และประเมินข้อมูล (Analyze and Evaluate) คือสามารถแยกความจริงออกจากความเห็นสามารถวิเคราะห์ ความน่าเชื่อถือของข้อมูลและการตระหนักในหน้าที่พลเมืองคือ สามารถร้องเรียนหน่วยงานที่เกี่ยวข้องเมื่อพบเห็นการทำผิดกฎหมายส่วนตัวชี้วัดเกี่ยวกับ “การส่งข้อมูลออก” ประกอบด้วยการมีทักษะในการผลิตสื่อ (Create) คือสามารถเลือกวิธีการนำเสนอที่เหมาะสมกับวัตถุประสงค์และเนื้อหาที่ต้องการนำเสนอ การมีส่วนร่วม (Participate) ในการใช้สื่อสังคมออนไลน์อย่างสร้างสรรค์ คือ การเคารพความคิดเห็นที่แตกต่าง การโต้แย้งโดยใช้หลักเหตุและผล การใช้ภาษาแบบสันติวิธีการไม่ใช้ถ้อยคำดูหมิ่น ผู้อื่น และการน าเสนอหรือแชร์ข้อมูลที่เป็นประโยชน์ต่อผู้อื่นและสังคม และการรู้สิทธิ หน้าที่ และความ รับผิดชอบตามกฎหมาย คือไม่ใช้คอมพิวเตอร์ทำร้ายหรือละเมิดผู้อื่น สร้างหลักฐานที่เป็นเท็จ ละเมิด การใช้ทรัพยากรคอมพิวเตอร์โดยที่ตนเองไม่มีสิทธิ์ (Copyright) และต้องคำนึงถึงผลกระทบที่จะเกิดขึ้น ต่อสังคมอันเกิดจากการกระทำของตน

ณัฐณิชา คุ้มแพทย์ (2563) ได้ทำการวิจัยเกี่ยวกับการละเมิดสิทธิความเป็นส่วนตัวและสิทธิในชื่อเสียงโดยการประจานในพื้นที่ซื้อขายสินค้าออนไลน์ จากการสำรวจสภาพปัญหาในพื้นที่เครือข่ายสังคมออนไลน์ พบว่าผู้ประกอบธุรกิจส่วนใหญ่ที่นำข้อความการสนทนาออนไลน์และข้อมูลของผู้บริโภคมาประจานเกิดจากการที่ผู้บริโภคขอยกเลิกคำสั่งซื้อหรือสั่งซื้อแล้วหายเงียบไปโดยไม่โอนเงินให้แก่ผู้ประกอบธุรกิจ โดยโพสต์ของผู้ประกอบธุรกิจที่เป็นการประจานผู้บริโภคที่สามารถเข้าถึงได้ในขณะนี้สามารถแบ่งออกเป็น 2 กรณีหลัก คือ กรณีแรก ผู้บริโภคได้ขอยกเลิกการสั่งซื้อกับผู้ประกอบธุรกิจ ก็จะถูกประจานด้วยข้อความการสนทนาออนไลน์ที่ผู้บริโภคได้ยกเลิกคำสั่งซื้อ รวมถึงรูปบัญชีเครือข่ายสังคมออนไลน์ของผู้บริโภคอีกด้วย ยิ่งไปกว่านั้นกรณีที่ผู้บริโภคเคยติดต่อซื้อขายกับผู้ประกอบธุรกิจมาก่อน ผู้ประกอบธุรกิจก็จะนำข้อมูลเก่า ๆ ซึ่งอยู่ในเนื้อหาการสนทนาที่ผู้ประกอบธุรกิจบันทึกไว้มาประจานต่อสังคม ส่วนกรณีที่สองเป็นกรณีที่ผู้บริโภคไม่ได้บอกยกเลิกคำสั่งซื้อ แต่หายเงียบไปโดยไม่ได้โอนเงินให้ผู้ประกอบธุรกิจ ผู้บริโภคจะถูกประจานในลักษณะคล้ายกับกรณีแรก ดังนั้น ธุรกิจอีคอมเมิร์ซจะสามารถแข่งขันในตลาดต่อไปได้ ผู้ประกอบธุรกิจจะต้องมีมาตรการที่จะทำให้ผู้บริโภคมั่นใจว่าความเป็นส่วนตัวและความปลอดภัย

ณัฐธรณ์ เดชสกุล และ จอมเดช ตรีเมฆ (2563) ได้ทำการวิจัยเกี่ยวกับการศึกษาสถานการณ์ในปัจจุบันของการฉ้อโกงซื้อขายสินค้าทางอินเทอร์เน็ต รูปแบบของการฉ้อโกงซื้อขายสินค้าทางอินเทอร์เน็ต ปัญหาในกระบวนการยุติธรรมในคดีการฉ้อโกงซื้อขายสินค้าทางอินเทอร์เน็ต และแนวคิดและข้อเสนอแนะเกี่ยวกับการฉ้อโกงซื้อขายสินค้าทางอินเทอร์เน็ตจากการศึกษาวิจัยพบว่าสถานการณ์ปัจจุบันปัญหาการฉ้อโกงซื้อขายสินค้าทางอินเทอร์เน็ตในประเทศไทยพบว่าเหยื่อในการฉ้อโกงซื้อขายสินค้าทางอินเทอร์เน็ตในประเทศไทยเป็นเพศหญิงซึ่งอยู่ในวัยทำงานโดยมีสาเหตุเกิดจากความโลภของเหยื่อทำให้เกิดเหยื่อขาดความ ระมัดระวังตัวนอกจากนี้คนร้ายยังสามารถสร้างความน่าเชื่อถือโดยหลองลวงเหยื่อได้อย่างแนบเนียน ในด้านของปัญหาในกระบวนการยุติธรรม ผลการวิจัยค่อนข้างชัดเจนว่ากระบวนการยุติธรรมมีความล่าช้า เนื่องจากเจาหน้าที่ขาดความรู้ความชำนาญมีเจ้าหน้าที่รองรับไม่เพียงพอและความยากในการรวบรวมพยานหลักฐาน ดังนั้นแนวคิดและข้อเสนอแนะของผู้ให้ข้อมูลสำคัญจากการศึกษาในครั้งนี้ส่วนใหญ่มีแนวคิดว่าการให้ความรู้แก่เหยื่อและเจ้าหน้าที่ผู้ปฏิบัติงานในกระบวนการยุติธรรมนั้นสามารถแก้ไขปัญหาการฉ้อโกงซื้อขายสินค้าทางอินเทอร์เน็ต

สลิลพร อิศรางกูร ณ อยุธยา (2561) ได้ทำการวิจัยเรื่องแนวทางการป้องกันการหลอกลวงให้โอนเงินในธุรกิจขนาดกลางและขนาดเล็ก ผลการวิจัยพบว่าแนวทางการแก้ไขปัญหาการถูกหลอกลวงให้โอน

เงินผิดบัญชีมีดังนี้ 1) การพัฒนาระบบ KYC (Know Your Customer) และควรมีการแลกเปลี่ยนข้อมูลระหว่างธนาคาร รวมถึงเพิ่มระดับความลึกของข้อมูลที่จะสอบถามลูกค้าก่อนการเปิดบัญชี เพื่อ ป้องกันความเสี่ยงมิให้เกิดการเปิดบัญชีของมิจฉาชีพ ซึ่งจะเสี่ยงต่อการโอนเงินไปสู่บัญชีของแฮกเกอร์ 2) การใช้เทคโนโลยีบล็อกเชน (Blockchain) เพื่อลดความเสี่ยงจากการถูกหลอกลวงให้โอนเงินผิดบัญชีระบบบล็อกเชนเป็นเทคโนโลยีการเก็บข้อมูลการชำระเงินแบบใหม่ที่ตัดคนกลางออกไปและนำข้อมูลมาเก็บไว้ที่ทุกคนที่อยู่ในระบบและเชื่อมต่อผู้ใช้ทุกคนเหมือนห่วงโซ่ทำให้เกิดความโปร่งใส เนื่องจากธุรกรรมการโอนเงินระหว่างประเทศจะเกิดขึ้นได้อย่างสมบูรณ์ก็ต่อเมื่อทุกฝ่าย ในเครือข่ายยอมรับความถูกต้อง ดังนั้นเมื่อข้อมูลการโอนเงินถูกบันทึกแล้วจะไม่สามารถเข้าไป เปลี่ยนแปลงข้อมูลได้ ระบบบล็อกเชนจึงช่วยแก้ปัญหาการถูกหลอกลวงให้โอนเงินผิดบัญชีโดย แฮกเกอร์ 3) การจัดงานสัมมนาหรือการจัดอบรมให้ความรู้เกี่ยวกับความเสี่ยงจากการถูกหลอกลวงให้โอนเงินผิดบัญชีซึ่งวิทยากรหรือผู้บรรยายอาจเป็นเจ้าหน้าที่ที่มีความรู้ความเชี่ยวชาญด้านการค้าระหว่างประเทศของธนาคารเองหรือการเชิญวิทยากรจากหน่วยงานรัฐเพื่อให้ข้อมูลและความเสี่ยงในการทำธุรกรรมระหว่างประเทศต่าง ๆ แก่ผู้ประกอบการนำเข้า

มูลนิธิแม่ฟ้าหลวง ในพระบรมราชูปถัมภ์ (2564) ได้เผยกลโกงออนไลน์ของมิจฉาชีพยุค New Normal ซึ่งมีกลโกงดังนี้ 1) เสนองานออนไลน์โดยการหลอกให้ทำงานแล้วไม่จ่ายค่าตอบแทนหรือจ่ายให้น้อยกว่าตกลง 2) ลวงให้บริจาคโดยอาจสร้างเรื่องราวที่ไม่เป็นจริง เพื่อล่อลวงให้โอนเงินช่วยเหลือเข้าบัญชีมิจฉาชีพ 3) ล่อลวงข้อมูลส่วนตัวโดยอาจจะผ่านอีเมล์ปลอม (Phishing email) หรือติดต่อมาโดยตรงโดยแอบอ้างเป็นผู้เชี่ยวชาญหรือเจ้าหน้าที่ และได้เสนอข้อแนะนำในการใช้ชีวิตในโลกออนไลน์ให้ห่างไกลจากกลโกงต่าง ๆ ดังนี้ 1) ห่างให้ไกลจากคนหรือเว็บไซต์ที่ไม่น่าไว้ใจ ตลอดจนโฆษณาชวนเชื่อที่เกินจริง อย่าเชื่อใจคนง่าย โดยเฉพาะคนที่เพิ่งรู้จักกันผ่านออนไลน์ 2) ปิดกั้นข้อมูลส่วนตัวที่สำคัญ อย่าให้ใครรู้ได้เป็นดี โดยเฉพาะรหัส OTP บัตรประชาชน บัญชีธนาคาร บัตรเครดิต/เดบิต 3) ติดตั้งแอปจำพวกแอนตี้ไวรัส ศึกษาการตั้งค่าความเป็นส่วนตัว และหมั่นอัปเดตระบบปฏิบัติการโทรศัพท์มือถือเป็นเวอร์ชั่นล่าสุดจากผู้ให้บริการโดยตรงเพื่อเสริมระบบความปลอดภัยให้ทันสมัยอยู่เสมอ พร้อมเปลี่ยนรหัสผ่านบ่อย ๆ 4) จ่ายเงินแต่ละทีต้อง "ตั้งสติให้ดี" ตรวจสอบให้ถี่ถ้วน ทั้งชื่อผู้โอน จำนวนเงิน บัญชีดูน่าสงสัยหรือไม่ เช็คทุกครั้งที่ได้รับการแจ้งเตือน

Akkarakantrakorn (2020) ได้ทำการศึกษาด้วยวิธีการแบบผสมผสานเพื่อตรวจสอบปัจจัยที่นำไปสู่การซื้อทางออนไลน์ในขณะที่รวบรวมหลักฐานเพื่อพัฒนาแนวทางในการรวบรวมหลักฐานดิจิทัล กลุ่มตัวอย่างเชิงปริมาณจากกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีจำนวน 95 คน ในขณะที่กลุ่มตัวอย่างเชิงคุณภาพประกอบด้วยตำรวจ 6 นายจากหน่วยงานเดียวกันและผู้บริหารระดับสูงในหน่วยงานต่าง ๆ 13 คน ซึ่งได้รับการประสานงานกับหน่วยงานภาครัฐและรัฐในการประสานงานด้านข้อมูลดิจิทัล การรวบรวมพยานหลักฐาน การศึกษานี้ใช้การสนทนากลุ่มและการสัมภาษณ์เชิงลึก ใช้แบบสอบถามค่าร้อยละ ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน ผลการวิจัยพบว่าการฉ้อโกงจากการซื้อของออนไลน์ทำได้ 3 วิธี คือ 1) การหลอกลวงผู้ซื้อ 2) การหลอกลวงผู้ขาย และ 3) การหลอกลวงผู้ซื้อและผู้ขาย นอกจากนี้ยังพบว่า แนวทางที่สำคัญในการรับป้องการและลดปัญหาการฉ้อโกงออนไลน์ก็คือ การสร้างการรับรู้ของประชาชนในการป้องกันและลดความเสี่ยงจากการฉ้อโกงการซื้อสินค้าออนไลน์

พิรุฬห์รัตน์ ศรีแจ่ม และธันย์พันธ์ ใคร้วานิช (2561) ได้ทำงานวิจัยเกี่ยวกับปัจจัยของกลโกงในการทำธุรกรรมทางการเงินในยุคดิจิทัล ซึ่งจากการวิจัยพบว่ารูปแบบกลโกงทุกธุรกรรมการเงิน มีดังนี้ 1) การ

ถูกแอบอ้าง 2) การสั่งสินค้าแบบออนไลน์ 3) การหลอกให้รางวัล 4) การหลอกอาชีพเสริมออนไลน์ 5) การหลอกเรียกเก็บเงิน 6) การหลอกลวงให้บริจาค จากแบบสอบถามออนไลน์จำนวนทั้งหมดที่เก็บข้อมูลมานั้นมีจำนวน 745 ชุดนำข้อมูลที่ได้มารวบรวมเพื่อประกอบการวิเคราะห์และประมวลผลทดสอบความสัมพันธ์ของตัวแปรด้วยสถิติ Analysis of Variance (ANOVA) พบว่าผู้ตอบแบบสอบถามส่วนใหญ่เสียหายจากการถูกแอบอ้าง จำนวน 745 คน สูญเงินเฉลี่ย 731 บาท รองลงมาคือเสียหายจากการสั่งสินค้าจำนวน 744 คน สูญเงินเฉลี่ย 895 บาท ต่อมาคือเสียหายจากรางวัลจำนวน 743 คน สูญเงินเฉลี่ย 814 บาท เสียหายจากการหลอกอาชีพจำนวน 743 คน สูญเงินเฉลี่ย 1,154 บาท เสียหายจากการเรียกเก็บจำนวน 742 คน สูญเงินเฉลี่ย 165 บาท และน้อยที่สุดคือเสียหายจากการบริจาคจำนวน 107 คน สูญเงินเฉลี่ย 66 บาท รวมมีความเสียหายโดยรวมต่อการสำรวจครั้งนี้โดยเฉลี่ยคือ 14,666.98 บาท

2.3.3 การทบทวนวรรณกรรมในต่างประเทศที่เกี่ยวข้อง

จากการทบทวนวรรณกรรมของต่างประเทศที่เกี่ยวข้อง ที่ได้จากการสืบค้นในฐานข้อมูลต่าง ๆ ของต่างประเทศผ่านทาง https://scholar.google.com/ ด้วยการค้นหาจากคำสำคัญ เช่น cyber scam, cybersecurity scam, cyber fraud, cybersecurity fraud เป็นต้น พบว่ามีบทความวิจัยและบทความวิชาการในช่วง3-4 ปีที่ผ่านมาที่น่าสนใจ ดังนี้

Ihmaidi และคณะ (2006) ได้นำเสนอระบบการซื้อสินค้าออนไลน์ที่ปลอดภัย เพื่อช่วยให้ผู้ใช้อินเทอร์เน็ตมั่นใจในการใช้บัตรเครดิตในการซื้อสินค้าออนไลน์ โดยระบบที่นำเสนอนี้ มีการใช้ลายนิ้วมือร่วมกับการตรวจสอบเพื่อยืนยันตัวตนของผู้ถือบัตร ทั้งนี้ระบบที่นำเสนอจะมีการเข้ารหัสข้อมูลของการ์ดและมีการใช้อัลกอริธึมในการอำพรางข้อมูลไว้ในภาพประเภทพิเศษ โดยระบบนี้จะต้องมีการใช้ซอฟต์แวร์พิเศษในการสร้างภาพ Electronic Internet Shopping Card (EISC) และอำพรางข้อมูลเพื่อใช้ในการยืนยันตัวตนในการการซื้อสินค้าออนไลน์แต่ละครั้ง ก่อนที่จะมีการอนุมัติให้ชำระเงินผ่านบัตรเครดิตโดยบริษัทผู้ออกบัตร(หรือธนาคาร)

Gunjan และคณะ (2013) ได้ทำการศึกษาเกี่ยวกับอาชญากรรมไซเบอร์ในประเทศอินเดีย และได้แบ่งอาชญากรรมไซเบอร์ออกเป็นประเภทต่าง ๆ ประมาณ 20 ประเภท ได้แก่ อาชญากรรมทางการเงิน สื่อลามกออนไลน์ การขายบทความที่ผิดกฎหมาย การพนันออนไลน์ อาชญากรรมทรัพย์สินทางปัญญา การปลอมแปลงอีเมล การหมิ่นประมาททางไซเบอร์ การสะกดรอยตามทางไซเบอร์ การระเบิดอีเมล การโจมตีแบบปฏิเสธการให้บริการ การโจมตีของไวรัสหรือหนอนคอมพิวเตอร์ ม้าโทรจันและคีย์ล็อกเกอร์ การขโมยเวลาใช้งานอินเทอร์เน็ต การขโมยเว็บไซต์ การฉ้อโกงทางอีเมล การก่อการร้ายทางไซเบอร์ และ สงครามไซเบอร์ เป็นต้น นอกจากนี้คณะผู้วิจัยดังกล่าวยังได้ทำการศึกษาเบื้องต้นเกี่ยวกับอีเมลฟิชชิ่งและฟิชชิ่งทางโทรศัพท์ด้วย แล้วได้กล่าวสรุปว่า ความรู้เกี่ยวกับอาชญากรรมทางไซเบอร์และความรู้ที่เกี่ยวข้องเป็นประเด็นที่มีความสำคัญ

More และคณะ (2015) ได้ทำการศึกษาเพื่อทบทวนเกี่ยวกับสถานการณ์ของการธนาคารออนไลน์และการโจมตีทางไซเบอร์ในอินเดีย โดยมุ่งเน้นไปที่อาชญากรรมไซเบอร์ที่เกี่ยวข้องกับการธนาคารออนไลน์และกลเม็ดและเทคนิคใหม่ ๆ ที่แฮกเกอร์ใช้ โดยมีการนำข่าวอาชญากรรมไซเบอร์ที่เกี่ยวข้องกับการธนาคารออนไลน์ และรายงานของหน่วยงานรัฐและองค์กรต่างประเทศมาศึกษาด้วย จากการศึกษานี้พบว่า อาชญากรรมไซเบอร์ที่เกี่ยวข้องกับการธนาคารออนไลน์ในอินเดียมีแนวโน้มเพิ่มขึ้น

โดยอาชญากรรมทางไซเบอร์ส่วนใหญ่กระทำโดยเยาวชนในกลุ่มอายุ 18-30 ปีและเป็นเพศชาย ดังนั้น หน่วยงานบังคับใช้กฎหมายจำเป็นต้องมีความพร้อมในการป้องกันอาชญากรรมทางไซเบอร์ดังกล่าว

Zachariah และ Ismail Z. (2016) ได้ทำการศึกษาเกี่ยวกับภัยทางไซเบอร์ที่แฝงมากับซื้อขายสินค้าและบริการออนไลน์ จากนั้นผู้วิจัยได้นำเสนอกรอบการทำงานหรือเฟรมเวิร์คที่เกี่ยวข้องกับลูกค้า รวมไปถึงกระบวนในการซื้อสินค้าออนไลน์และการชำระเงินโดยใช้ Online Payment Alternative Solution (OPAS) ซึ่งเป็นแอปพลิเคชันมือถือที่ถูกพัฒนาขึ้น เพื่อเพิ่มความปลอดภัยของกรอบการทำงาน งานดังกล่าว มีการใช้การเข้ารหัสแบบ Blowfish ของ Dynamic One Time Password (OTP) และ One Time Password Encryption Key (OTPEK) จากนั้น OTP และ OTPEK ที่เข้ารหัสจะถูกฝังไว้ในภาพ captcha โดยใช้เทคนิคการอำพรางข้อมูลที่เรียกว่า Steganography Bit Significant Bit (LSB) จากนั้นส่งไปยัง OPAS ของลูกค้าเพื่อขออนุมัติการชำระเงินแบบเรียลไทม์ ซึ่งผู้วิจัยระบุว่า ระบบที่พัฒนาขึ้นได้รับการทดสอบภายใต้เงื่อนไขที่ทำการศึกษา พบว่า ระบบสามารถทำงานได้อย่างถูกต้องตามและมีประสิทธิภาพ

Olujide และ Olusegu (2017) ได้ผลการศึกษาที่สะท้อนถึงผลกระทบของอาชญากรรมไซเบอร์ต่อการพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce) ในประเทศไนจีเรีย และได้กล่าวถึงการเติบโตและผลประโยชน์ของการการพาณิชย์อิเล็กทรอนิกส์ ตลอดจนอาชญากรรมไซเบอร์ และผลกระทบต่อธุรกิจและสังคมโดยทั่วไป ในขณะที่ประชาชนทั่วไปมีการใช้คอมพิวเตอร์มากขึ้น จึงมีความเป็นไปได้สูงที่อาชญากรรมไซเบอร์จะกลายเป็นเรื่องปกติ นอกจากนี้ผู้เขียนยังได้ระบุว่า ไนจีเรียได้รับการจัดอันดับให้เป็นหนึ่งในประเทศที่มีอาชญากรรมอิเล็กทรอนิกส์ในระดับสูงสุด ความปลอดภัยทางไซเบอร์จึงจำเป็นต้องได้รับการแก้ไขอย่างจริงจังเนื่องจากส่งผลกระทบต่อภาพลักษณ์ของประเทศต่อสายตาทั่วโลก ไนจีเรียมีศักยภาพที่ดีในด้านการพาณิชย์อิเล็กทรอนิกส์ แต่ด้วยปัญหาเชิงลบที่กล่าวไว้ข้างต้น การต่อสู้กับอาชญากรรมในโลกไซเบอร์ด้วยวิธีการแบบองค์รวมจึงเป็นสิ่งจำเป็น ซึ่งรวมถึงการรวบรวมมาตรการทางเทคนิคที่เหมาะสม รวมไปถึงการยับยั้งทางกฎหมาย ในช่วงท้ายผู้เขียนได้กล่าวว่า หน่วยงานด้านความมั่นคงของรัฐบาลความจำเป็นที่จะต้องติดตามความก้าวหน้าทางเทคโนโลยีและความมั่นคงปลอดภัยไม่ให้ล้าหลังกว่าอาชญากรไซเบอร์

Sarmah และคณะ (2017) ได้มีการนำเสนอบทความเพื่อเผยแพร่ความรู้เกี่ยวกับอาชญากรรมหรือความผิดที่เกิดขึ้นผ่านอินเทอร์เน็ตหรือโลกไซเบอร์ พร้อมกับกฎหมายที่บังคับใช้กับอาชญากรรมไซเบอร์และอาชญากรไซเบอร์ นอกจากนี้ ผู้เขียนยังได้นำเสนอวิวัฒนาการของอาชญากรรมไซเบอร์ โดยได้มีการจำแนกอาชญากรรมไซเบอร์ออกเป็น 4 ประเภทหลัก ๆ คือ 1) อาชญากรรมไซเบอร์ต่อบุคคล 2) อาชญากรรมไซเบอร์ต่อทรัพย์สิน 3) อาชญากรรมไซเบอร์ต่อองค์กร และ 4) อาชญากรรมไซเบอร์ต่อสังคม ผู้เขียนยังได้ระบุด้วยว่า อาชญากรรมไซเบอร์กลายเป็นภัยคุกคามที่ยิ่งใหญ่ต่อมนุษยชาติ การป้องกันอาชญากรรมในโลกไซเบอร์จึงเป็นส่วนสำคัญสำหรับสังคม วัฒนธรรม และความมั่นคงปลอดภัยของประเทศ ดังนั้นรัฐบาลอินเดียจึงได้ออกกฎหมายต่าง ๆ เพื่อจัดการกับอาชญากรรมทางไซเบอร์ อย่างไรก็ตาม เนื่องจากอาชญากรรมไซเบอร์ส่วนหนึ่งเกิดขึ้นจากการเชื่อมต่ออินเทอร์เน็ตระหว่างประเทศ จึงสร้างความซับซ้อนทั้งทางเทคนิคและกฎหมายในการสืบสวนและดำเนินคดีอาชญากรรมเหล่านี้ ดังนั้น ผู้เขียนจึงได้ระบุในช่วงท้ายว่า ในการที่จะดำเนินการกับอาชญากรรมไซเบอร์ จำเป็นต้องมีการประสานความร่วมมือระหว่างประเทศต่าง ๆ

Van De Weijer และ Leukfeldt (2017) ได้ทำการศึกษาและนำเสนอลักษณะบุคลิกภาพ 5 แบบของเหยื่ออาชญากรรมทางไซเบอร์ในประเทศเนเธอร์แลนด์ โดยทำการศึกษาและสำรวจกลุ่มตัวอย่างชาวดัตช์จำนวน 3,648 คน เพื่อศึกษาความสัมพันธ์ระหว่างการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์และลักษณะสำคัญจากบุคลิกภาพ 5 แบบ ซึ่งประกอบด้วย ความเป็นที่พอใจ ความมีมโนธรรม ความมั่นคงทางอารมณ์ และการเปิดกว้างต่อประสบการณ์ เพื่อเปรียบเทียบและตรวจสอบความสัมพันธ์ระหว่างลักษณะบุคลิกภาพ และเหยื่อ 3 กลุ่ม ซึ่งประกอบด้วยเหยื่ออาชญากรรมในโลกไซเบอร์ เทียบกับผู้ที่ไม่ได้เป็นเหยื่ออาชญากรรมแบบดั้งเดิม และผู้ที่ไม่ได้เป็นเหยื่อทางอาชญากรรมทางไซเบอร์ จากนั้นทำการวิเคราะห์ด้วยเทคนิค multinomial logistic regression ซึ่งพบว่า ผู้ที่มีความมั่นคงทางอารมณ์สูงกว่าเท่านั้นถึงจะมีโอกาสน้อยในการตกเป็นเหยื่อของอาชญากรรมในโลกไซเบอร์

Mangoli (2017) ได้กล่าวว่า อาชญากรรมไซเบอร์เป็นภัยคุกคามใหญ่ของอินเดีย โดยอินเดียถูกจัดอยู่ในอันดับต้น ๆ ของโลกจากการจัดอันดับประเทศที่ได้รับผลกระทบจากอาชญากรรมไซเบอร์ โดยอ้างรายงานของ Security and Defence Agenda (SDA) และ McAfee ผู้เขียนจึงได้ทำการศึกษาเกี่ยวกับการเกิดอาชญากรรมทางไซเบอร์ในอินเดียที่เพิ่มขึ้นอย่างมาก โดยศึกษาทั้งจากที่มีการบันทึกไว้โดยสำนักงานหน่วยงานรัฐของอินเดีย ซึ่งพบว่าอาชญากรรมไซเบอร์ได้เพิ่มขึ้นตามการใช้งานที่เพิ่มขึ้นในเครือข่ายอิเล็กทรอนิกส์และเครือข่ายสังคม นอกจากนี้ผู้เขียนยังได้ใช้วิธีการรวบรวมแหล่งข้อมูลจากสื่อสิ่งพิมพ์ หนังสือ นิตยสาร และจากอัตราการเกิดอาชญากรรมไซเบอร์ที่บันทึกในปีก่อน ๆ ทำให้ทราบตัวเลขที่คาดการณ์การเกิดอาชญากรรมไซเบอร์ในอินเดียว่าอาจเพิ่มขึ้นถึง 3,000,000 ครั้ง ในปี 2558 ซึ่งคิดเป็นสองเท่าเมื่อเทียบกับปี 2557 ผู้เขียนได้ระบุด้วยว่า การปรับปรุงหน่วยงานตำรวจของอินเดียให้ทันสมัยเป็นสิ่งจำเป็น ทั้งนี้ก็เพื่อให้สามารถจัดการกับภัยที่มากับเทคโนโลยีอิเล็กทรอนิกส์และเครือข่ายสังคมออนไลน์ และหน่วยงานตำรวจควรเป็นผู้นำในการให้ความรู้และสร้างความตระหนักรู้ให้กับประชาชน

Yoshida และคณะ (2017) ได้ทำการศึกษาและนำเสนอวิธีการในการตรวจจับการฉ้อโกงจากการซื้อขายสินค้าออนไลน์ที่เกิดขึ้นในญี่ปุ่นในรูปแบบที่มีการสั่งสินค้าออนไลน์แล้ว แล้วเมื่อสินค้าถูกส่งถึงลูกค้าแล้วลูกค้าที่เป็นมิจฉาชีพก็จะหายตัวไปในขณะที่ผู้ขายก็ไม่ได้รับเงินที่ปกติจะชำระผ่านด้วยการหักเงินจากบัญชี ด้วยการนำเสนอแนวทางในการศึกษาด้วยวิธีการใหม่ กล่าวคือ ใช้วิธีการทำเหมืองข้อมูลที่หลากหลายบนพื้นฐานของสถิติ ไม่ใช่การทำเหมืองข้อมูลเพียงรูปแบบเดียว คุณสมบัติหลักที่นำเสนอในการศึกษานี้คือ การใช้ธรรมชาติของของการเกิดอาชญากรรมทางเศรษฐกิจมาช่วยในการวิเคราะห์ ไม่ว่าจะเป็นนอาชญากรรมทางเศรษฐกิจ ใช้ระบบการชำระเงินผ่านด้วยการหักเงินจากบัญชี และมีการเช่าอพาร์ตเมนต์ระยะสั้น ลักษณะสินค้าที่มิจฉาชีพสั่งมักจะเป็นสินค้าที่เปลี่ยนเป็นเงินสดได้ง่าย ทั้งนี้ ในการวิเคราะห์ข้อมูลที่ใช้ในการศึกษานี้มีการนำที่อยู่ ข้อมูลคุกกี้ของเว็บบราวเซอร์ และชนิดของสินค้าออนไลน์

Nasution และคณะ (2018) ได้นำเสนอปรากฏการณ์ของ CYBER-CRIME และ การหลอกลวงฉ้อโกงในร้านค้าออนไลน์ ซึ่งอินเทอร์เน็ตได้พัฒนาเป็นช่องทางสำคัญสำหรับการซื้อสินค้า ทำให้อินเทอร์เน็ตเป็นสื่อหรือช่องทางการตลาดที่ได้รับความนิยม เนื่องจากการขายสินค้าจะทำได้ง่ายขึ้นและผู้บริโภคสามารถเข้าถึงได้มากขึ้นแล้ว ราคาไม่แพงสำหรับสินค้าอุปโภคบริโภค แต่ด้านลบจาก e-shopping ที่ทำให้เกิด "การตกเป็นเหยื่อการฉ้อโกง" ทำให้ผู้ใช้อินเทอร์เน็ตแต่ละคนมีความเสี่ยงที่จะเผชิญกับด้านมืดของอินเทอร์เน็ตที่เรียกว่าอาชญากรรมทางไซเบอร์ เช่น ในช่วงปี 2559 ระดับอาชญากรรมไซเบอร์ทั่วโลกมีมูลค่าสูงถึง 450 พันล้านเหรียญสหรัฐ ตัวเลขดังกล่าวอาจเพิ่มขึ้นอย่าง

ต่อเนื่องโดยเฉพาะในเมืองใหญ่ ในบทความดังกล่าวระบุว่า จากการสำรวจโดยสถาบันรักษาความปลอดภัยไซเบอร์ CISSReC 2017 พบว่าระดับความตระหนักรู้ของผู้ใช้อินเทอร์เน็ตเกี่ยวกับภัยทางไซเบอร์ในอินโดนีเซียยังค่อนข้างต่ำ

Reep-van den Bergh และ Junger (2018) ได้ทำการศึกษาด้วยการตรวจสอบข้อมูลเกี่ยวกับเหยื่อ โดยการค้นหาข้อมูลจากฐานข้อมูลออนไลน์ และประสานงานไปยังสำนักงานสถิติแห่งชาติหลายแห่งในยุโรป แล้วทำการสำรวจ คัดเลือกข้อมูลที่เกี่ยวข้องกับเหยื่ออาชญากรรมแต่ละราย ซึ่งในการศึกษาดังกล่าว มีการแบ่งการฉ้อโกงออนไลน์ออกเป็น 6 ประเภท ได้แก่ การฉ้อโกงจากการซื้อสินค้าออนไลน์ การฉ้อโกงธนาคารออนไลน์ หรือการชำระเงิน การฉ้อโกงทางไซเบอร์อื่น ๆ (เช่น การฉ้อโกงค่าธรรมเนียมขั้นสูง) ภัยคุกคามทางไซเบอร์ หรือการล่วงละเมิด มัลแวร์ และการแฮ็กข้อมูล จากการศึกษาดังกล่าวพบว่า อัตราความชุกของอาชญากรรมประจำปีอยู่ระหว่าง 1-3% สำหรับการฉ้อโกงจากการซื้อสินค้าออนไลน์ น้อยกว่า 1-2% สำหรับการฉ้อโกงทางธนาคารหรือการชำระเงินออนไลน์ นอกจากนี้ ยังพบประเด็นว่า ความชุกของอาชญากรรมไซเบอร์ (และแนวโน้ม) สามารถวัดได้ดีก็ต่อเมื่อมีการตั้งคำถามที่เหมาะสมกับแต่ละประเทศ นอกจากนี้ ควรมีการแบ่งประเภทของความผิดทางไซเบอร์ที่แตกต่างกันอย่างสม่ำเสมอ และควรมีคำถามคัดกรองเพื่อให้ได้คำตอบที่แม่นยำยิ่งขึ้น

Purba (2019) ได้ทำการศึกษาในประเทศอินโดนีเซียเกี่ยวกับการทำธุรกรรม e-commerce ที่ใช้อินเทอร์เน็ตทั้งในระบบท้องถิ่นและระดับประเทศ และศึกษาเกี่ยวกับการเลือกใช้กฎหมายและการใช้อำนาจศาลเพื่อจัดการกับอาชญกรรม e-commerce จากการศึกษาดังกล่าว ผู้วิจัยได้ทำการจำแนกรูปแบบการเกิดอาชญากรรม e-commerce เอาไว้อย่างน้อย 15 รูปแบบ ตัวอย่างเช่น การแคร็กโปรแกรม (Cracking) การแฮ็กระบบหรือข้อมูล (Hacking) การโจมตีด้วยม้าโทรจัน (Trojan horse) การรั่วไหลของข้อมูล (Data leakage) การจารกรรมข้อมูล (Cyber Espionage) การปลอมแปลงข้อมูล (Data Forgery) การเข้าถึงข้อมูลหรือระบบโดยไม่ได้รับอนุญาต (Unauthorized Access) การละเมิดทรัพย์สินทางปัญญา (Offense against Intellectual Property) และการเผยแพร่สื่อผิดกฎหมาย (Illegal Contents) เป็นต้น

Fan (2019) ได้ทำการศึกษาผลกระทบของการฉ้อโกงทางไซเบอร์ที่เกี่ยวข้องกับการซื้อขายสินค้าออนไลน์ในประเทศกานา ซึ่งเป็นประเทศที่มีโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศที่ไม่ดี การเติบโตของผู้ใช้เทคโนโลยีสารสนเทศยังไม่มาก และการขาดกฎระเบียบและการบังคับใช้กฎหมายการ รวมไปถึงการฝึกอบรม จึงกลายเป็นสาเหตุพื้นฐานที่ทำให้การสร้างความปลอดภัยทางออนไลน์เป็นเรื่องยากและด้วยเหตุนี้จึงขาดความไว้วางใจ ซึ่งเป็นประเด็นหลักที่ได้จากการศึกษานี้ ในขณะที่การซื้อของออนไลน์ซึ่งเป็นความก้าวหน้าทางเทคโนโลยีที่สะดวกสบายและรูปแบบการทำธุรกรรมที่ค่อนข้างมีชื่อเสียงในฝั่งตะวันตก ต้องอาศัยความไว้วางใจระหว่างลูกค้าและผู้ขายในระดับที่มาก

Karo (2019) ได้ทำการศึกษาเชิงวิเคราะห์ทางกฎหมายเกี่ยวกับกฎหมายอาญาที่เกี่ยวข้องการฉ้อโกงจากการซื้อขายสินค้าออนไลน์ในอินโดนีเซีย ซึ่งงานวิจัยนี้ได้นำเสนอผลการวิเคราะห์ขอบเขตของการฉ้อโกงออนไลน์ที่ได้มีการกล่าวไว้ในกฎหมายและระเบียบข้อบังคับของอินโดนีเซีย รวมไปถึงการบังคับใช้กฎหมายโดยผู้มีอำนาจเพื่อจัดการการฉ้อโกงออนไลน์ การศึกษานี้ใช้การพิจารณาคดีเป็นบรรทัดฐานโดยใช้ข้อมูลตั้งต้นจากหนังสือ บทความต่าง ๆ เป็นต้น จากผลการศึกษาพบว่า มีความพยายามในการบังคับใช้กฎหมายเพื่อแก้ปัญหาการฉ้อโกงออนไลน์ในปัจจุบัน เพื่อให้สามารถดำเนินการได้ทั้งในเชิงการป้องกัน และปราบปราม

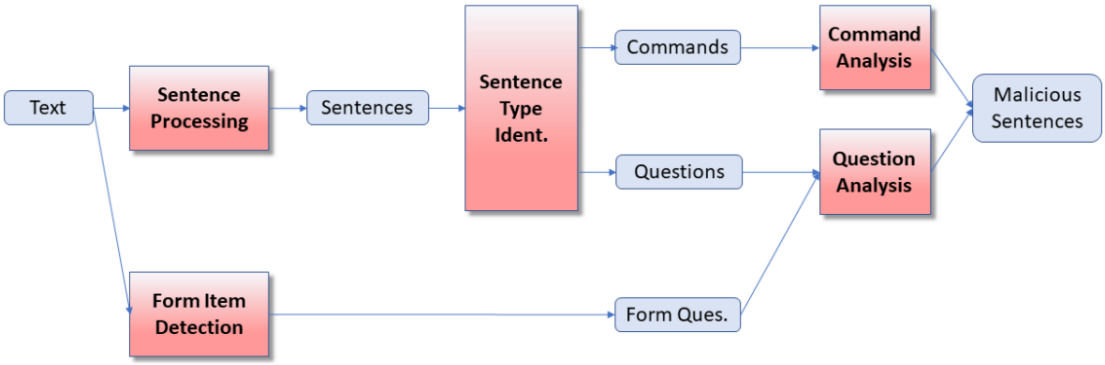
Ajayi (2019) ได้ทำการศึกษาเกี่ยวกับการหลอกลวงทางไซเบอร์ซึ่งพบมากในหมู่เยาวชนในเมืองของประเทศไนจีเรีย และกลายเป็นหนึ่งในภัยคุกคามด้านความปลอดภัยและเศรษฐกิจ โดยมีการจัดการและการพัฒนากลยุทธ์ในการสร้างกลุ่มธุรกิจที่ผิดกฎหมาย เพื่อหลบเลี่ยงการลงโทษจากผู้ที่เสียหายและหน่วยงานบังคับใช้กฎหมายระหว่างประเทศ โดยนักหลอกลวงทางไซเบอร์ในไนจีเรียได้คิดค้นวิธีการต่าง ๆ ทั้งกลยุทธ์ในการปรับใช้ในลักษณะภาษาสแลงและการจัดการทางธุรกรรมการเงิน และสังคม ในการศึกษานี้ผู้วิจัยได้รวบรวมข้อมูลด้วยการใช้เทคนิคทางภาษา โดยใช้แนวคิดทางภาษาท้องถิ่น ซึ่งสามารถตรวจสอบกลยุทธ์ทางภาษาที่นักหลอกลวงทางไซเบอร์ในประเทศไนจีเรียทางตะวันตกเฉียงใต้ใช้ในสื่อสังคมออนไลน์และความสัมพันธ์ทางธุรกรรมการเงิน ผลการวิจัยนี้แสดงให้เห็นถึงความสามารถในตรวจสอบภาษาที่แสดงถึงลักษณะของภาษาที่นักต้มตุ๋นในภูมิภาคใช้

Ali (2019) ได้ศึกษาเกี่ยวกับประเด็นของอาชญากรรมทางไซเบอร์และรวมรวบกิจกรรมอาชญากรรมไซเบอร์ที่ส่งผลต่อการเติบโตของภาคธุรกิจในคาบสมุทรอาหรับ (Gulf Countries Council: GCC) ข้อมูลของการวิจัยได้รวบรวมผ่านแบบสอบถาม การสำรวจจากพนักงานของธนาคารและจากประชาชนทั่วไป มีการอภิปรายเกี่ยวกับวิธีการเสริมสร้างมาตรการรักษาความปลอดภัยและปรับปรุงระดับความปลอดภัยของธนาคารออนไลน์ตลอดจนการเติบโตของธุรกิจในคาบสมุทรอาหรับ จากการศึกษาพบว่าอาชญากรรมไซเบอร์เป็นหนึ่งในประเด็นสำคัญที่ควรได้รับการจัดการอย่างเหมาะสมโดยอุตสาหกรรมการธนาคารและการเงิน เนื่องจากมีผลกระทบอย่างมากต่อสถาบันการเงินและองค์กรธุรกิจต่าง ๆ ในคาบสมุทรอาหรับ ซึ่งในการโจมตีทางไซเบอร์ในแต่ละปีทำให้ประเทศคาบสมุทรดังกล่าวสูญเสียมากถึง 1 พันล้านดอลลาร์ เพื่อเพิ่มความปลอดภัยให้มากขึ้น ดังนั้นจึงควรนำมาตรการความปลอดภัยมาใช้ ทั้งนี้องค์กรต้องเข้าใจเรื่องผลกระทบของอาชญากรรมไซเบอร์ทางการเงินและต้องตระหนักถึงภัยคุกคามออนไลน์ รวมถึงดำเนินการพิจารณามาตรการต่าง ๆ ที่ช่วยในการเสริมสร้างการรับรู้ของบุคคลากรในเรื่องความมั่นคงปลอดภัยและการรักษาสภาพแวดล้อมทางธุรกิจทางการเงินที่ยั่งยืน

Giri (2019) ได้นำเสนอบทวิเคราะห์ความมั่นคงปลอดภัยบนระบบเครือข่ายในด้านองค์ประกอบด้านต่าง ๆ ประกอบด้วย อาชญากรรมบนระบบเครือข่ายอินเทอร์เน็ต (Cyber Crime), การโจมตีหรือคุกคามผ่านระบบเครือข่ายอินเทอร์เน็ต (Cyber Threat), การวางกลยุทธ์ทางความปลอดภัยของระบบเครือข่ายอินเทอร์เน็ต (Cyber Security Cyber) และกฎหมายที่เกี่ยวกับระบบเครือข่ายอินเทอร์เน็ต (Cyber Law) ของประเทศเนปาล นอกจากนี้ ผลการศึกษาและสำรวจยังพบว่าความปลอยภัยในระบบเครือข่ายอินเทอร์เน็ตเป็นความสำคัญเกี่ยวกับความมั่นคงของชาติ ดังนั้นโครงการ e-Government จะเป็นแนวทางในการแก้ไขปัญหาดังกล่าว ซึ่งจะช่วยให้หน่วยงานภาครัฐช่วยจัดการภัยคุกคามในรูปแบบต่าง ๆ ได้ ซึ่งสหราชอาณาจักร (UK) ก็ได้มีการจัดตั้งสถานที่ดำเนินการรักษาความปลอดภัยภายในสำนักงานใหญ่ของสำนักงานรัฐมนตรี ในขณะที่นานาชาติส่วนใหญ่จะจัดตั้งส่วนงานดังกล่าวไว้ที่พื้นที่ข้างเคียงกับสำนักงานใหญ่ของกองทัพ

Kim et al. (2019) ได้ทำงานวิจัยเรื่องการป้องกัน ตรวจจับข้อมูล อัตโนมัติ จากผู้หลอกลวง การหลอกลวงหรือการโจมตีเพื่อให้ได้ซึ่งข้อมูลเป็นภัยคุกคามที่พบได้บ่อยและเป็นอันตรายอย่างยิ่งในปัจจุบัน โดยกลโกงมักส่งผลให้เกิดการสูญเสียทางการเงินโดยการโน้มน้าวให้เหยื่อกระทำการที่ไม่ได้รับคำแนะนำที่ดี เช่น การส่งเงิน หรือเกลี้ยกล่อมให้ส่งข้อมูลส่วนตัวไปให้ โดยในงานวิจัยนี้เป็นการนำเสนอวิธีการตรวจจับการหลอกลวง โดยเน้นที่การหลอกลวงที่ส่งถึงตัวบุคคล ทางโทรศัพท์ หรือทางข้อความ/ข้อความแชท โดยสร้างมือที่ชื่อว่า Scam Detection Assistant (SDA) ขึ้นมา ซึ่งจะทำการวิเคราะห์เนื้อหาการ

โจมตีเพื่อตรวจจับข้อความที่ไม่เหมาะสมที่เข้าข่ายการโจมตีข้อมูล ทำการเน้นไปที่ภาษาธรรมชาติที่ใช้ในการในการโจมตี ทำการวิเคราะห์เชิงความหมายของเนื้อหาเพื่อตรวจจับข้อความที่มีเจตนาที่ไม่ดี โดยมีโครงการการทำงานวิจัยดังรูปที่ 2-5

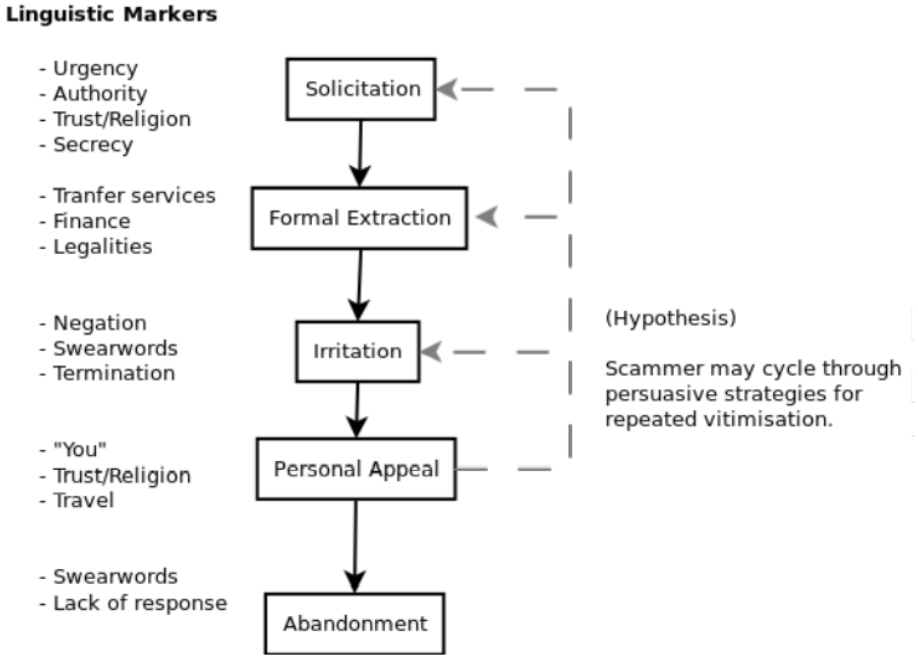


รูปที่ 2-5 โครงสร้างของ Scam Detection Assistant (SDA)

ในงานนี้ได้ใช้สคริปต์ของภาษา Python เป็นหลัก และใช้ภาษา Java เมื่อจำเป็นเพื่อเชื่อมต่อกับเครื่องมือเฉพาะ ในการประเมิน SDA เพื่อระบุอีเมลฟิชชิง ในงานวิจัยนี้ได้ใช้ชุดอีเมลฟิชชิ่งทั้งหมด 187,048 รายการข้อมูล แต่ลบออกไป 100,000 รายการข้อมูล โดย 100,000 รายการข้อมูลนั้นนำไปใช้สำหรับสร้างเป็นฐานข้อมูลที่จะใช้ในการตรวจสอบ คัดแยกข้อมูล ซึ่งจะเหลือ 87,048 รายการข้อมูล สำหรับนำมาประเมิน ผลการทำงานวิจัยพบว่า ความแม่นยำ (Precision) อยู่ที่ = 0.800 และเรียกคืน (Recall) = 0.650 งานวิจัยนี้จึงสรุปได้ว่า การทดสอบเกี่ยวกับอีเมลฟิชชิ่งแสดงให้เห็นว่าการใช้การตอบคำถามและความหมายแบบกริยา-อ็อบเจกต์ในรูปแบบที่เป็นประโยชน์ในการตรวจจับการหลอกลวง วิธีการ SDA สามารถตรวจจับการโจมตีแบบข้อความที่เป็นภาษาธรรมชาติได้

Ribaux and Souvignet (2020) ได้ทำงานวิจัยเรื่อง การจัดการกับการฉ้อโกงออนไลน์ ในการนำความรู้ทางวิทยาศาสตร์ทุกสาขามาประยุกต์ใช้เพื่อพิสูจน์ข้อเท็จจริง งานวิจัยนี้เกิดขึ้นสืบเนื่องจาก เมื่อวันที่ 6 สิงหาคม 2019 สมาชิกของกลุ่มโรงเรียนความยุติธรรมทางอาญา นิติวิทยาศาสตร์ และอาชญาวิทยาจำนวน 119 คน ที่มหาวิทยาลัยโลซาน ตกเป็นเป้าหมายของมิจฉาชีพออนไลน์ ด้วยการปลอมแปลงอีเมลในฐานะผู้อำนวยการโรงเรียนเพื่อพยายามชักชวนให้เหยื่อซื้อบัตรของขวัญทางระบบดิจิทัลและส่งรหัสการใช้บัตรไปยังผู้กระทำความผิด โดยบทความนี้ผู้เขียนคนแรกเป็นผู้อำนวยการโรงเรียน และผู้เขียนคนที่สองเป็นผู้เชี่ยวชาญด้านนิติวิทยาศาสตร์ดิจิทัลและเป็นศาสตราจารย์ของโรงเรียน ซึ่งทั้งสองคนทำงานร่วมกันแบบเรียลไทม์เพื่อจัดการกับการฉ้อโกงที่เกิดขึ้น โดยงานวิจัยนี้มีวัตถุประสงค์เพื่อดึงบทเรียนจากกรณีนี้จากหลากหลายมุมมองตั้งแต่นิติวิทยาศาสตร์ไปจนถึงความปลอดภัยทางไซเบอร์ รวมการแก้ไขปัญหาทั้งด้านภาคปฏิบัติไปจนถึงภาควิชาการ ผลการวิจัยจากเหตุการณ์นี้สามารถสรุป การตอบสนองต่อเหตุการณ์นี้ในทางปฏิบัติเป็น 4 ขั้นตอนดังนี้ 1) ตรวจจับการฉ้อโกง 2) จัดการภาวะวิกฤต 3) วิเคราะห์หลังเหตุการณ์ และ 4) รายงานข้อมูลให้ทุกคนรับทราบ เพื่อพัฒนาแบบเป็นจำลองการทำงานแบบเรียลไทม์ที่มีประสิทธิภาพโดยพัฒนาเป็นนวัตกรรมใหม่สำหรับการป้องกัน ตรวจจับ วิเคราะห์ สอบสวน และตอบสนองต่อการฉ้อโกงทางออนไลน์ ในอนาคตเกิดขึ้น

Edwards et al., (2017) ได้ทำงานวิจัยเรื่อง การตรวจจับการชักชวนโดยอัตโนมัติของมิจฉาชีพออนไลน์ในการฉ้อโกงค่าธรรมเนียม โดยบทความนี้ ได้ทำการให้ตัวเองตกเป็นเป้าหมายเพื่อให้เป็นเหยื่อของมิจฉาชีพออนไลน์ ซึ่งสมาชิกที่จงใจตกเป็นเหยื่อของมิจฉาชีพออนไลน์ตั้งใจทำให้มิจฉาชีพเสียเวลาเพื่อดูกลยุทธ์ของการหลอกล่อของมิจฉาชีพ ตรวจสอบดูวิธีการใช้คำพูดในการโน้มน้าวใจของมิจฉาชีพออนไลน์เมื่อเหยื่อตอบโต้คุยด้วย สังเกตวิธีการเพื่อหลวงลวงของมิจฉาชีพ ซึ่งจากการวิจัยสามารถสรุปกระบวนการโน้มน้าวมิจฉาชีพออนไลน์ได้ดังภาพที่ 2-6



รูปที่ 2-7 กระบวนการโน้มน้าวมิจฉาชีพออนไลน์

เริ่มต้นจากมีการชักจูง เชิญชวนในรูปแบบต่าง ๆ เช่น ส่งข้อความเชิงมีเรื่องเร่งด่วน ส่งข้อความเชิงข่มขู่โดยอ้างผู้มีอำนาจ ส่งข้อความทางด้านความเชื่อ/ศาสนา และส่งข้อความเชิงบอกว่าเป็นความลับ จากนั้นทำการประเมินเหยื่อในการหลอกลวงในรูปแบบของมิจฉาชีพที่วางแผนเอาไว้เช่นในรูปแบบ การบริการรับส่ง การเงิน กฎหมาย ต่าง ๆ จากนั้นเพิ่มความความฉุนเฉียวในการสนทนาขึ้นเพื่อให้เหยื่อเกิดการทำตามให้มากที่สุด จากนั้นสังเกตปฏิกิริยาของเหยื่อถ้าเหยื่อจะหลุดมือ จะใช้มีการใช้คำพูดออกแบบนี้เพื่อดึงให้เหยื่อเข้าไปในกระบวนใหม่ แต่ถ้าเห็นแล้วเหยื่อไม่ทำตามเป็นแน่แท้แล้วก็จะทำการปล่อยเหยื่อคนนั้นไป

Shaari et al., (2019) ได้ทำงานวิจัยเกี่ยวกับกลโกงหาคู่ออนไลน์ในมาเลเซียโดยทำการวิเคราะห์บทสนทนาออนไลน์ระหว่างมิจฉาชีพออนไลน์และเหยื่อ งานวิจัยนี้เป็นการทำงานวิจัยเพื่อระบุขั้นตอนและกลยุทธ์ที่เกี่ยวข้องกับการหลอกลวงเรื่องรัก ๆ ใคร่ ๆ ทางออนไลน์ในมาเลเซียเป็นหลัก นอกจากนั้นยังมีจุดมุ่งหมายเพื่อระบุรูปแบบของภาษาหลอกลวงที่ใช้ในการหลอกลวงเรื่องรัก ๆ ใคร่ ๆ ทางออนไลน์ในมาเลเซียผ่านการวิเคราะห์ทางภาษาที่ครอบคลุมของการสนทนาออนไลน์ที่เกิดขึ้นจริงระหว่างมิจฉาชีพออนไลน์และเหยื่อ ข้อมูลที่ใช้ได้จากฐานข้อมูลกรมตำรวจมาเลเซียคดีหลอกลวงเรื่องรัก ๆ ใคร่ ๆ ที่ได้เกิดขึ้นมาทำการรวบรวม โดยใช้ข้อมูลจากฐานข้อมูล 30 ชุดของการสื่อสารออนไลน์ระหว่างมิจฉาชีพออนไลน์กับเหยื่อชาวมาเลเซีย 30 คนโดยใช้วิธีวิเคราะห์เนื้อหา วิเคราะห์โดยใช้แบบจำลอง Brown และ

Levinson Politeness Model รวมถึงใช้ Scammers Persuasive Techniques Model ของ Whitty's ผลการวิจัยชี้ให้เห็นรูปแบบการหลอกลวงและรูปแบบการสนทนาทางภาษาของมิจฉาชีพออนไลน์ในการเกลี้ยกล่อมและหลอกลวงเหยื่อ ซึ่งงานวิจัยนี้สรุปได้ทั้งหมด 3 กลยุทธ์ และ 16 วิธีการขั้นตอนในการหลอกลวงเหยื่อดังนี้

กลยุทธ์ที่ 1 การติดต่อและสร้างความสัมพันธ์

กลยุทธ์ที่ 2 การสร้างความไว้วางใจและพัฒนาความสัมพันธ์ส่วนตัว

ขั้นตอนที่ 1 อ้างสิทธิ์ในข้อมูลพื้นฐานของมิจฉาชีพออนไลน์แสดงความคล้ายคลึงกันระหว่างมิจฉาชีพกับเหยื่อที่เป็นเป้าหมาย

ขั้นตอนที่ 2 มิจฉาชีพออนไลน์จะแจ้งและปฏิบัติตามความสนใจและความต้องการของเหยื่อ

ขั้นตอนที่ 3 มิจฉาชีพออนไลน์แสดงความกังวลเกี่ยวกับความต้องการและความต้องการของเหยื่อ

ขั้นตอนที่ 4 มิจฉาชีพออนไลน์พูดเกินจริงเพื่อดึง ความสนใจ/ความเห็นอกเห็นใจ/การอนุมัติ ต่อเหยื่อ

ขั้นตอนที่ 5 มิจฉาชีพออนไลน์เพิ่มความสนใจให้กับเหยื่อ

ขั้นตอนที่ 6 มิจฉาชีพออนไลน์สร้างข้อเสนอที่น่าสนใจ

ขั้นตอนที่ 7 มิจฉาชีพออนไลน์แสดงการกระทำของการอยู่ร่วมกันโดยรวมเหยื่อไว้ในแผนการในอนาคตของมิจฉาชีพออนไลน์

ขั้นตอนที่ 8 มิจฉาชีพออนไลน์เรียกร้องเหตุผลหรือให้เหตุผลในการกระทำของมิจฉาชีพออนไลน์

ขั้นตอนที่ 9 มิจฉาชีพออนไลน์ระบุว่าต้องการให้เหยื่อผูกมัดตัวเองให้ทำอะไรบางอย่างกับตัวมิจฉาชีพออนไลน์

ขั้นตอนที่ 10 มิจฉาชีพออนไลน์เสนอของขวัญที่น่าสนใจ

ขั้นตอนที่ 11 ทั้งผู้มิจฉาชีพออนไลน์และเหยื่อแสดงความเห็นอกเห็นใจ ความเข้าใจ ความร่วมมือซึ่งกันและกัน

ขั้นตอนที่ 12 มิจฉาชีพออนไลน์สวมบทบาทเป็นตัวละครอื่น (ผู้มีอำนาจ ทนายความ และตำรวจ) เพื่อเสนอข้อแนวทางใหม่โดยมีเงินมาเกี่ยวข้อง

กลยุทธ์ที่ 3 การรักษากลโกง ใช้เหยื่อล่อ และการมีเหตุที่ทำให้ชีวิตเดือดร้อน

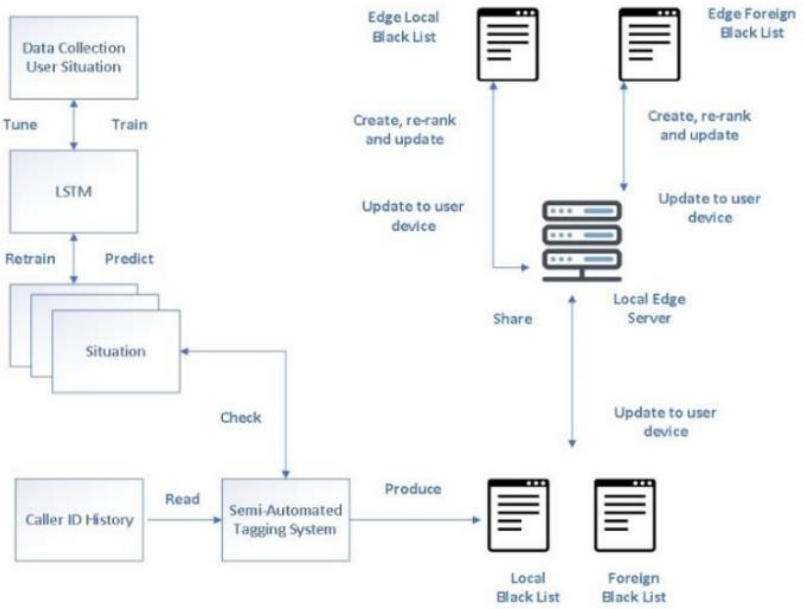
ขั้นตอนที่ 13 คำสั่งและคำขอ: มิจฉาชีพออนไลน์ระบุความต้องการให้เหยื่อทำหรือหลีกเลี่ยงการทำบางสิ่ง

ขั้นตอนที่ 14 คำแนะนำและ/หรือคำแนะนำ: มิจฉาชีพออนไลน์เกลี้ยกล่อมให้เหยื่อทำตามที่บอก

ขั้นตอนที่ 15 การส่งการเตือน: มิจฉาชีพออนไลน์เตือนหรือระบุว่าเหยื่อควรจำไว้ว่าให้ทำอะไรบางอย่าง

ขั้นตอนที่ 16 ภัยคุกคาม คำเตือน กล้า: มิจฉาชีพออนไลน์ระบุว่าจะดำเนินการบางอย่างหากผู้ที่ตกเป็นเหยื่อปฏิเสธที่จะทำบางสิ่ง

Yu et al., (2020) ได้ทำงานวิจัยเรื่อง การใช้ Edge Computing ในสถานการณ์ต่าง ๆ ที่ช่วยให้จัดหาตรวจสอบ จัดเก็บ เป็นระบบบัญชีดำในการระบุเลขโทรศัพท์ของมิจฉาชีพออนไลน์ได้อย่างมีประสิทธิภาพ ซึ่งวิธีการแบบดั้งเดิมในการตรวจหาเบอร์โทรศัพท์ในการทำกิจกรรมต้องอาศัยการสร้างระบบหมายเลขบัญชีดำ อย่างไรก็ตาม อาชญากรสามารถปลอมแปลงหมายเลขโทรศัพท์ของตนได้อย่างง่ายเพียงแค่เปลี่ยนหมายเลขผ่าน VoIP (Voice over IP) หรือใช้หมายเลขโทรศัพท์มือถือเสมือน (VMN) ที่มีราคาค่อนข้างต่ำ การตรวจสอบ ID ที่หละหลวมในระบบอัตโนมัติของ API ระดับสูง โดยในบทความนี้นำเสนอแนวทางใหม่ที่ใช้สถานการณ์ได้ในการขึ้นบัญชีดำหมายเลขโทรศัพท์ที่ไม่ต้องการ ในขณะที่ยังคงอัตราการตรวจจับสูงผ่านการจัดหาฝูงชนแบบกระจาย (Distributed crowd sourcing) โดยระบบที่พัฒนาขึ้นประกอบด้วย 2 ส่วน 1) ส่วนแรกเป็นระบบรวบรวมกำหนดการรายวันของผู้ใช้ในอนุกรมเวลาเป็นข้อมูลตามสถานการณ์และใช้ข้อมูลเพื่อฝึก Long Short Term Memory (LSTM) ออกมาเป็นโมเดลการเรียนรู้เชิงลึก เพื่อทำนายสถานการณ์ของผู้ใช้ในอนาคตเราใช้แอปพลิเคชันการแท็กแบบกึ่งอัตโนมัติเพื่อแท็กสายเรียกเข้าแต่ละรายการโดยอ่านประวัติการโทรเทียบกับสถานการณ์ที่คาดการณ์ไว้ หมายเลขโทรศัพท์ที่เป็นอันตรายจะโดนติดแท็กว่าอันตรายหากอยู่ในสถานการณ์ที่ไม่ถูกต้องหรืออาจเป็นอันตรายกับระบบส่วนอื่น ๆ 2) ส่วนที่สอง Distributed crowd sourcing ใช้เพื่อรวมหมายเลขโทรศัพท์ที่มีอันดับเป็นอันตรายต่ออุปกรณ์ต่าง ๆ เมื่อมีการสร้างบัญชีดำระดับ ก็จะมีการอัพเดตรายการในเครื่องโดยเผยแพร่กลับไปยังอุปกรณ์ของผู้ใช้ปลายทางด้วยบัญชีดำ edge local และ edge foreign blacklist จากการการประเมินระบบซึ่งใช้การประเมินโดยการใช้เบอร์โทรศัพท์โทรเข้าไปจริง ผลการวิจัยพบว่าการออกแบบสามารถมีอัตราการตรวจจับอยู่ในเกณฑ์ที่เหมาะสม ภาพที่ 2-8 เป็นเวิร์คโฟลว์รายละเอียดและส่วนประกอบของระบบ



ภาพที่ 2-8 เวิร์คโฟลว์รายละเอียดและส่วนประกอบของระบบ

Retnowinarni (2020) ได้ทำการศึกษาเกี่ยวกับกฎหมายที่เกี่ยวข้องกับการทำธุรกรรมผ่านสื่อออนไลน์ซึ่งอาศัยความไว้วางใจซึ่งกันและกันระหว่างผู้ขายและผู้ซื้อ โดยการศึกษานี้ครอบคลุมกฎหมายที่

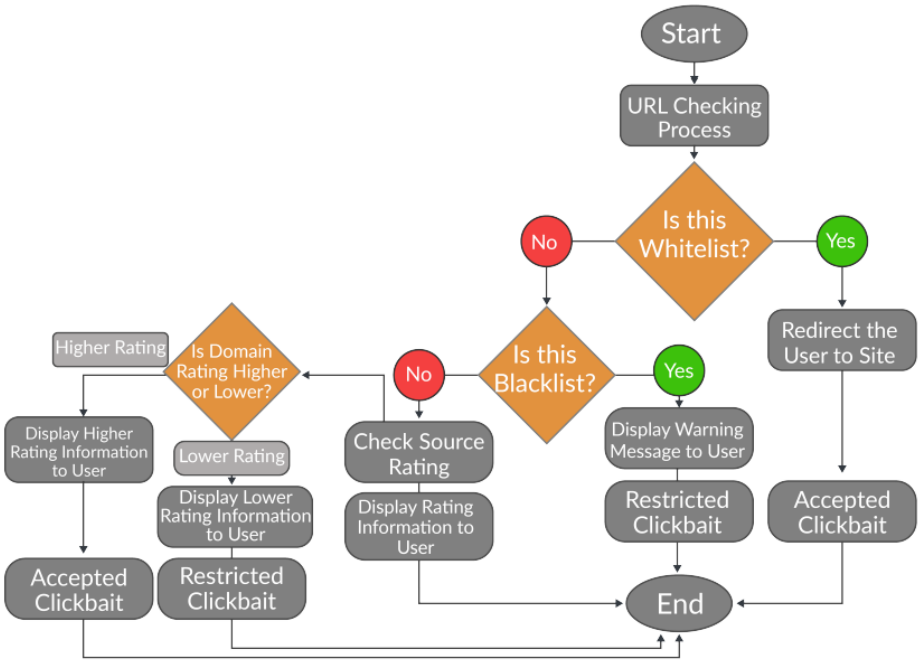
ให้การรับรองสิทธิและหน้าที่ของทั้งสองผู้ซื้อและผู้ขายสินค้าออนไลน์ ตลอดจนกฎหมายอาญาและกฎหมายอื่น ๆ เช่น กฎหมายที่เกี่ยวข้องกับการคุ้มครองผู้บริโภค ในประเทศอินโดนีเซีย จากการศึกษาผู้วิจัยได้สรุปประเด็นสำคัญเกี่ยวกับนโยบายกฎหมายอาญาต่อผู้กระทำผิดเกี่ยวกับการซื้อขายสินค้าออนไลน์ว่า ได้รับการควบคุมและคุ้มครองจากกฎหมายเกี่ยวกับข้อมูลและธุรกรรมทางอิเล็กทรอนิกส์ที่ได้มีการออกไว้แล้ว แต่ยังสามารถใช้ประมวลกฎหมายอาญาโดยเครื่องมือในการดำเนินคดีที่เกี่ยวข้องกับอาชญากรรมทางไซเบอร์ได้ นอกจากนี้ยังสามารถใช้กฎหมายคุ้มครองผู้บริโภคในการพิจารณาคดีได้ด้วย ในกระบวนการบังคับใช้กฎหมายอาญาสำหรับการฉ้อโกงทางออนไลน์นั้น ผู้เสียหายสามารถการแจ้งต่อเจ้าหน้าที่ตำรวจพร้อมด้วยหลักฐานเบื้องต้น จากนั้นตำรวจจะรวมรวมพยานหลักฐาน ตลอดจนเอกสารอิเล็กทรอนิกส์ต่าง ๆ ที่นอกเหนือจากเอกสารหลักฐานตามประมวลกฎหมายอาญาปกติ เพื่อดำเนินคดี อย่างไรก็ตาม อุปสรรคที่ผู้บังคับใช้กฎหมายประสบในการทำธุรกรรมออนไลน์ก็คือการค้นหาตำแหน่งหรือที่อยู่ของผู้กระทำผิด

Jakhrani และ Mastoi (2020) ได้ทำการศึกษาบทบาทของศาลคุ้มครองผู้บริโภคในประเทศปากีสถานที่จัดตั้งขึ้นภายใต้พระราชบัญญัติคุ้มครองผู้บริโภค (2014) เพื่อศึกษาว่าระบบกฎหมายนี้สามารถปกป้องสิทธิของผู้บริโภคออนไลน์ในจังหวัด Sindh ได้อย่างไรบ้าง โดยการศึกษานี้ดำเนินการผ่านการสัมภาษณ์อย่างละเอียด และมีการใช้แบบสอบถามร่วมด้วย การสำรวจและเก็บข้อมูลจัดทำขึ้นในเมืองต่าง ๆ ของจังหวัด Sindh โดยมีผู้ตอบแบบสอบถามกลับ 43 คน ซึ่งประกอบด้วยผู้พิพากษา 15 คนและทนายความ 28 คน ผลการศึกษาสามารถชี้ให้เห็นได้ว่า ศาลคุ้มครองผู้บริโภคสามารถทำงานได้อย่างถูกต้องและพิสูจน์ความยุติธรรมต่อสาธารณชนในจังหวัด Sindh ได้ตามกฎหมาย อย่างไรก็ตามผู้บริโภคออนไลน์จำเป็นให้ความสำคัญและเพิ่มความตระหนักรู้เกี่ยวกับการซื้อขายสินค้าออนไลน์ ตลอดจนการศึกษาเกี่ยวกับสิทธิของผู้บริโภคเพื่อปกป้องตนเอง

Iqbal และคณะ (2021) ได้ทำการศึกเกี่ยวกับอาชญากรรมทางไซเบอร์โดยทำการศึกษาในประเทศอินโดนีเซีย เกี่ยวกับพัฒนาการของอาชญากรรมไซเบอร์ และประเด็นต่าง ๆ ที่เกี่ยวข้อง ตลอดจนกฎหมายที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ และตัวอย่างการเกิดอาชญากรรมไซเบอร์ในอินโดนีเซีย นอกจากนี้ยังได้ทำการศึกษาข้อมูลทุติยภูมิจากหนังสือและบทความที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ ซึ่งจากการศึกษาดังกล่าวได้มีการแบ่งประเภทการก่ออาชญากรรมไซเบอร์ในอินโดนีเซียออกมาได้มากว่า 10 ประเภท โดยพบว่าการฉ้อโกงเป็นอาชญากรรมไซเบอร์ที่พบมากที่สุดและมากกว่าอาชญากรรมไซเบอร์หรืออาชญากรรมออนไลน์ประเภทอื่นอย่างชัดเจน

Dempere และ Malik (2021) ได้ทำการศึกษาเกี่ยวกับการฉ้อโกงทางการเงินของผู้บริโภคในประเทศสหรัฐอาหรับเอมิเรตส์ โดยใช้วิธีการสำรวจข้อมูลจากทั้งนักเรียนนักศึกษา เจ้าหน้าที่และอาจารย์และศิษย์เก่า จากสถาบันการศึกษาแห่งหนึ่ง ที่ตอบคำถามในแบบสำรวจครบ จำนวน 1,631 คน (จากทั้งหมดที่ได้สอบถามเป็นจำนวน 3,299 คน) แล้วพบว่า ผู้ที่ตกเป็นเหยื่อของการฉ้อโกงทางการเงินมีแนวโน้มที่จะมีอายุมากขึ้น โดยเป็นผู้ที่มีการศึกษาระดับมัธยมศึกษาที่มากขึ้นและมียอดบัตรเครดิตรายเดือนสูง เมื่อวิเคราะห์ความน่าจะเป็นของนักเรียนที่จะกลายเป็นเหยื่อการฉ้อโกงทางการเงินพบว่าสำหรับเหยื่อที่เป็นนักเรียนนักศึกษาพบว่าอายุเป็นปัจจัยสำคัญที่เกี่ยวข้องกับการถูกฉ้อโกง อย่างไรก็ตามเมื่อวิเคราะห์ตัวอย่างย่อยของผู้ตอบแบบสอบถามทั้งหมดพบว่า ยอดคงเหลือในบัตรเครดิตเป็นปัจจัยที่มีความสัมพันธ์เชิงบวกและมีนัยสำคัญกับโอกาสหรือความน่าจะเป็นที่จะตกเป็นเหยื่อของการฉ้อโกงทางการเงิน

Razaque et al., (2022) ได้ทำงานวิจัยเรื่อง การตรวจจับ Clickbait โดยใช้ Deep Recurrent Neural Network โดยทั่วไปผู้ที่ใช้โซเชียลเน็ตเวิร์กมักจะตกเป็นเหยื่อของ Clickbait จากมิจฉาชีพออนไลน์ เนื่องจากพวกมิจฉาชีออนไลน์พยายามสร้างพาดหัวข่าวที่ดึงดูดให้ผู้ใช้ส่วนใหญ่คลิกลิงก์ที่แนบมา เมื่อผู้ที่ใช้โซเชียลเน็ตเวิร์กหลงเชื่อคลิกลิงก์ที่สร้างขึ้นเส้นทางในการเข้าถึงข้อมูลจะถูกเปลี่ยนเป็นเส้นทางไปยังแหล่งข้อมูลที่เป็นการฉ้อโกงโดยจะทำการขโมยข้อมูลส่วนตัวของเหยื่อออกมา เพื่อป้องกันปัญหานี้ที่เกิดขึ้นในงานวิจัยนี้ มีการเสนอส่วนขยายเบราว์เซอร์ใหม่ชื่อ ClickBaitSecurity เพื่อช่วยในการประเมินความปลอดภัยของลิงก์ ส่วนขยายนี้จะใช้อัลกอริธึมการค้นหารายการที่ถูกต้องและผิดกฎหมาย (Legitimate and illegitimate list search: LILS) และอัลกอริธึมการตรวจสอบอันดับโดเมน (Domain rating check: DRC) โดยอัลกอริธึมทั้งสองนี้จะเป็นการรวมคุณลักษณะการค้นหาแบบไบนารีเพื่อตรวจจับเนื้อหาที่เป็นอันตรายได้อย่างรวดเร็วและมีประสิทธิภาพยิ่งขึ้น นอกจากนี้ ClickBaitSecurity ยังใช้ประโยชน์จากคุณสมบัติของเครือข่ายประสาทเทียมแบบลึก (Deep recurrent neural network: RNN) ซึ่งจากทำงานวิจัยพบว่า โซลูชัน ClickBaitSecurity ที่เสนอมีความแม่นยำมากขึ้นในการตรวจหาลิงก์ที่เป็นอันตรายและปลอดภัย เมื่อเทียบกับโซลูชันที่มีอยู่ ซึ่งกระบวนการทำงานดังรูปที่ 2-9



รูปที่ 2-9 ขั้นตอนการวิเคราะห์ clickbait

รูปที่ 2-9 เป็นขั้นตอนการวิเคราะห์ clickbait เริ่มต้นทำการประมวลวิเคราะห์ตรวจสอบ URL ว่าเป็น Whitelist หรือไม่ (ในงานวิจัยนิยามคำว่า Whitelist และ Blacklist ไว้ดังนี้ Whitelist คือ เว็บไซต์นั้นเป็นเว็บไซต์ใน List ที่ปลอดภัยอนุญาตให้เข้าถึง ในส่วนของ Blacklist นั้นจะเป็นเว็บไซต์ที่ทำ List เอาไว้ว่าเป็นเว็บไซต์ที่หลอกลวงของมิจฉาชีพออนไลน์ที่ทำการกำจัด URL นั้นทิ้งไม่ได้เหยื่อสามารถคลิกได้) ถ้าเมื่อตรวจสอบว่าเป็น Whitelist ก็จะสามารถเข้าถึงเว็บไซต์นั้น ๆ ได้ แต่ถ้าไม่ใช่ให้ไปให้ไปตรวจสอบว่า Blacklist หรือไม่ถ้าใช่ให้กำจัดทิ้ง ถ้าไม่ใช่ตรวจสอบและให้คะแนนผู้ใช้ตัดสินใจรวมถึงแสดงข้อมูลการให้คะแนนแก่ผู้ใช้ ถ้าไม่มั่นใจอีกให้ไปที่คะแนนของ Domain ว่ามีคะแนนสูงหรือต่ำ ถ้าคะแนน

Domain ต่ำ แสดงข้อมูลการให้คะแนนที่ต่ำกว่าให้กับผู้ใช้แล้วกำจัดเว็บไซต์นั้นทิ้ง แต่ถ้าคะแนน Domain นั้นสูง ก็แสดงข้อมูลการให้คะแนนให้กับผู้ใช้แล้วใช้งานเว็บไซต์นั้นได้ ซึ่งทั้งหมดเป็นกระบวนการ clickbait ของงานวิจัยนี้

บรรณานุกรม

กรกนก นิลดำ, เสริมศิริ นิลดำ, อิงดอย ศรีลาพัฒน์, ภควัฒน์ สวนงาม, วรักษณ์กมล มงคลอัศศิริ และ ปฐมพร ปัญญะติ, “วิธีการกลโกง ช่องทางการสื่อสาร และประสบการณ์ในการถูก มิจฉาชีพออนไลน์หลอกลวงของผู้สูงอายุ ในจังหวัดเชียงราย,” CRRU Journal of Communication Chiang Rai Rajabhat University., Vol. 3(3), pp. 50–67, 2563.

ฐิติมา อินกล่ำ, “วาทกรรมทางการสื่อสารเพื่อการหลอกลวงทำธุรกรรมทางการเงินออนไลน์ ผ่านเครื่องอิเล็กทรอนิกส์,” Academic Journal Uttaradit Rajabhat University., Vol. 11(2), pp. 86-100, 2559.

ณัฏฐกาญจน์ ศุกลรัตนเมธี และ นุชประภา โมกข์ศาสตร์, “การรู้เท่าทันสื่อสังคมออนไลน์ของเยาวชนเพื่อการเป็นพลเมืองในสังคมประชาธิปไตย,” สำนักวิจัยและพัฒนา สถาบันพระปกเกล้า, กันยายน 2562.

ณัฐณิชา คุ้มแพทย์, “การละเมิดสิทธิความเป็นส่วนตัวและสิทธิในชื่อเสียงโดยการประจาน ในพื้นที่ซื้อขายสินค้าออนไลน์,” CMU Journal of Law and Social Sciences., Vol. 13(1) pp. 24-53, 2563.

ณัฐธรณ์ เดชสกุล และ จอมเดช ตรีเมฆ, “ปัญหาการฉ้อโกงซื้อขายสินค้าทางอินเทอร์เน็ตในประเทศไทย,” งานประชุมวิชาการระดับชาติมหาวิทยาลัยรังสิตประจาปี 2563., pp. 1141-1151, 1 พฤษภาคม 2563

พิมลพรรณ บุญยะเสนา และ สุขุม พันธุ์ณรงค์, “การวิเคราะห์พฤติกรรมการใช้จ่ายเงินของเด็กและเยาวชนที่ติดเกม: กรณีศึกษาเยาวชนในพื้นที่จังหวัดเชียงใหม่และลำพูน,” วารสารศรีนครินทรวิโรฒวิจัยและพัฒนา (สาขามนุษยศาสตร์และสังคมศาสตร์)., Vol. 3(5), pp. 51-62, 2554.

พิรุฬห์รัตน์ ศรีแจ่ม และ ธันย์พันธ์ ใคร้วานิช, “กลโกงการทำธุรกรรมทางการเงินในยุคดิจิทัล,” การประชุมวิชาการระดับชาติครั้งที่ 15 และเครือข่ายวิจัยประชำชื่น ครั้งที่ 5 โลกไร้พรมแดน : ทิศทางการศึกษา สุขภาวะ และนวัตกรรม., วิทยาลัยครุศาสตร์ร่วมกับสายงานวิจัยและพัฒนา มหาวิทยาลัยธุรกิจบัณฑิตย์, 20 มีนาคม 2563.

มูลนิธิแม่ฟ้าหลวง ในพระบรมราชูปถัมภ์, “รูปแบบโกงออนไลน์ 2564” สืบค้นออนไลน์ เมื่อวันที่ 27 พฤษภาคม 2564, https://home.maefahluang.org/17623530/new-normal-phising

สถาบันดำรงราชานุภาพ กระทรวงมหาดไทย, “รูปแบบ/พฤติกรรมการหลอกลวงในปัจจุบัน ใช้ประกอบในการลงพื้นที่ครั้งที่ ๒ ของทีมขับเคลื่อนฯ ระดับตำบล ป้องกันไม่ให้ประชาชนถูกหลอกในรูปแบบต่างๆ โดยเชื่อมโยง ประเด็นความรู้หัวข้อ วิถีไทย วิถีพอเพียง และรู้สิทธิรู้หน้าที่ รู้กฎหมาย” สถาบันดำรงราชานุภาพ สำนักงานปลัดกระทรวงมหาดไทย กระทรวงมหาดไทย, ๒๑ มีนาคม ๒๕๖๑. http://www.stabundamrong.go.th/web/thainiyom/deceive.pdf

สลิลพร อิศรางกูร ณ อยุธยา, “แนวทางการป้องกันการหลอกลวงให้โอนเงิน: ศึกษากรณีธุรกิจขนาดกลางและขนาดเล็ก” ศิลปศาสตรมหาบัณฑิต สาขาวิชานิติเศรษฐศาสตร์ คณะนิติศาสตร์และคณะเศรษฐศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2561.

ดี.พี.ลอว์ แอนด์ เซอร์วิส จำกัด. (2562). *พระราชบัญญัติการเล่นแชร์ พ.ศ.2534*. Retrieved May 10, 2021, From https://dplawandservice.com/2019/09/พระราชบัญญัติการเล่นแช/

ประชาชาติธุรกิจ. (2563). *“พีชพชร” ใช้ พรบ.คอมพิวเตอร์ เอาผิดคนแฮกไอจี*. Retrieved May 10, 2021, From https://today.line.me/th/v2/article/K89JaR

ปุณิกา และ ปริยานุช. (2560). *พระราชบัญญัติห้ามเรียกดอกเบี้ยเกินอัตราพ.ศ. ๒๕๖๐*. Retrieved May 10, 2021, From http://web.krisdika.go.th/data/law/law2/%CB04/%CB04-20-2560-a0001.htm

มนตรี สีทอง. (2564). *ระบบสารสนเทศสำนักงานตำรวจแห่งชาติ*. Retrieved May 10, 2021, From https://www.police9.go.th/media/documents/summary-crimes.pdf

ราชกิจจานุเบกษา. (2560). *พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐*. Retrieved May 10, 2021, From http://www.ratchakitcha.soc.go.th/DATA/PDF/2560/A/010/24.PDF

สถาบันนิติธรรมาลัย. (2564). *หมวด ๓ ความผิดฐานฉ้อโกง (มาตรา ๓๔๑ – ๓๔๘)*. Retrieved May 10, 2021, From https://www.drthawip.com/criminalcode/1-53

สำนักงานกฎหมายทนายความกอบเกียรติ. (2562). *คดีมโนสาเร่ เป็นอย่างไร*. Retrieved May 10, 2021, From https://www.kobkiat.com/17382923/คดีมโนสาเร่-เป็นอย่างไร

สุรพงษ์ ชัยจันทร์. (2561). *การปฏิบัติงานเชิงรุกเพื่อการป้องกนัอาชญากรรมตำรวจภูธรภาค 7*. Retrieved May 10, 2021, From http://www.dsdw2016.dsdw.go.th/doc_pr/ndc_2560-2561/PDF/8575s/รวม.pdf

Wichianlaw. (2561). *ทนายความและที่ปรึกษากฎหมาย*ลิขสิทธิ์. Retrieved May 10, 2021, From https://wichianlaw.blogspot.com/2018/05/blog-post_8.html

Edwards, M., Peersman, C., Rashid, A., & Lancaster, S. (2017). Scamming the scammers: Towards automatic detection of persuasion in advance fee frauds. 26th International World Wide Web Conference 2017, WWW 2017 Companion, 1291–1299.

Kim, M., Song, C., Kim, H., Park, D., Kwon, Y., Namkung, E., Harris, I. G., & Carlsson, M. (2019). Scam detection assistant: Automated protection from scammers. 2019 1st International Conference on Societal Automation, SA 2019, 1–8.

Razaque, A., Alotaibi, B., Alotaibi, M., Hussain, S., Alotaibi, A., & Jotsov, V. (2022). Clickbait Detection Using Deep Recurrent Neural Network. Appl. Sci. 12, 504, 1-19 https://doi.org/10.3390/app12010504

Ribaux, O., & Souvignet, T. R. (2020). "Hello are you available?" Dealing with online frauds and the role of forensic science. Forensic Science International: Digital Investigation, 33, 300978. https://doi.org/10.1016/j.fsidi.2020.300978

Shaari, A. H., Kamaluddin, M. R., Paizi Fauzi, W. F., & Mohd, M. (2019). Online-dating romance scam in Malaysia: An analysis of online conversations between scammers and victims. GEMA Online Journal of Language Studies, 19(1), 97–115. https://doi.org/10.17576/gema-2019-1901-06

Yu, C. Y., Chang, C. K., & Zhang, W. (2020). An Edge Computing Based Situation Enabled Crowdsourcing Blacklisting System for Efficient Identification of Scammer Phone Numbers. Proceedings - 2020 International Conference on Computational Science

and Computational Intelligence, CSCI 2020, 776–781.
https://doi.org/10.1109/CSCI51800.2020.00146

บทที่ 3
ข้อมูลเกี่ยวกับผู้เสียหาย

ในปัจจุบันสภาพสังคมมีความสลับซับซ้อนมาก อาชญากรรมประเภทฉ้อโกงมีความสลับซับซ้อนมากขึ้นตามไปด้วย ถึงแม้ว่าการฉ้อโกงในบางรูปแบบอาจจะมีลักษณะคล้ายคลึงกันกับที่เคยปรากฏในอดีตเมื่อหลายสิบปีก่อน แต่ก็มีการสร้างเครือข่ายองค์กรอาชญากรรม หรือนำเทคโนโลยีสารสนเทศมาใช้ในการฉ้อโกง ซึ่งจะทำให้มีชาวบ้านที่ไม่รู้เท่าทัน ก็จะหลงเชื่อและตกเป็นผู้ถูกหลอกลวงมากขึ้น ในบทนี้คณะผู้วิจัยจึงขอกล่าวถึง รูปแบบการฉ้อโกงที่เกี่ยวข้องกับโครงการนี้ รวมถึงวิเคราะห์สถิติต่าง ๆ ที่เกี่ยวข้องกับคดีฉ้อโกงออนไลน์จากแหล่งข้อมูลที่รวบรวมได้

3.1 รูปแบบการกระทำความผิด

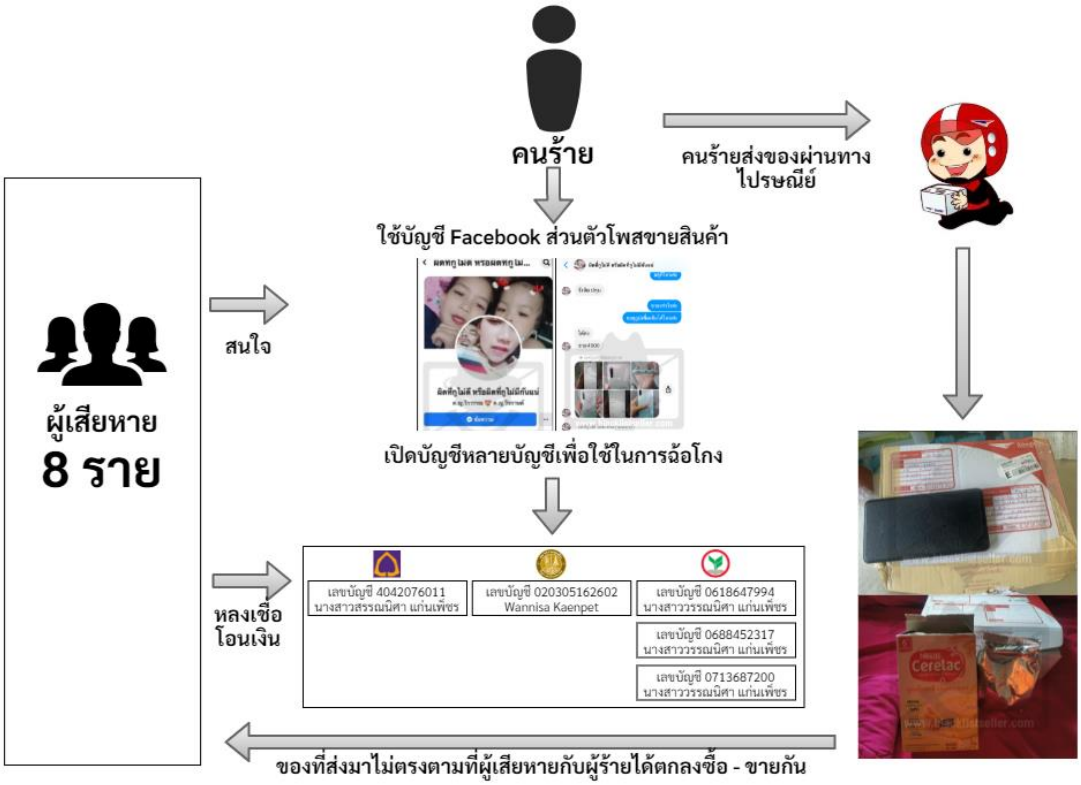
โครงการนี้ มุ่งเน้นศึกษาการฉ้อโกงออนไลน์ที่ครอบคลุมรูปแบบการกระทำความผิดดังต่อไปนี้

3.1.1 การซื้อขายตามเว็บประกาศขายผ่านทางสื่อสังคมออนไลน์ต่างๆ เช่น เฟสบุ๊ก อินสตราแกรม ไลน์ หรือการทำธุรกรรมอื่น ๆ ทางออนไลน์ แล้วไม่ได้รับสินค้าตามกำหนด

กรณีนี้ เป็นเคสที่มีผู้เสียหายมากที่สุด โดยมิจฉาชีพส่วนใหญ่นิยมใช้เป็นจำนวนมาก โดยจะอาศัยการประกาศสินค้าผ่านช่องทางสื่อสังคมออนไลน์ เพื่อซื้อขายสินค้ากับผู้เสียหาย เนื่องจากเป็นช่องทางที่สะดวกและการยืนยันตัวตนของผู้ใช้งานในแต่ละแพลตฟอร์มยังไม่รัดกุมมากนัก ทำให้ผู้เสียหายตกเป็นเหยื่อจำนวนมาก โดยกรณีที่พบได้มากคือการสั่งซื้อสินค้าและไม่ได้รับสินค้าเลย หรือสั่งซื้อสินค้าชนิดหนึ่งแต่ได้รับสินค้าอีกชนิดหนึ่ง เป็นต้น หลังจากที่มิจฉาชีพได้ทำการตกลงซื้อขายกับเหยื่อแล้ว เมื่อเหยื่อโอนเงินมา ก็จะบล็อกช่องการติดต่อ หรืออาจจะส่งสินค้าชนิดอื่นให้กับผู้เสียหาย แสดงตัวอย่างดังรูปที่ 3-1

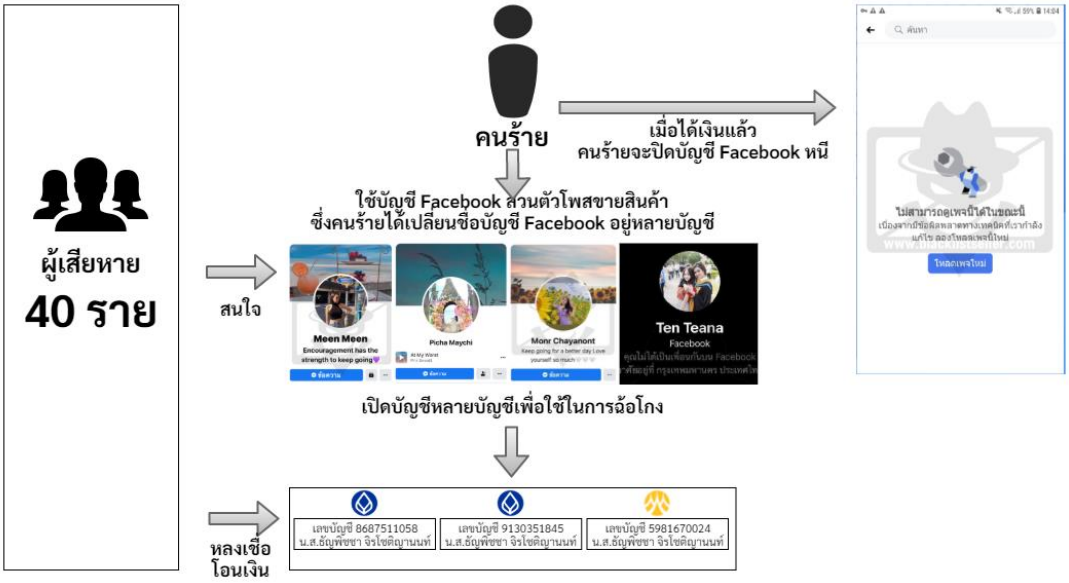
3.1.2 ขายสินค้าผ่านออนไลน์ถูกกว่าท้องตลาด แล้วไม่มีสินค้าส่งจริง

กรณีนี้ เกิดจากการประกาศขายสินค้าผ่านช่องทางออนไลน์ โดยมิจฉาชีพได้ตั้งราคาของสินค้าให้ถูกกว่าตามท้องตลาดทั่วไป เมื่อเหยื่อเห็นประกาศขายสินค้าที่มีราคาถูกกว่าปกติ จึงรีบตัดสินใจทำการซื้อขาย เนื่องจากกลัวว่าจะมีผู้อื่นมาซื้อสินค้าดังกล่าวตัดหน้าไป ทำให้ขาดความระมัดระวังในการซื้อสินค้า จึงเป็นเหตุให้ตกเป็นเหยื่อของมิจฉาชีพได้โดยง่าย แสดงตัวอย่างดังรูปที่ 3-2



บัญชีธนาคารที่ใช้หลอกลวงทั้งหมด 5 บัญชี
มูลค่าความเสียหายมากกว่า 68,350 บาท

รูปที่ 3-1 กรณีตัวอย่างหลอกขายสินค้าแล้วไม่ได้รับสินค้าตามที่ตกลง

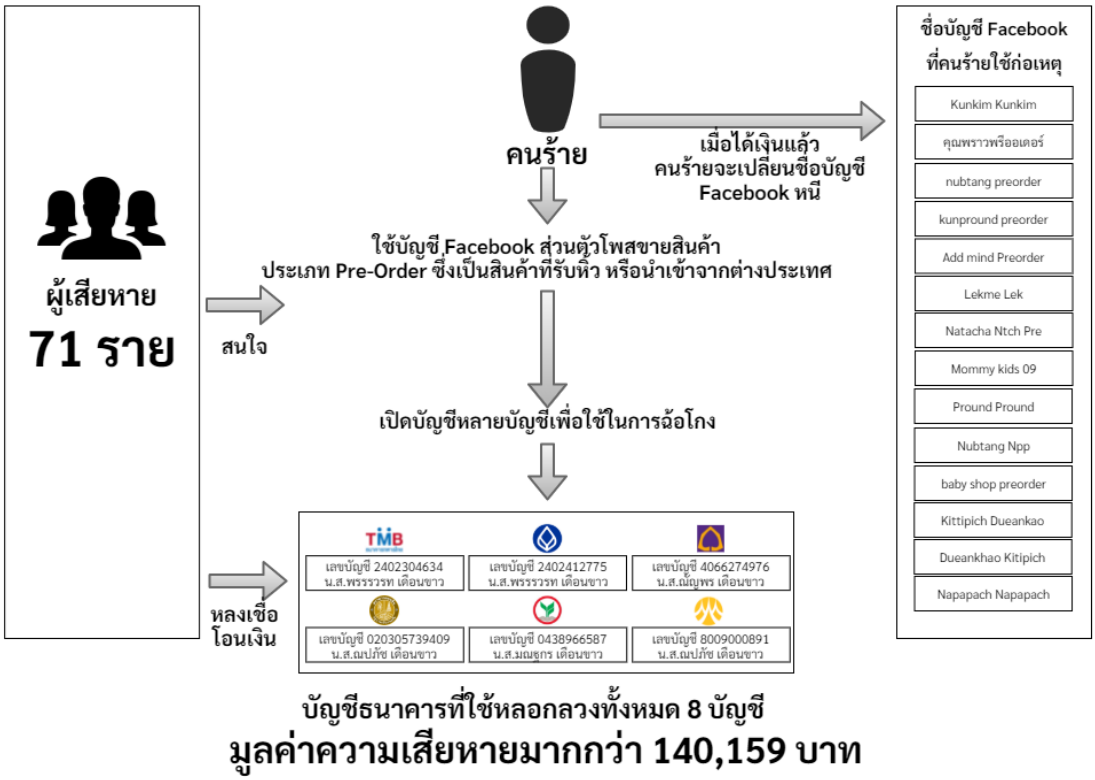


บัญชีธนาคารที่ใช้หลอกลวงทั้งหมด 3 บัญชี
มูลค่าความเสียหายมากกว่า 12,940 บาท

รูปที่ 3-2 กรณีตัวอย่างขายสินค้าถูกกว่าท้องตลาดแล้วไม่ส่งจริง

3.1.3 ล่อลวงให้โอนเงินค่าสินค้าล่วงหน้า (Pre-order)

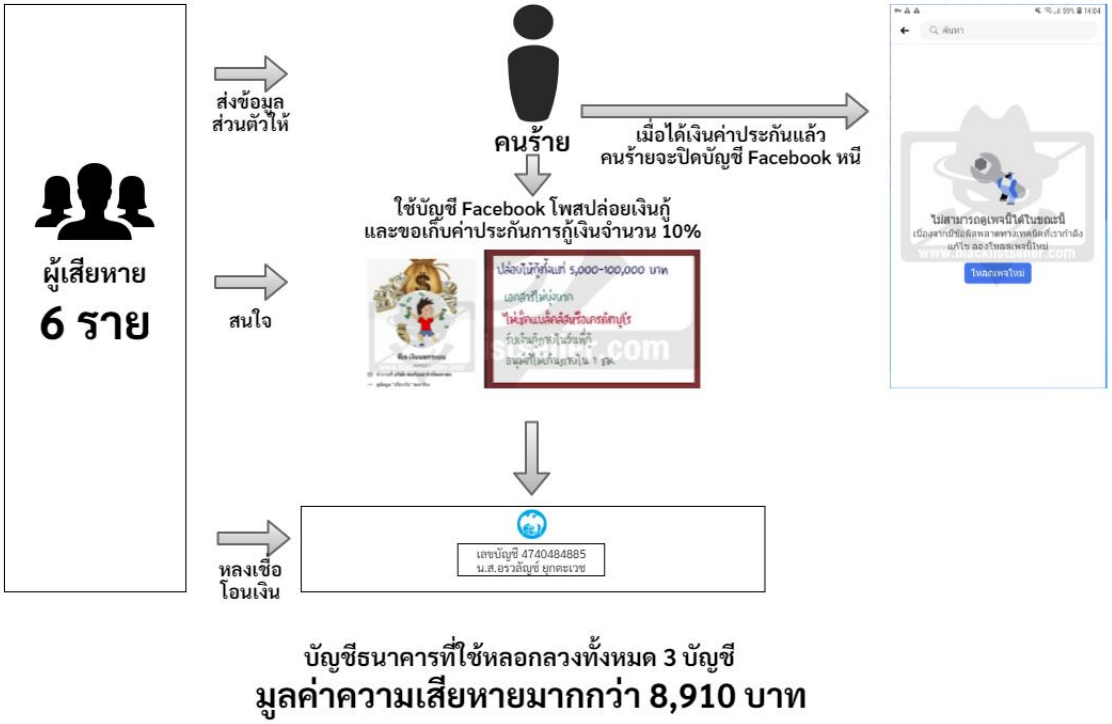
กรณีนี้เกิดเนื่องมาจาก สินค้า Pre-order อาจจะเป็นสินค้าที่ต้องสั่งทำเป็นพิเศษ หรือเป็นสินค้านำเข้าจากต่างประเทศ โดยมิจฉาชีพจะเริ่มจากการให้เหยื่อชำระค่าสินค้า เพื่อเป็นค่ามัดจำสำหรับสินค้ามาก่อน จากนั้นจะล่อลวงให้เหยื่อด้วยการยื่นข้อเสนอว่า หากชำระจำนวนเต็มมาก่อนจะให้ส่วนลด เมื่อเหยื่อหลงเชื่อและโอนเงินไปตามข้อเสนอ สุดท้ายเหล่ามิจฉาชีพก็ไม่ได้มีการส่งสินค้าให้จริง ทำให้เกิดความเสียหายขึ้น แสดงตัวอย่างดังรูปที่ 3-3



รูปที่ 3-3 กรณีตัวอย่างหลอกให้โอนเงินค่าสินค้าล่วงหน้า

3.1.4 ล่อลวงให้โอนเงินค่าทำสัญญาปล่อยเงินกู้นอกระบบดอกเบี้ยต่ำ อนุมัติง่าย ไม่ต้องตรวจสอบเครดิตบูโร

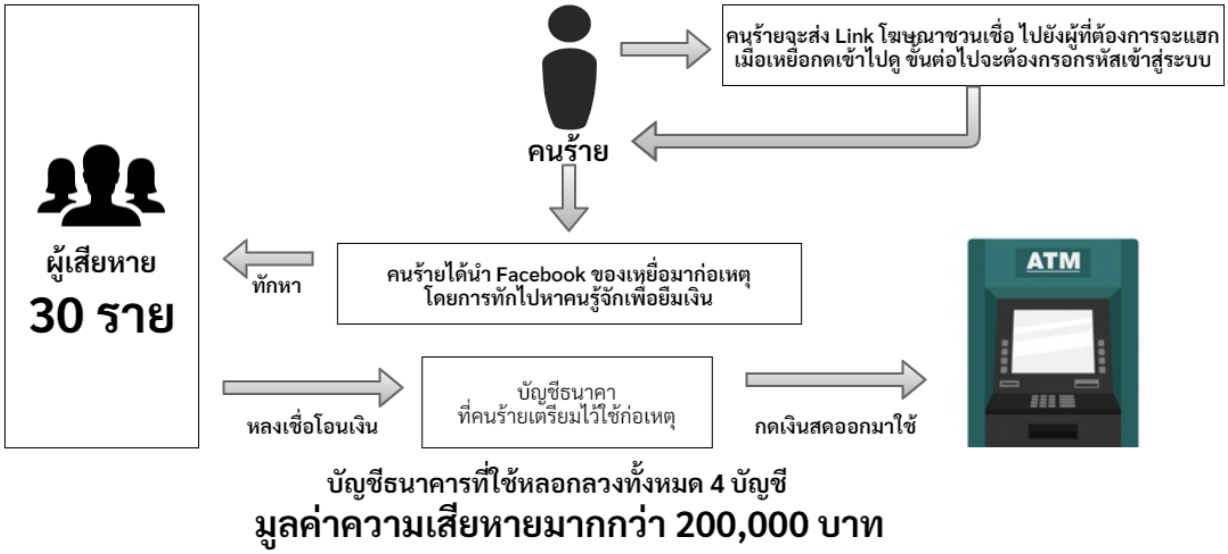
กรณีนี้ มิจฉาชีพจะใช้วิธีสร้างเพจเกี่ยวกับการให้กู้เงินนอกระบบ โดยอาจจะมีรูปแบบการหลอกลวงว่าสามารถกู้เงินได้โดยง่าย เช่น คนที่ติดแบล็กลิสต์ก็กู้ได้ โดยไม่ต้องมีหลักประกัน หรือสามารถพิจารณาอนุมัติเงินกู้ให้เสร็จได้ภายใน 1 ชั่วโมง เป็นต้น เมื่อมีเหยื่อให้ความสนใจ ก็จะขอหลักฐานของเหยื่อ และขอให้เหยื่อจ่ายเงินให้ โดยอ้างว่าเป็นค่าธรรมเนียมดำเนินการ สำหรับการกู้เงิน จากนั้นมิจฉาชีพจะทำเอกสารปลอม ส่งให้เหยื่อ โดยมักใส่ QR Code หรือ Barcode เพื่อทำให้ดูน่าเชื่อถือ โดยกว่าที่เหยื่อจะรู้ตัวก็ถูกมิจฉาชีพโกงไปเรียบร้อยแล้ว แสดงตัวอย่างดังรูปที่ 3-4



รูปที่ 3-4 กรณีตัวอย่างหลอกโอนเงินค่าทำสัญญาปล่อยเงินกู้นอกระบบ

3.1.5 หลอกให้โอนเงินโดยการใช้การสวมรอยบัญชีอีเมล์ หรือ โซเชียลมีเดีย

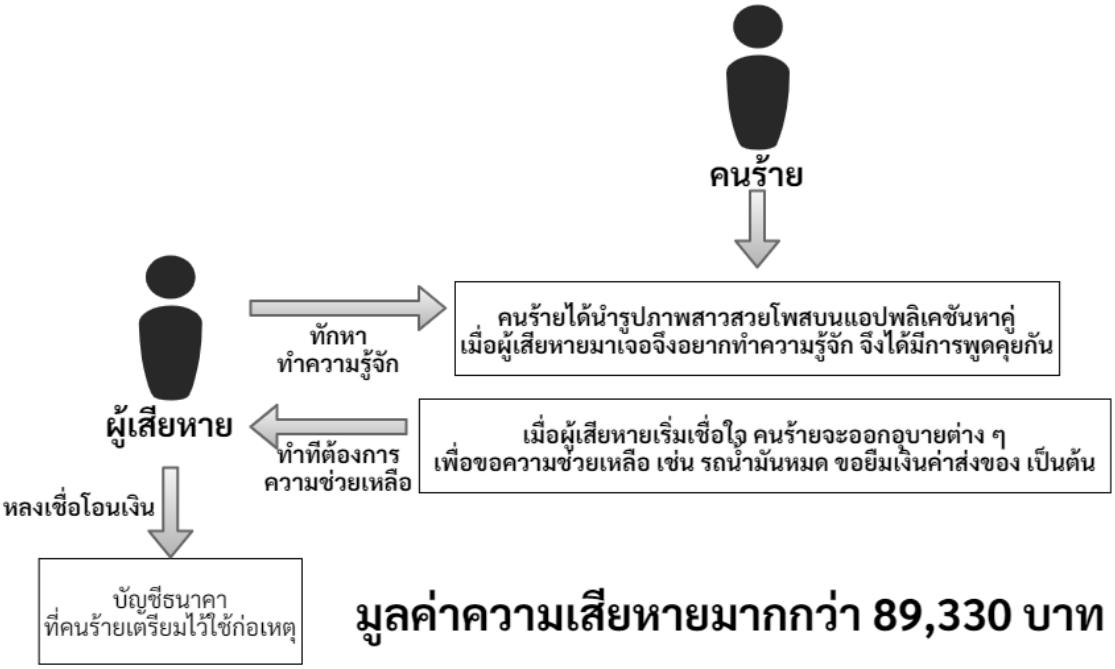
กรณีนี้จะเริ่มจากมิจฉาชีพจะแฮกบัญชีโซเชียลมีเดีย เช่น facebook, twitter อาจจะใช้วิธีการสุ่มกรอกรหัสผ่าน หรือส่งลิงค์โฆษณาให้ผู้เสียหาย เมื่อผู้เสียหายคลิกลิงค์เข้าไป ก็จะถูกมิจฉาชีพสวมรอยบัญชีเป็นที่เรียบร้อย จากนั้นมิจฉาชีพจะใช้บัญชีโซเชียล ทักไปหาเพื่อนที่มีรายชื่อในบัญชีนั้น เพื่อขอยืมเงิน หรือให้ชำระค่าสินค้าต่าง ๆ ให้ โดยที่เจ้าของบัญชีโซเชียลมีเดียไม่รู้ตัว แสดงตัวอย่างดังรูปที่ 3-5



รูปที่ 3-5 กรณีตัวอย่างหลอกให้โอนเงินโดยการใช้การสวมรอยบัญชี

3.1.6 แอบอ้างเป็นบุคคลต่าง ๆ หลอกว่าจะโอนเงินหรือส่งของให้ผ่านทางสื่อสังคมออนไลน์ Facebook Instagram Line

กรณีนี้ เป็นกรณีมิจฉาชีพที่หลอกเอาเงินเหยื่อผ่านโซเชียลเน็ตเวิร์ก โดยใช้รูปโปรไฟล์เป็นชายชาวต่างชาติหน้าตาดี สร้างเรื่องราว เข้ามาทำความรู้จักกับเหยื่อ ทำให้เหยื่อลุ่มหลงและไว้วางใจ ก่อนจะล่อลวงให้ส่งเงินไป รวมถึงการอุบายหลอกว่า จะส่งของไปให้ เช่น แหวนเพชร หรือของมีค่ามาหมั้น เพราะต้องการเดินทางไปใช้ชีวิตคู่อยู่ที่เมืองไทยด้วยกัน ซึ่งถัดไปไม่กี่วันก็จะมีคนโทรศัพท์มาหาเหยื่อ อ้างว่าเป็นเจ้าหน้าที่ไปรษณีย์ หรือพนักงานบริษัทส่งพัสดุ แจ้งว่ามีผู้ส่งพัสดุมาให้จากต่างแดน เป็นสิ่งของที่มีราคาแพงมูลค่าหลายล้านบาท โดยผู้รับต้องจ่ายเงินค่าภาษีก่อน จึงจะสามารถรับของไปได้ โดยมีมูลค่าความเสียหายจำนวนตั้งแต่หลักหมื่นถึงหลักแสนบาท แสดงตัวอย่างดังรูปที่ 3-6



รูปที่ 3-6 กรณีตัวอย่างโรแมนซ์สแกม

3.2 กลุ่มผู้เสียหาย

ทางคณะผู้วิจัยได้แบ่งกลุ่มคดีที่ผู้เสียหายถูกหลอกลวงเป็นคดี “ฉ้อโกง” ตามกฎหมายแยกไว้เป็น 2 พฤติกรรมแห่งคดี คือ

3.2.1 ฉ้อโกง “ความผิดฐานฉ้อโกง” (อ้างอิงตัวบท ตาม ป.วิอาญา มาตรา 341 ผู้ใดโดยทุจริตหลอกลวงผู้อื่นด้วยการแสดงข้อความ อันเป็นเท็จ หรือปกปิดข้อความจริงซึ่งควรบอกให้แจ้งและโดยการหลอก ลวงดังว่านั้นได้ไปซึ่งทรัพย์สินจากผู้ถูกหลอกลวง หรือบุคคลที่สามหรือ ทำให้ผู้ถูกหลอกลวงหรือบุคคลที่สามทำ ถอนหรือทำลายเอกสารสิทธิ ผู้นั้นกระทำความผิดฐานฉ้อโกง ต้องระวางโทษจำคุกไม่เกินสามปี หรือ ปรับไม่เกินหกพันบาท หรือทั้งจำทั้งปรับ) ซึ่งในกรณีนี้ ผู้เสียหาย สามารถประนีประนอมยอมความหรือไกล่เกลี่ยกับผู้ต้องหาได้ตลอดเวลา

3.2.2 ความผิด “ฉ้อโกงประชาชน” (อ้างอิงตัวบท ตาม ป.วิอาญา มาตรา 343 ถ้าการกระทำความผิดตาม มาตรา 341 ได้กระทำ ด้วยการแสดงข้อความอันเป็นเท็จต่อประชาชน หรือด้วยการปกปิดความจริง ซึ่งควรบอกให้แจ้งแก่ประชาชน ผู้กระทำต้องระวางโทษ จำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ ถ้าการกระทำความผิดดังกล่าวในวรรคแรก ต้องด้วยลักษณะ ดังกล่าวในมาตรา 342 อนุมาตรา หนึ่งอนุมาตราด้วย ผู้กระทำต้องระวางโทษจำคุกตั้งแต่หกเดือนถึงเจ็ดปี และปรับตั้งแต่หนึ่งพัน บาทถึงหนึ่งหมื่นสี่พันบาท) กรณีนี้ถือเป็นคดีอาญาแผ่นดิน ไม่สามารถไกล่เกลี่ยได้ แม้ผู้เสียหายอยากจะถอนคำร้องทุกข์ (แจ้งความ) ก็ไม่สามารถกระทำได้ เนื่องจากคดีอาญาแผ่นดิน รัฐเป็นผู้เสียหาย ตำรวจและอัยการต้องดำเนินคดีต่อจนถึงชั้นศาลและมีคำพิพากษาออกมา

3.3 การวิเคราะห์ปัจจัยภายในและปัจจัยภายนอกของการเกิดการฉ้อโกงออนไลน์

3.3.1 ปัจจัยภายใน

ปัจจัยภายในที่ทำให้เกิดปัญหาการฉ้อโกงออนไลน์หรือปัญหามิจฉาชีพออนไลน์ก็คือปัจจัยที่เกิดขึ้นจากตัวผู้เสียหายหรือเหยื่อเอง ซึ่งอาจเกิดได้จากหลายปัจจัยย่อย เช่น

1) ลักษณะของจิตใจที่ได้รับการถ่ายทอดมาจากบรรพบุรุษหรือถ่ายทอดทางกรรมพันธุ์

2) นิสัยใจคอ อารมณ์ ทัศคติ และความประพฤติ ที่เกิดจากการหล่อหลวมจากการอบรมเลี้ยงดูของครอบครัว ฐานะเศรษฐกิจของครอบครัวที่อาจต้องต่อสู้ดิ้นรน ตลอดจนสภาพแวดล้อม

3) ความรู้และความตระหนักรู้เท่าทันภัยที่มากับเทคโนโลยีอินเทอร์เน็ตและสื่อสังคมออนไลน์

ซึ่งปัจจัยภายในเหล่านี้นำไปสู่สภาวะที่ผู้เสียหายหรือเหยื่อเกิดความโลภหรือความอยากได้อยากมีที่เกินพอดี และเป็นความอยากได้อยากมีที่ขาดความสมเหตุสมผล เช่น

1) การสั่งซื้อสินค้าออนไลน์ที่มีราคาถูก เนื่องจากเห็นว่าราคาถูกกว่าท้องตลาด

2) การโอนเงินซื้อสินค้าล่วงหน้า (Pre-order) เพราะเห็นว่าเป็นสินค้าแบรนเนมมีคามลักลอบนำเข้ามาในราคาที่ถูกกว่าราคาปกติที่ซื้อจากหน้าร้านซึ่งมีการเสียภาษีจากศุลกากร

3) การโอนเงินค่าทำสัญญาเงินกู้นอกระบบที่เห็นแก่อัตราดอกเบี้ยที่ต่ำกว่าอัตราดอกเบี้ยจากธนาคารทั่วไป

นอกจากนี้ในกรณีของผู้เสียหายที่ขาดสติสัมปชัญญะแม้เพียงชั่วขณะก็อาจตกเป็นเหยื่อของมิจฉาชีพออนไลน์ได้ เช่น

1) การถูกล่อลวงให้ไว้ว่าใจและมีใจเสน่ห์แล้วสุดท้ายถูกหลอกให้โอนเงินให้หรือส่งของมีค่าไปให้ เช่น แหวนเพชร

2) การถูกหลอกให้โอนเงินโดยใช้การหลวมรอยบัญชีโซเชียลมีเดียหรืออีเมล์ของเพื่อนหรือบุคคลใกล้ชิด โดยอ้างว่ามีเหตุจำเป็นเร่งด่วนและต้องการเข้าช่วยเหลือโดยด่วน

3) การถูกหลอกให้ลงทุนแล้วได้ผลตอบแทนที่สูงเกินจริง เช่น เล่นแชร์ดอกเบี้ยสูงร้อยละ 20 ต่อเดือน เป็นต้น

ยิ่งไปกว่านั้นในกรณีที่ผู้ใช้งานขาดความรู้และความตระหนักรู้ จึงไม่รู้เท่าทันภัยที่มากับโลกออนไลน์หรือภัยทางไซเบอร์ (Cyber) ก็อาจต่อเป็นเหยื่อของมิจฉาชีพออนไลน์ได้เช่นกันยกตัวอย่างเช่น

1) การขาดความรู้เรื่องฟิชชิ่งที่มากับข้อความ SMS หรือ E-Mail ที่ถูกส่งมาเพื่อหลอกเอา Login และ Password ที่ใช้ในการทำธุรกรรมของเหยื่อ

2) ขาดความตระหนักรู้และขาดความระมัดระวังในการเข้าเว็บไซต์ที่อาจมีอันตรายแฝงต่อข้อมูล เช่น เว็บเล่นการพนัน เว็บดาวน์โหลดซอฟต์แวร์ฟรีหรือซอฟต์แวร์เถื่อน เป็นต้น

ฉะนั้น เพื่อไม่ให้ตกเป็นเหยื่อของมิจฉาชีพออนไลน์ประชาชนจะต้องมีความรู้ มีสติสัมปชัญญะและไม่โลภมาก

3.3.1 ปัจจัยภายนอก

ปัจจัยภายนอกสามารถแบ่งได้เป็น 2 ส่วนหลัก ๆ คือ

1) ปัจจัยด้านโอกาส ซึ่งในที่นี้จะเน้นเฉพาะกรณีของการฉ้อโกงออนไลน์หรือมิจฉาชีพออนไลน์ ซึ่งต้องอาศัยอินเทอร์เน็ตในการเข้าถึงสื่อสังคมออนไลน์ต่าง ๆ อย่างไรก็ดีด้วยความก้าวหน้าของเทคโนโลยีอินเทอร์เน็ตและเทคโนโลยีการสื่อโทรคมนาคม ไม่ว่าจะเป็นเทคโนโลยี 4G/5G เทคโนโลยีไวไฟ (WiFi) และเทคโนโลยีใยแก้วนำแสง (Fiber Optic) ทำให้ประชาชนหรือบุคคลทั่วไปสามารถเข้าถึงสื่อสังคมออนไลน์ สามารถทำธุรกรรมและซื้อขายสินค้าออนไลน์ได้โดยง่าย เพราะสามารถเข้าถึงทุกที่ทุกเวลาเมื่อมีอินเทอร์เน็ต นั้นหมายความว่าเทคโนโลยีอินเทอร์เน็ตและเทคโนโลยีการสื่อโทรคมนาคม กลายเป็นช่องทางที่สำคัญที่อาจทำให้ประชาชนหรือบุคคลทั่วไปที่ขาดความตระหนักรู้ ขาดสติสัมปชัญญะและมีความอย่างได้อย่างมีที่เกินพอดี กลายเป็นเหยื่อของมิจฉาชีพออนไลน์ได้โดยง่าย ฉะนั้นจึงควรหลีกเลี่ยงการใช้อินเทอร์เน็ตพร่ำเพื่อและเข้าเว็บไซต์หรือสื่อสังคมออนไลน์ที่ไม่เหมาะสม และควรหลีกเลี่ยงการเชื่อมต่อ WiFi สาธารณะเพราะอาจเป็นช่องทางหนึ่งที่มิจฉาชีพออนไลน์ใช้ในการโจรกรรมข้อมูลส่วนตัวของเหยื่อหรือผู้เสียหาย

2) ปัจจัยด้านมิจฉาชีพหรือคนร้าย ในที่นี้หมายถึงบุคคลหรือกลุ่มบุคคลที่ประสงค์ต่อทรัพย์สินหรือเงินทองของเหยื่อหรือผู้เสียหายโดยจะหาวิธีการต่าง ๆ ในการล่อหลวงหรือหลอกให้เหยื่อหลงเชื่อหรือไว้วางใจแล้วยินยอมทำตามเงื่อนไขที่บุคคลหรือกลุ่มบุคคลเหล่านั้นได้วางแผนไว้ เพื่อให้ได้ทรัพย์สินเงินทองหรือสิ่งของที่ต้องการ ฉะนั้นไม่ควรรับเพิ่มเพื่อนจากบุคคลที่ไม่รู้จักเว้นแต่จะเป็นเพื่อนของเพื่อนที่ไว้วางใจได้ หรืออาจมีการตรวจสอบให้แน่ใจก่อนรับเพิ่มเพื่อน และไม่ควรเปิดเผยข้อมูลส่วนตัวในรูปแบบสาธารณะบนสื่อสังคมออนไลน์ นอกจากนี้ผู้ใช้งานสื่อสังคมออนไลน์ควรพึงระวังภัยที่มาในรูปแบบของโรแมนซ์สแกม ที่อาจจะมาในรูปแบบของชาวต่างชาติที่ติดต่อเข้ามาผ่านแอพหาคู่ โดยทำการพูดคุยตีสนิมแล้วสอบถามข้อมูลส่วนตัว เมื่อเหยื่อหรือผู้เสียหลงเชื่อหรือไว้วางใจ จากนั้นจะทำการหลอกให้โอนเงินหรือทำธุรกรรมบางอย่าง ซึ่งสุดท้ายเหยื่อก็ตกเป็นผู้เสียหาย

3.4 ช่องทางการรับแจ้งเหตุ

กรณีที่ถูกมิจฉาชีพทำการฉ้อโกงผ่านช่องทางออนไลน์ ผู้เสียหายสามารถเข้าแจ้งความเพื่อดำเนินคดีกับผู้ขายที่ฉ้อโกงได้ โดยช่องทางในการรับแจ้งเหตุที่เกิดจากการฉ้อโกงออนไลน์ มีดังนี้

(1) เว็บไซต์ Blacklistseller ช่องทางนี้จะเป็นการแจ้งเตือนผู้ซื้อสินค้าออนไลน์ โดยรวบรวมข้อมูลผู้ที่ได้รับความเดือดร้อนจากการซื้อสินค้าออนไลน์ หรือการโอนเงินผ่าน E-Banking เข้ามาแจ้งรายละเอียดให้ผู้อื่น ถือเป็นเว็บไซต์ที่มีข้อมูลจากผู้เสียหายมากที่สุด

(2) สถานีตำรวจ ช่องทางนี้ จะใช้แจ้งความร้องทุกข์ต่อพนักงานสอบสวน สำหรับผู้เสียหายที่ต้องการเอาผิดกับผู้ต้องหา

(3) กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (TCSD) เป็นหน่วยงานสำหรับสืบสวนสอบสวน ป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี

(4) ศูนย์รับเรื่องร้องเรียนปัญหาออนไลน์ 1212 OCC เป็นอีกช่องทางหนึ่งสำหรับการรับเรื่องร้องเรียน ดำเนินการภายใต้โครงการขับเคลื่อนเศรษฐกิจและสังคมดิจิทัล ที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม มอบหมายให้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ มีเป้าหมายสำหรับรับเรื่องร้องเรียนปัญหาที่เกิดจากการซื้อขายทางออนไลน์ รวมถึงการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ สามารถแจ้งได้หลายช่องทาง เช่น โทรศัพท์ เว็บไซต์ อีเมล ข้อความ

3.5 แหล่งข้อมูลอื่น ๆ

3.5.1 ข้อมูลจากเว็บไซต์ Blacklistseller

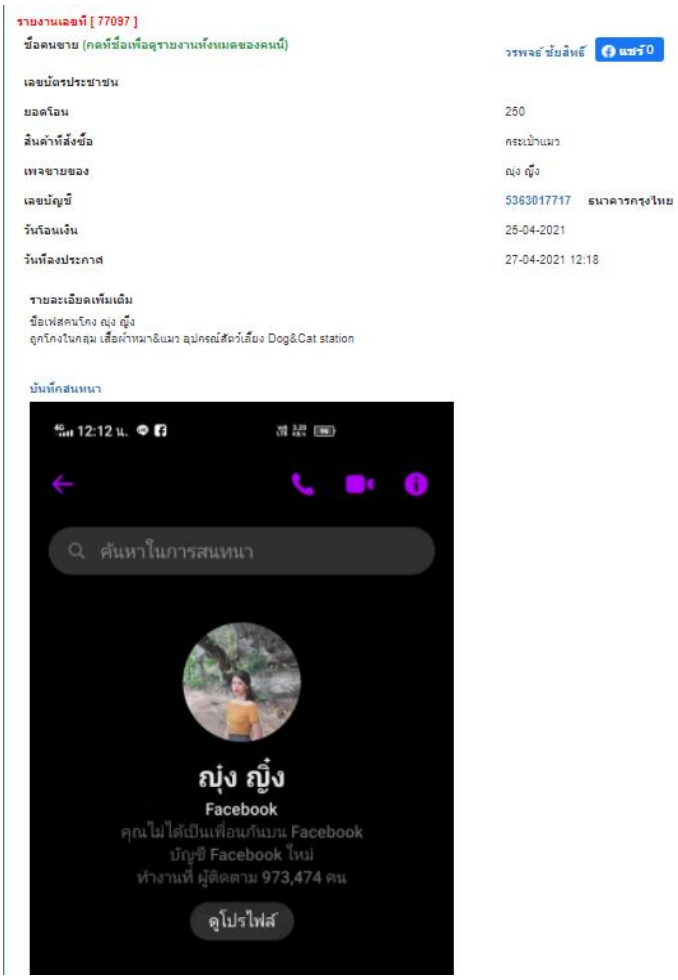
เว็บไซต์ Blacklistseller เป็นเว็บไซต์ศูนย์กลางการตรวจสอบคนโกงออนไลน์ มีไว้สำหรับตรวจสอบชื่อและเลขบัญชีก่อนโอนเงิน เพื่อป้องกันการโดนโกง โดยมีผู้เสียหายที่ถูกมิจฉาชีพฉ้อโกงไปเป็นผู้ให้ข้อมูลเพื่อเตือนภัย จากการรวบรวมข้อมูลในช่วงปี มกราคม 2563 - พฤษภาคม 2564 พบว่า มีเคสที่แจ้งเข้ามาผ่านทางเว็บไซต์ทั้งสิ้น 53,264 เคส โดยแต่ละเคสจะมีข้อมูลประกอบไปด้วย ชื่อมิจฉาชีพ เลขบัตรประชาชน ยอดโอน สินค้าที่สั่งซื้อ เพจขายของ เลขที่บัญชี วันที่โอนเงิน วันที่ลงประกาศ รายละเอียดเพิ่มเติม รวมทั้งรูปภาพการสนทนาระหว่างผู้เสียหายกับมิจฉาชีพ แสดงตัวอย่างดังรูปที่ 3-7

จากข้อมูลเดือน มกราคม 2563 - พฤษภาคม 2564 จำนวนทั้งหมด 53,264 เคสนั้น พบว่า มีข้อมูลบางส่วนที่ไม่สามารถนำมาใช้งานได้เนื่องจากมีข้อผิดพลาดในข้อมูลวันที่ หลังจากตัดข้อมูลส่วนดังกล่าวออกจะเหลือข้อมูลที่นำมาใช้หาเชิงสถิติจำนวนทั้งสิ้น 49,559 เคส

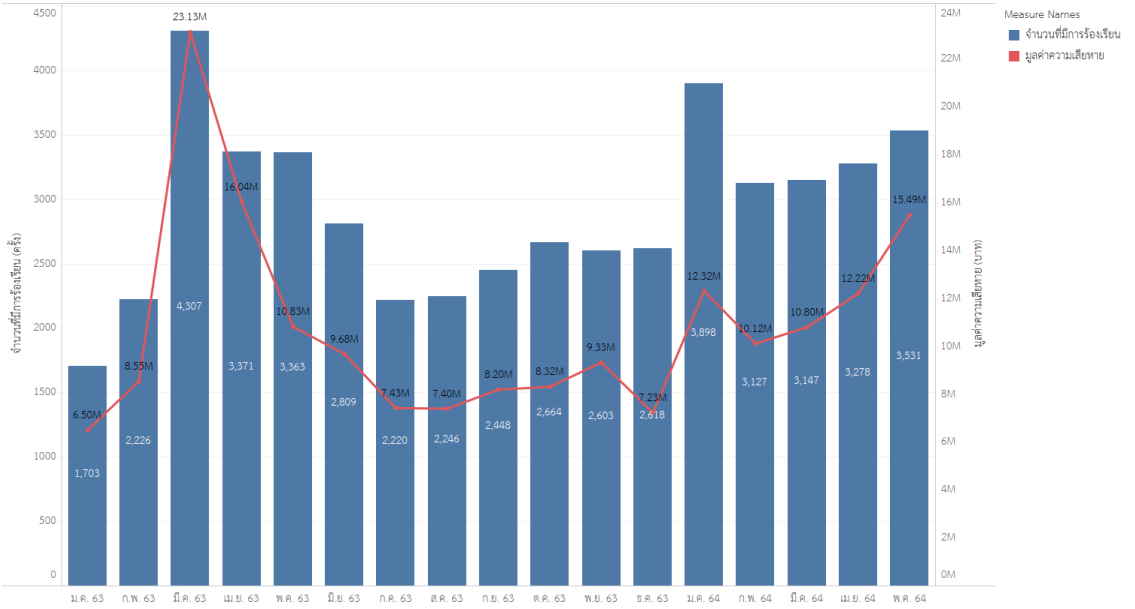
จากที่กล่าวมาข้างต้น ได้นำข้อมูลดังกล่าวมาตั้งข้อสมมุติฐานดังนี้

1) ตั้งแต่ มกราคม 2563 - พฤษภาคม 2564 มีแนวโน้มการกระทำความผิดมากยิ่งขึ้น หรือไม่

จากข้อมูลที่ได้ทำการศึกษา หากพิจารณาในภาพรวมจะเห็นได้ว่า ในเดือนมีนาคม 2563 จะมีการร้องเรียน เข้ามามากที่สุด และจะค่อย ๆ ลดลงจนทรงตัวในช่วงเดือน สิงหาคม 2563 - ธันวาคม 63 หลังจากนั้นยอดการกระทำความผิดก็พุ่งขึ้นในเดือน มกราคม 2564 และมีแนวโน้มพุ่งสูงขึ้นในช่วงเดือน กุมภาพันธ์ 2464 - พฤษภาคม 2564 ดังแสดงในรูปที่ 3-8



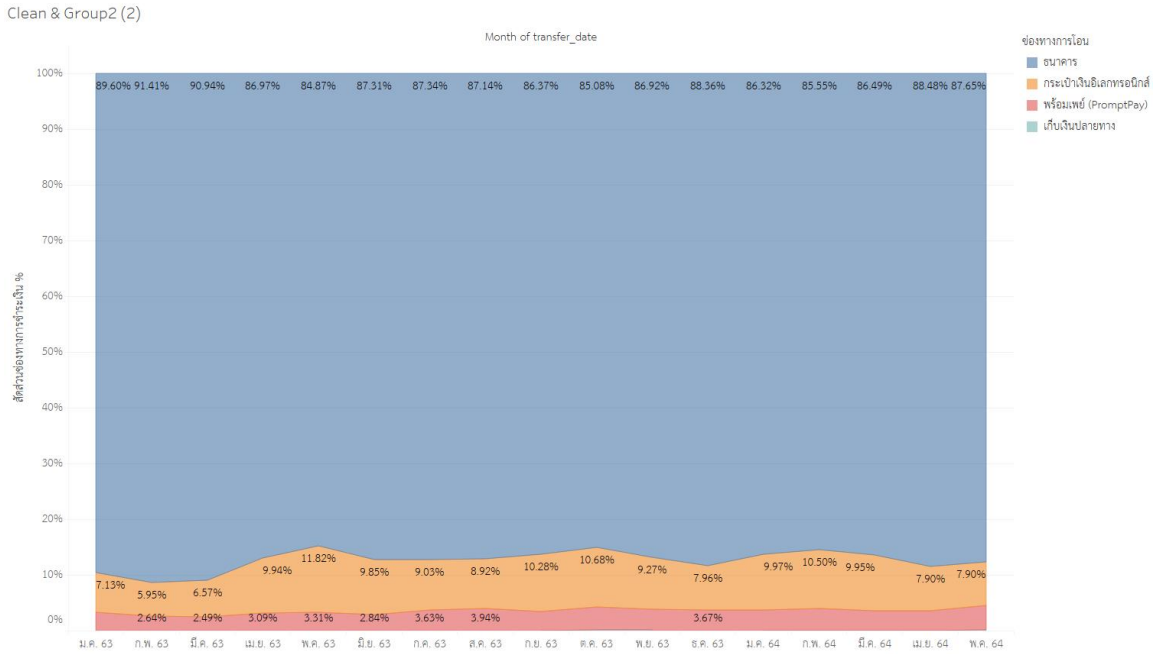
รูปที่ 3-7 ตัวอย่างข้อมูลจากเว็บไซต์ Blacklistseller



รูปที่ 3-8 การเปรียบเทียบระหว่างจำนวนเรื่องร้องเรียนกับมูลค่าความเสียหาย

2) ช่องทางการชำระสินค้าที่ผู้กระทำความผิดเลือกใช้ คือช่องทางใด และช่องทางดังกล่าวมีแนวโน้มที่จะใช้กระทำความผิดน้อยลงหรือไม่

จากข้อมูลทั้งหมด 49,559 เคส นำมาคัดกรองข้อมูลที่ไม่สามารถนำมาจำแนกกลุ่มได้จะเหลือจำนวนทั้งสิ้น 48,974 เคส และจากจำนวนดังกล่าว สามารถนำมาแบ่งกลุ่มได้ดังนี้ 1) ธนาคาร 2) กระเป๋าเงินอิเล็กทรอนิกส์ 3) พร้อมเพย์ 4) เก็บเงินปลายทางหลังจากที่ทำการแบ่งกลุ่มและจัดสัดส่วน พบว่าตั้งแต่ มกราคม 2563 - พฤษภาคม 2564 ผู้กระทำความผิดเลือกใช้ช่องทางการชำระเงินผ่านบัญชีธนาคาร โดยมีอัตราการใช้เฉลี่ยอยู่ที่ 87.42% และช่องทางที่ผู้กระทำความผิดเลือกใช้รองลงมาคือกระเป๋าเงินอิเลกทรอนิกส์ โดยเฉลี่ยอยู่ที่ 9.08% และช่องทางการชำระผ่านพร้อมเพย์จะอยู่ที่ 3.46% และช่องทางเก็บเงินปลายทางจะเป็นช่องทางที่ผู้กระทำความผิดเลือกใช้น้อยที่สุดจะอยู่ที่ 0.03% ดังแสดงในรูปที่ 3-9



รูปที่ 3-9 แสดงสัดส่วนช่องทางการชำระสินค้าที่มิจฉาชีพออนไลน์นิยมใช้มากที่สุด

3) ช่องทางการชำระเงินที่ผู้กระทำความผิดเลือกใช้มากที่สุดใด และมีแนวโน้มที่จะเลือกใช้ดังกล่าวน้อยลงหรือไม่

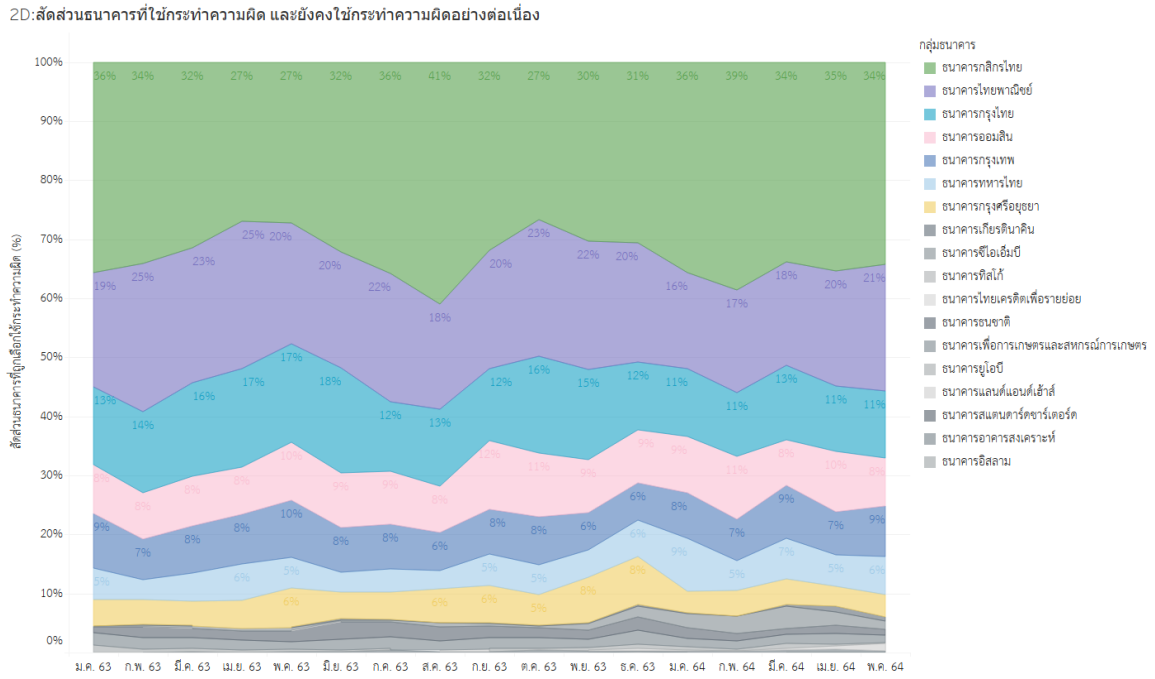
จากข้อมูล พบว่า ธนาคารที่ผู้กระทำความผิดเลือกใช้มากที่สุดอยู่ คือ ธนาคารกสิกรไทยที่มีอัตราเฉลี่ยการใช้งานอยู่ที่ 32.86% และยังคงถูกเลือกใช้งานมากที่สุดอย่างต่อเนื่องจนถึงพฤษภาคม 2564 นอกจากธนาคารกสิกรแล้วยังมีธนาคารอื่น ๆ ที่ถูกผู้กระทำความผิดใช้เป็นช่องทางการโอนเงินดังนี้ ธนาคารไทยพาณิชย์ 20.54% ธนาคารกรุงไทย 13.65% ธนาคารออมสิน 9.09% ธนาคารกรุงเทพ 7.83% ธนาคารทหารไทย 5.40% ธนาคารกรุงศรีอยุธยา 4.90% ธนาคารธนชาติ 1.71% ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร 1.66% ธนาคารซีไอเอ็มบี 1.19% ธนาคารยูโอบี 0.44% ธนาคารเกียรตินาคิน ธนาคารแลนด์แอนด์เฮ้าส์ 0.22% ธนาคารอาคารสงเคราะห์ 0.22% ธนาคารอิสลาม 0.02% ธนาคารไทยเครดิตเพื่อรายย่อย 0.02% ธนาคารสแตนดาร์ดชาร์เตอร์ 0.01% ธนาคารทิสโก้ 0.01% ดังแสดงในรูปที่ 3-10

4) จากข้อมูลวันที่โอนเงิน นำมาเปรียบเทียบกับวันที่มีร้องเรียนเข้ามาในเว็บไซต์ นั้นกว่าผู้เสียหายจะรู้ตัวหรือแจ้ง ผ่านไปกี่วันหลังจากถูกโกง

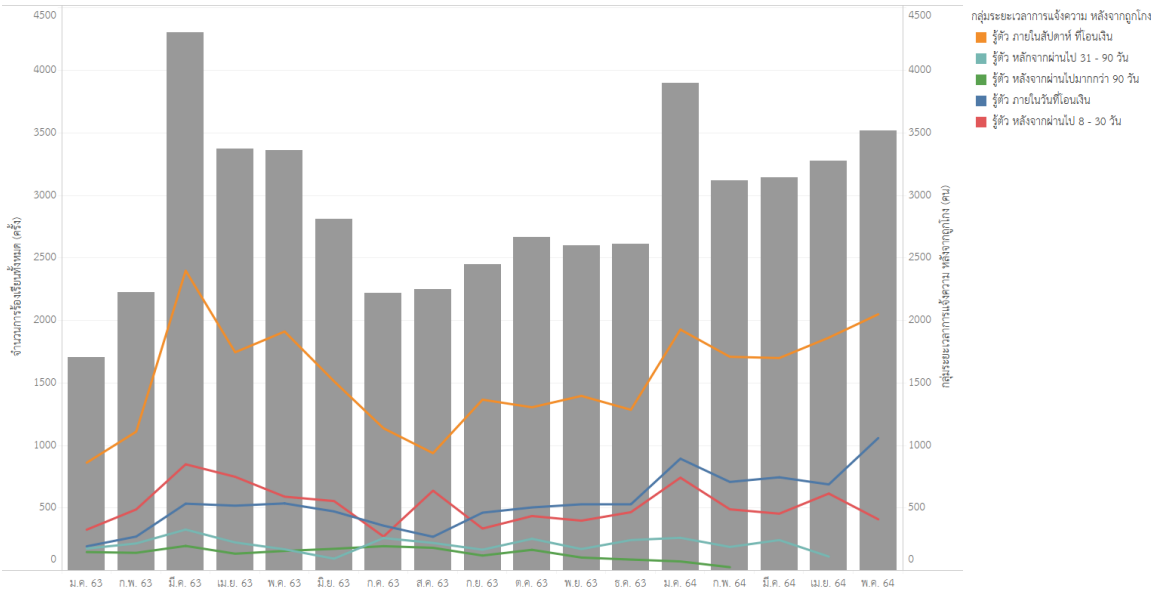
จากข้อมูล พบว่า ผู้เสียหาย 52.95% จะรู้ตัวว่าถูกโกงและทำการร้องเรียนเข้ามาในเว็บไซต์ภายใน 1 สัปดาห์ และ มีอัตราส่วน 18.72% ของกลุ่มผู้เสียหายที่รู้ตัวว่าถูกโกงภายในวันที่ทำการโอนเงินให้ผู้กระทำความผิด และมีกลุ่มผู้เสียหายที่รู้ตัวว่าถูกโกงและทำการแจ้งเข้ามาในเว็บไซต์ หลังจากผ่านไปมากกว่า 1 สัปดาห์ แต่ไม่เกิน 1 เดือน จำนวนทั้งสิ้น 17.79% นอกจากนั้นยังมีผู้เสียหายที่รู้หลังจากผ่านไป 1 เดือน แต่ไม่เกิน 3 เดือน และรู้ตัวหลังจากผ่านไปแล้วมากกว่า 3 เดือน ทั้งสิ้น 6.71% และ 3.83% ตามลำดับ ดังแสดงในรูปที่ 3-11

5) จากข้อมูลใบแจ้งความ ที่อยู่ในเว็บไซต์ นำมาตั้งสมมุติฐานว่าตั้งแต่ มกราคม 2563 - พฤษภาคม 2564 มีอัตราส่วนที่ผู้เสียหายไปแจ้งความดำเนินคดีและอัปโหลดลดใบแจ้งความเข้ามาในเว็บไซต์ มากขึ้นหรือลดลง

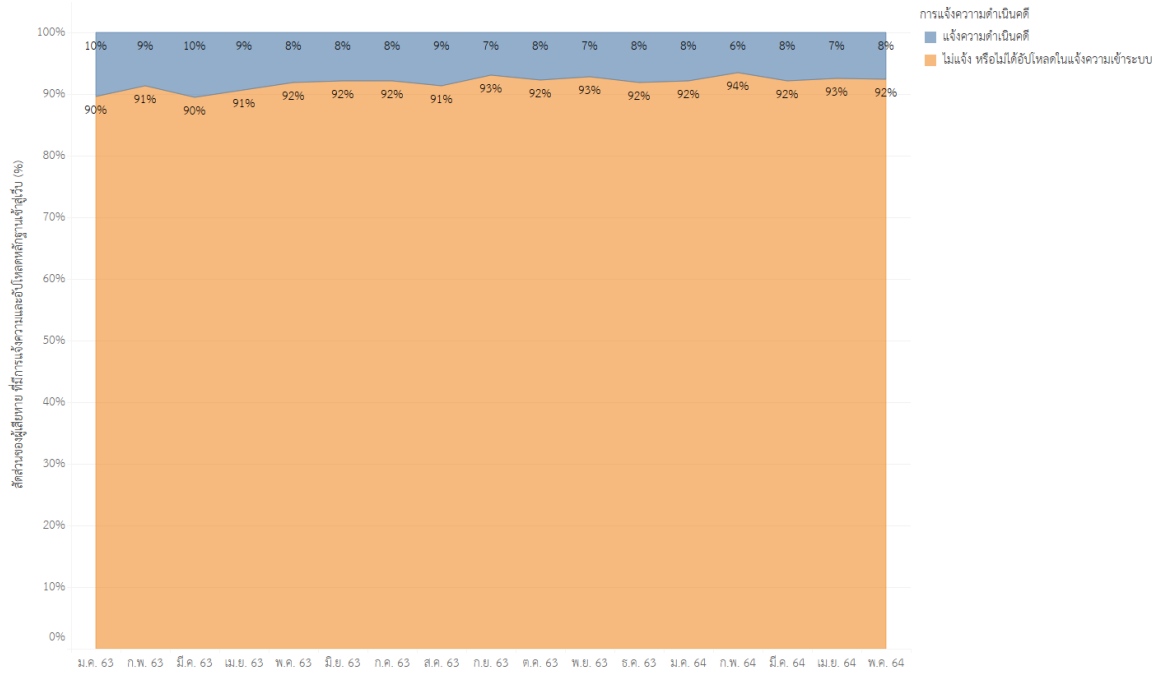
จากรูปจะสังเกตได้ว่าอัตราส่วนที่ผู้เสียหายไปแจ้งความดำเนินคดีจะอยู่ในเกณฑ์ 8-10% เท่านั้น ไม่มีแนวโนมที่จะเพิ่มขึ้นหรือลดลงแต่อย่างใด ดังแสดงในรูปที่ 3-12



รูปที่ 3-10 แสดงข้อมูลเปรียบเทียบธนาคารพาณิชย์ที่มิจฉาชีพออนไลน์นิยมใช้มากที่สุด



รูปที่ 3-11 แสดงการเปรียบเทียบระยะเวลาการร้องเรียนเมื่อทราบว่าถูกฉ้อโกง



รูปที่ 3-12 แสดงสัดส่วนจำนวนการแจ้งความของผู้เสียหายในเว็บไซต์

3.5.2 ข้อมูลจากศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติ (Police Cyber Taskforce)

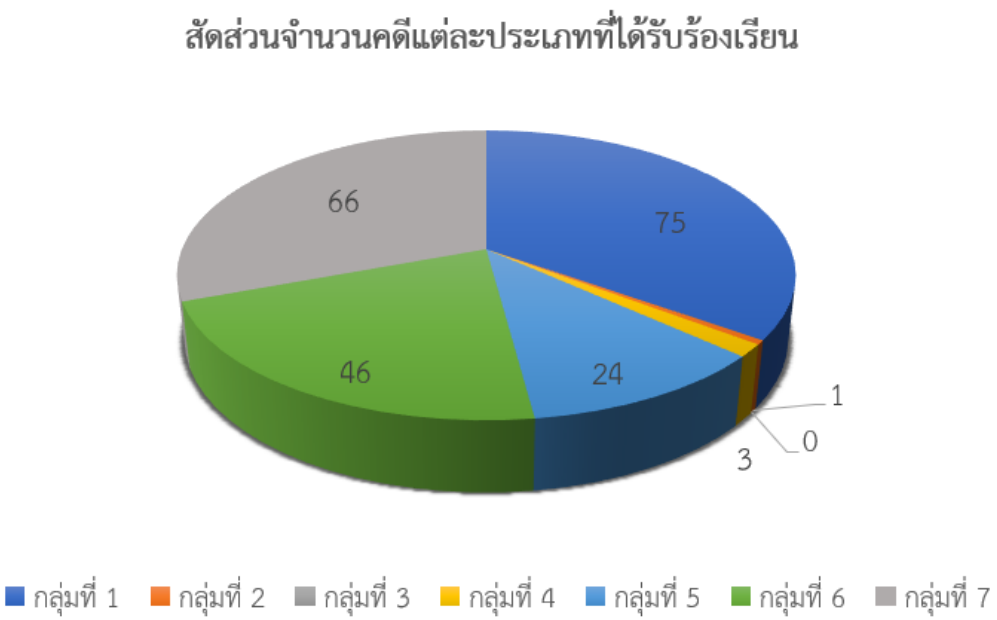
จากข้อมูลการรับเรื่องร้องเรียนจากศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติ เมื่อช่วงเดือนพฤศจิกายน 2562 – เดือนมีนาคม 2563 พบจำนวนคดีที่ได้รับแจ้งเป็นจำนวน 215 คดี โดยมีข้อมูลประกอบไปด้วย วันเดือนปีที่รับแจ้ง รายละเอียดของเรื่อง มูลค่าความเสียหาย วันเดือนปีที่เกิดเหตุ ชื่อผู้เสียหาย อายุ ที่อยู่และเบอร์โทรศัพท์ของผู้เสียหาย ผู้ถูกกล่าวหา ช่องทางการรับแจ้ง พื้นที่รับผิดชอบ ประเภทคดี ผู้รับผิดชอบ และผลการดำเนินการ ดังแสดงในรูปที่ 3-13

จากการแบ่งรูปแบบคดีฉ้อโกงของข้อมูลที่ได้รับ พบว่า รูปแบบคดีฉ้อโกงที่มีจำนวนมากที่สุด คือ กลุ่มคดีฉ้อโกงประเภทหลอกขายสินค้าแล้วไม่ได้รับสินค้าตามที่ตกลง มีจำนวน 75 คดี คิดเป็น 35% รองลงมาเป็นกลุ่มคดีฉ้อโกงประเภทโรแมนซ์สแกม มีจำนวน 46 คดี คิดเป็น 21% และกลุ่มคดีฉ้อโกงที่มีจำนวนผู้ร้องเรียนน้อยที่สุดคือ กลุ่มขายสินค้าผ่านออนไลน์ถูกกว่าท้องตลาด แล้วไม่มีสินค้าส่งจริง มีจำนวน 1 คดี คิดเป็น 0.46% นอกจากมียังมีกลุ่มที่เป็นคดีฉ้อโกงประเภทอื่น ๆ ที่ไม่ได้กล่าวไว้ข้างต้น เช่น หลอกให้ร่วมลงทุนรูปแบบต่าง ๆ ไม่ว่าจะเป็นทอง หุ้น หรือแม้ลงทุนผ่านบริษัท รวมถึงยังมีหลอกซื้อบริการ เป็นต้น โดยมีจำนวน 66 คดี คิดเป็น 31% แสดงสัดส่วนของกลุ่มคดีต่าง ๆ ดังแสดงในรูปที่ 3-14

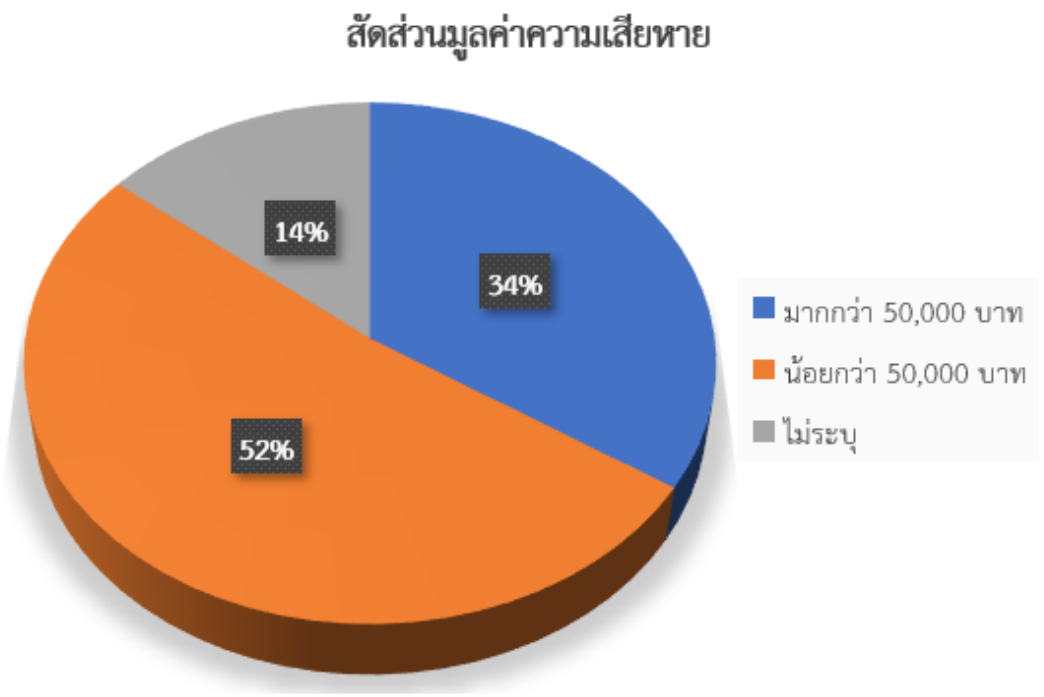
จากกลุ่มคดีที่เกี่ยวข้องกับการฉ้อโกงออนไลน์ จำนวน 149 คดี สามารถจำแนกมูลค่าความเสียหาย ได้เป็น 3 กลุ่ม ได้แก่ กลุ่มที่มีมูลค่าความเสียหายมากกว่า 50,000 บาท กลุ่มที่มีมูลค่าความเสียหายน้อยกว่า 50,000 บาท และกลุ่มที่ไม่ระบุมูลค่าความเสียหาย โดยกลุ่มที่มีจำนวนคดีมากที่สุดคือ กลุ่มที่มีมูลค่าความเสียหายน้อยกว่า 50,000 บาท มีจำนวน 77 คดี คิดเป็น 52% รองลงมาคือกลุ่มที่มีมูลค่าความเสียหายมากกว่า 50,000 บาท มีจำนวน 51 คดี คิดเป็น 34% และกลุ่มที่ไม่ระบุมูลค่าความเสียหาย มีจำนวน 21 คดี คิดเป็น 21% ดังแสดงในรูปที่ 3-15

ลำดับ	ว/ด/ป	เรื่อง/พฤติการณ์	มูลค่าความ	ว/ด/ป	ผู้ร้องเรียน/ผู้เสียหาย	อายุ	ที่อยู่	โทร	ผู้ถูกกล่าวหา	ช่องทางรับแจ้ง	พื้นที่	ประเภ	ผู้รับผิดชอบ	ผลการดำเนินการ
1	1/11/62	ธนาคารไทยพาณิชย์ฯ ได้ส่งข้อความแจ้งเตือนการชำระค่าสินค้า แต่ผู้แจ้งไม่ได้สั่งซื้อสินค้า	24,350	28 ต.ค. 62	[illegible]	27	ซ.หน้าวชิรพยาบาล แขวง/เขตดุสิต กทม.	[illegible]	ไม่มี	ศปอส.ตร.	น.	5	ร.ต.อ.วสันต์ แช่มมั่นคง พงส.สน.ธรรมศาลา 088-7283991	โทรแจ้งพงส.แล้ว
2	1/11/62	ผู้เสียหายสั่งยาไขข้อจากเวป แต่พอของมา	4,250	30 ต.ค. 62	[illegible]	55	47/129 ม.1 ต.บึงยี่โถ อ.	[illegible]	เวปไซต์ giverofdestiny	1599	ภ.1	1.3	พงส.สภ.ธัญญบุรี (ปทุมธานี)	แนะนำให้ผู้เสียหายแจ้งความก่อน
3	2/11/62	เฟสบุ๊ค “Sakarn At” มาหลอกยืมเงินเพื่อนของ	ไม่มี	2 พ.ย. 62	ไม่ประสงค์ออกนาม	ไม่มี	ไม่มี	ไม่มี	ไม่มี	1599	น.	1.3	พงส.สน.บางยี่ขัน	โทรกลับไป พบว่าไม่สามารถ
4	3/11/62	มีคนร้าย แอบแฮกข้อมูลมือถือ และเมล์ของผู้แจ้ง แต่ผู้แจ้งยังไม่ได้รับความเสียหายแต่อย่างใด	ไม่มี	3 พ.ย. 62	[illegible]	37	7/36 ม.1 ต.มะขาม อ. มะขาม จ.จันทบุรี	[illegible]	ไม่มี	1155	ภ.2	5	พงส.สภ.มะขาม (จันทบุรี)	โทรประสานหัวหน้างาน สอบสวน สภ.มะขามแล้ว
5	3/11/62	คนร้ายใช้เฟสบุ๊คชื่อ “Jerapon Somsuk” โพสต์	ไม่มี	30 ก.ย. 62	[illegible]	41	333/313 ม.1 ต.บางเพรียง	[illegible]	ไม่มี	1155	ภ.1	5	พงส.สภ.บางพลี	ได้โทรประสาน สว.(สอบสวน)
6	4/11/62	ผู้ต้องหานำรูปภาพลามกของผู้เสียหายไป	ไม่มี	22 ต.ค.62	[illegible]	18	เลขที่ 74 หมู่ ๑ ต.นาสีนวล	[illegible]	ไม่มี	1155	ไม่มี	5	อยู่ระหว่างเสนอ	อยู่ระหว่างเสนอผู้บังคับบัญชา
7	4/11/62	หลอกขายไอแพด โปร ๑๑ โพสใน	24,350	2 พ.ย.62	[illegible]	ไม่มี	5/11 ซ.พัฒนสิน ถ.นางลิ้นจี่	[illegible]	น.ส.พัชรกันย์ บุญธู่อิง	1155	น.	2.3	พ.ต.ท.ศุภชัย หาญคำหล้า	โทรประสานแล้ว
8	5/11/62	เฟสบุ๊ค "Piyanut PK Nutsu" โพสขายไอดีเกมส์	ไม่มี	4 พ.ย.62	[illegible]	ไม่มี	95/381 ถ.ลำลูกกาคลอง 8	ไม่มี	ไม่มี	1155	ภ.1	1.3	ร.ต.อ.ธีรศักดิ์ แสนโท	โทรแจ้งพงส.แล้ว
9	5/11/62	ผู้เสียหายถูกหลอกขายโทรศัพท์ยี่ห้อ แอปเปิ้ล	3,100	26 ต.ค.62	[illegible]	ไม่มี	๑๐๒ ม.๖ ต.คลองคะ	[illegible]	064-1014349	1155	ภ.6	2.3	พ.ต.ท.บุญยัง บุญเอี่ยม	โทรประสานแล้ว
10	6/11/62	ผู้เสียหายนำรถไปจำนำ ที่ลงประกาศในเพจ	๑.รถยนต์	2 พ.ย.62	[illegible]	39	ไม่มี	[illegible]	BKK autocash	ศปอส.ตร.	น.	2.3	พงส.สน.ห้วยขวาง	นัดหมายให้ผู้เสียหายเข้าพบ
11	7/11/62	คนร้ายเปิดเพจขายของผ่านเฟสบุ๊คหลายเพจ	70,000	มิ.ย.62	[illegible]	32	286/7	[illegible]	ไม่มี	ศปอส.ตร.	น.	2.3	ร.ต.ท.รัชวิทย์ สิทธิโชค	นัดหมายให้ผู้เสียหายเข้าพบ
12	7/11/62	แชร์ออนไลน์ ผ่านเฟสบุ๊คชื่อ “เกศดา	1,403,360	16 ส.ค.62	[illegible]	34	10/1 ม.1 ต.เมืองเพีย อ.กุด	[illegible]	เกศดา ปราบปรามและ	ศปอส.ตร.	น.	2.2	บก.ปอศ.	รวบรวมเอกสารร้องทุกข์
13	7/11/62	เพจเฟสบุ๊ค “บ้านหนังสือจอมทอง” ผู้เสียหาย	3,433	27 ต.ค.62	[illegible]	31	99/64 ซ.บางแวก 17 แขวง	[illegible]	บ้านหนังสือจอมทอง	1155	น.	2.3	ร.ต.ท.อังกูร จรัสเมธาวิทย์	นัดหมายให้ผู้เสียหายเข้าพบ
14	8/11/62	คนร้ายใช้อินสตราแกรมหักมาพูดคุยกับ	35,000	7 พ.ย.62	[illegible]	37	93 ถ.สมัครธรรมการ อ.	[illegible]	ไม่มี	1155	ภ.6	2.3	พ.ต.ท.ปรินทร ภู่ระย้า โทร.	นัดหมายให้ผู้เสียหายเข้าพบ
15	11/11/62	ผู้เสียหายได้รู้จักพูดคุยกับผู้ต้องหาผ่านทาง	300,000	ไม่มี	[illegible]	63	ไม่มี	ไม่มี	ไม่มี	1155	น.	1.2	พงส.สน.คลองตัน	โทรประสานงานให้ สน.โชคชัย
16	11/11/62	คนร้ายใช้เฟสบุ๊คชื่อ Chomput Funla-ong	ไม่มี	17 ต.ค. 62	[illegible]	28	ไม่มี	ไม่มี	ไม่มี	1155	ภ.7	1.3	พงส.สภ.อู่ทอง (สุพรรณ)	โทรประสานงานให้ สภ.อู่ทอง
17	11/11/62	คนร้ายใช้เฟสบุ๊คชื่อ "Maliwan Trayongkam"	39,500	ไม่มี	[illegible]	43	ไม่มี	ไม่มี	ไม่มี	1155	ภ.7	1.2	พงส.สภ.สภ.หัวหิน	แนะนำให้ผู้เสียหายร้องทุกข์ที่
18	12/11/62	หลอกให้ซื้อโทรศัพท์มือถือยี่ห้อไอโฟน X	5,650	11 พ.ย. 62	[illegible]	27	บ้านหนองน้ำใส ต.หนอง	[illegible]	063-8094487	1155	ภ.2	2.3	พงส.สภ.วัฒนานคร	โทรประสาน ร.ต.อ.นิรันฯ พงส.
19	12/11/62	หลอกให้ซื้อรองเท้า ในไลน์ชื่อ "อังกฤษ"	2,000	9 พ.ย. 62	[illegible]	19	ต.สุเทพ อ.เมือง จ.	[illegible]	นายอังกฤษ วิเศษสังข์	1155	ภ.5	2.3	พงส.สภ.เมืองเชียงใหม่	แนะนำให้ผู้เสียหายไปร้องทุกข์
20	12/11/62	หลอกซื้อขายเม็ดมะม่วงหิมพานต์โดยบัญชี	8,400	9 ต.ค.62	[illegible]	22	28/10 ม.4 ต.โคกกระบือ อ.	[illegible]	083-5209976	1155	ภ.7	2.3	พงส.สภ.เมืองสมุทรสาคร	แนะนำให้ผู้เสียหายไปร้องทุกข์
21	12/11/62	คนร้ายได้ปลอมเฟสบุ๊คเป็นภรรยาผู้ใหญ่บ้าน	20,800	11 พ.ย.62	[illegible]	45	617 หมู่ 3 ต.ไทยสามัคคี อ.	[illegible]	ไม่มี	1155	ภ.3	1.3	พงส.สภ.วังน้ำเขียว	ประสานพนักงานสอบสวนแล้ว
22	12/11/62	ผู้เสียหายถูกผู้ต้องหาหลอกลวงให้ซื้อขายแชร์	88,000	4 เม.ย.62	[illegible]	34	51/33 หมู่ 10 แขวงหนอง	[illegible]	ท้าว ออย ท้าว นับ	1155	น.	2.2	พงส.สน.หนองจอก	แนะนำผู้เสียหายร้องทุกข์ที่ สน.
23	12/11/62	ถูกหลอกลวงขาย ไอดีเกมส์ ชื่อ PUBG	20,000	11 พ.ย.62	[illegible]	16	128 หมู่ 1 ต.โคกสาะอาด	[illegible]	ไม่มี	1155	ภ.3	2.3	พงส.สภ.ลำปลายมาศ	ประสานงานให้ พงส. ดำเนินคดี
24	13/11/62	อีเมลของผู้เสียหายถูกlon in เข้าจากที่อื่น และ	800	12 พ.ย. 62	[illegible]	41	1492/103 ถ.ขุขันธ์ ต.เมือง	[illegible]	นวพร จาริชา/นางนิตยา	ศปอส.ตร.	น.	1.3	พงส.สน.คลองตัน	ประสานให้ผู้แจ้งไปร้องทุกข์ที่

รูปที่ 3-13 ตัวอย่างข้อมูลที่ได้รับจากศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ



รูปที่ 3-14 สัดส่วนรูปแบบการฉ้อโกงออนไลน์แต่ละประเภท
(กลุ่มที่ 1 – การซื้อขายตามเว็บประกาศขายผ่านทางสื่อสังคมออนไลน์ต่างๆ
กลุ่มที่ 2 - ขายสินค้าผ่านออนไลน์ถูกกว่าท้องตลาด แล้วไม่มีสินค้าส่งจริง
กลุ่มที่ 3 - ล่อลวงให้โอนเงินค่าสินค้าล่วงหน้า (Pre-order)
กลุ่มที่ 4 - ล่อลวงให้โอนเงินค่าทำสัญญาปล่อยเงินกู้นอกระบบดอกเบี้ยต่ำ อนุมัติง่าย ไม่ต้องตรวจสอบเครดิตบูโร
กลุ่มที่ 5 - หลอกให้โอนเงินโดยการใช้การสวมรอยบัญชีอีเมล์ หรือ โซเชียลมีเดีย
กลุ่มที่ 6 - แอบอ้างเป็นบุคคลต่าง ๆ หลอกว่าจะโอนเงินหรือส่งของให้ผ่านทางสื่อสังคมออนไลน์ Facebook Instagram Line
กลุ่มที่ 7 - กลุ่มอื่น ๆ)



รูปที่ 3-15 สัดส่วนมูลค่าความเสียหายของคดีฉ้อโกงออนไลน์

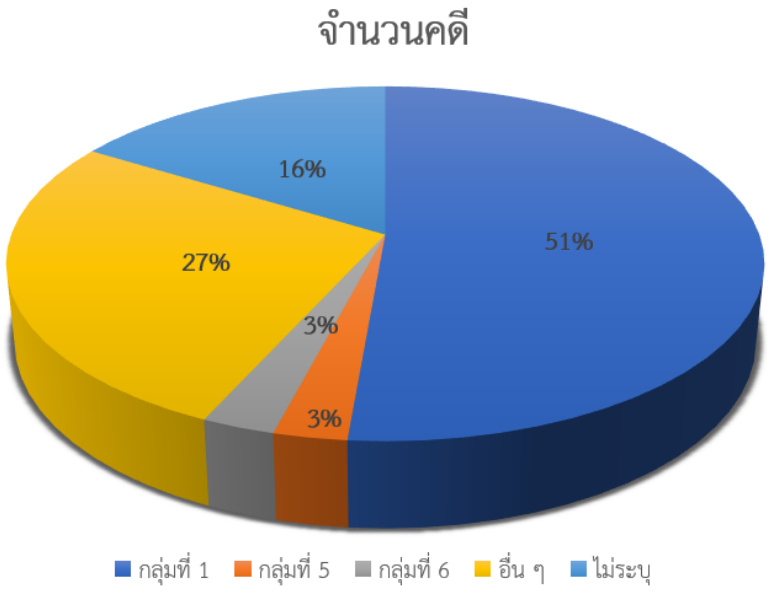
3.5.3 ข้อมูลบัญชีฉ้อโกงออนไลน์ กองบังคับการตำรวจนครบาล 8 (บก.น.8)

กองบังคับการตำรวจนครบาล 8 มีหน่วยงานในสังกัดรวม 13 หน่วยงาน ประกอบด้วย ฝ่ายอำนวยการ กองกำกับการสืบสวนสอบสวน และสถานีตำรวจอีก 11 แห่ง ได้แก่ สน.บุปผาราม สน.บางยี่เรือ สน.ตลาดพลู สน.บางมด สน.สมเด็จเจ้าพระยา สน.ปากคลองสาน สน.สำเหร่ สน.บุคคโล สน.บางคอแหลม สน.ราษฎร์บูรณะ และสน.ทุ่งครุ จากข้อมูลบัญชีคดีฉ้อโกงออนไลน์ในพื้นที่ ตั้งแต่วันที่ 1 ต.ค. 63 - 5 ก.ค. 64 พบจำนวนคดีที่รับแจ้งจำนวน 37 คดี โดยมีข้อมูลประกอบด้วย วันที่เกิดเหตุ วันที่รับแจ้ง พฤติการณ์ของคดี มูลค่าความเสียหาย

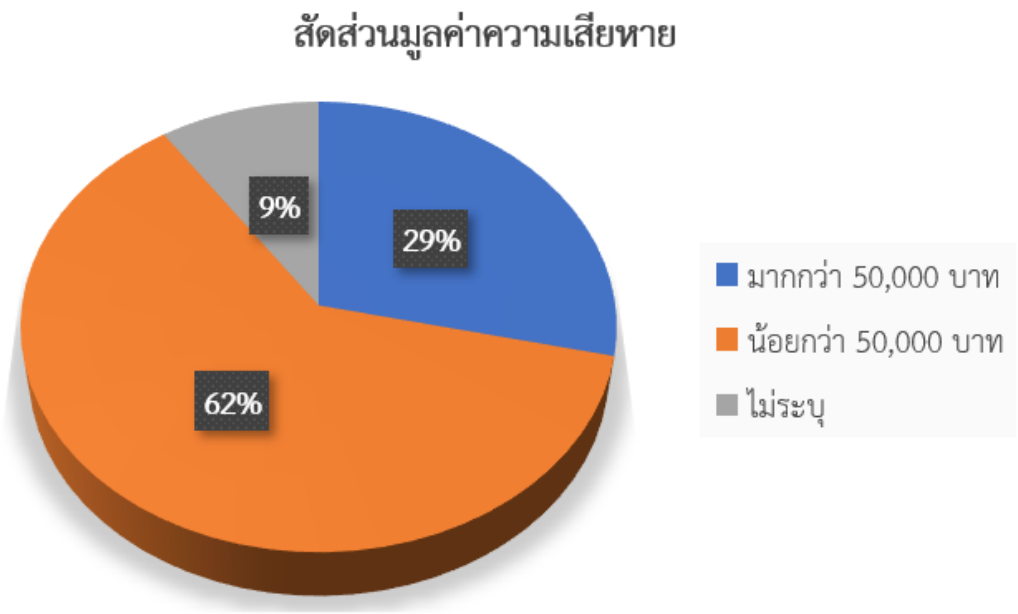
จากการศึกษาคดีฉ้อโกงออนไลน์ของกองบังคับการตำรวจนครบาล 8 ช่วงตั้งแต่วันที่ 1 ต.ค. 63 - 5 ก.ค. 64 เปรียบเทียบกับรูปแบบการกระทำความผิด ตามที่ได้กล่าวไว้ในหัวข้อ 1.1 สามารถสรุปได้ ดังนี้

รูปแบบคดีฉ้อโกงที่มีจำนวนมากที่สุด คือกลุ่มคดีฉ้อโกงประเภทหลอกขายสินค้าแล้วไม่ได้รับสินค้าตามที่ตกลง มีจำนวน 19 คดี คิดเป็น 51% รองลงมาเป็นกลุ่มคดีฉ้อโกงประเภทหลอกให้โอนเงินโดยการใช้การสวมรอยบัญชี และกลุ่มคดีฉ้อโกงโรแมนซ์สแกม มีจำนวนอย่างละ 1 คดี คิดเป็น 3% ส่วนกลุ่มของคดีฉ้อโกงอื่น ๆ เช่น โกงเงินค่าเช่าบ้าน โกงเงินค่าว่าจ้างทำงาน หลอกลวงให้ร่วมลงทุน มีจำนวน 10 คดี คิดเป็น 27% นอกจากนี้ยังมีคดีที่ไม่สามารถระบุได้ว่าเป็นการฉ้อโกงรูปแบบใดอีก 6 คดี คิดเป็น 16% แสดงสัดส่วนดังรูปที่ 3-16

จากกลุ่มคดีที่เกี่ยวข้องกับการฉ้อโกงออนไลน์ จำนวน 21 คดี สามารถจำแนกมูลค่าความเสียหายได้เป็น 3 กลุ่ม ได้แก่ กลุ่มที่มีมูลค่าความเสียหายมากกว่า 50,000 บาท กลุ่มที่มีมูลค่าความเสียหายน้อยกว่า 50,000 บาท และกลุ่มที่ไม่ระบุมูลค่าความเสียหาย โดยกลุ่มที่มีจำนวนคดีมากที่สุดคือ กลุ่มที่มีมูลค่าความเสียหายน้อยกว่า 50,000 บาท มีจำนวน 13 คดี คิดเป็น 62% รองลงมาคือกลุ่มที่มีมูลค่าความเสียหายมากกว่า 50,000 บาท มีจำนวน 6 คดี คิดเป็น 29% แสดงดังรูปที่ 3-17



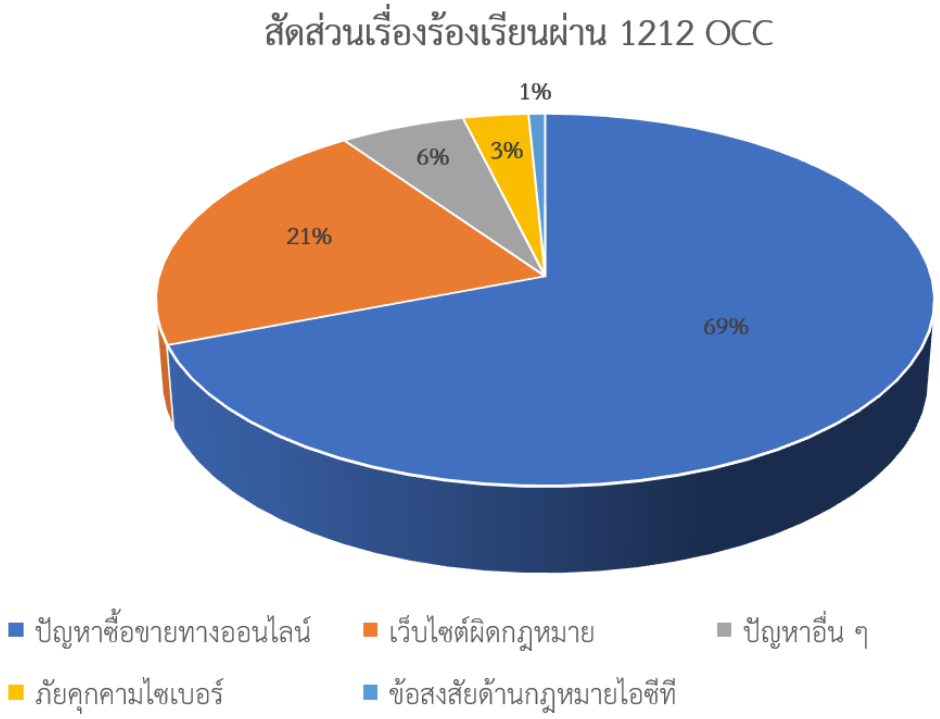
รูปที่ 3-16 สัดส่วนรูปแบบการฉ้อโกงออนไลน์แต่ละประเภท
(กลุ่มที่ 1 – การซื้อขายตามเว็บประกาศขายผ่านทางสื่อสังคมออนไลน์ต่างๆ
กลุ่มที่ 2 - ขายสินค้าผ่านออนไลน์ถูกกว่าท้องตลาด แล้วไม่มีสินค้าส่งจริง
กลุ่มที่ 3 - ล่อลวงให้โอนเงินค่าสินค้าล่วงหน้า (Pre-order)
กลุ่มที่ 4 - ล่อลวงให้โอนเงินค่าทำสัญญาปล่อยเงินกู้นอกระบบดอกเบี้ยต่ำ อนุมัติง่าย ไม่ต้องตรวจสอบเครดิตบูโร
กลุ่มที่ 5 - หลอกให้โอนเงินโดยการใช้การสวมรอยบัญชีอีเมล์ หรือ โซเชียลมีเดีย
กลุ่มที่ 6 - แอบอ้างเป็นบุคคลต่าง ๆ หลอกว่าจะโอนเงินหรือส่งของให้ผ่านทางสื่อสังคมออนไลน์ Facebook Instagram Line
อื่น ๆ – การฉ้อโกงประเภทอื่น ๆ
ไม่ระบุ – ไม่มีการระบุพฤติการณ์ของคดีความ)



รูปที่ 3-17 สัดส่วนมูลค่าความเสียหายของคดีฉ้อโกงออนไลน์

3.5.4 ข้อมูลจากศูนย์รับเรื่องร้องเรียนปัญหาออนไลน์ 1212 OCC

ภาพรวมการรับเรื่องร้องเรียนผ่าน 1212 OCC ในปี 2564 ที่ผ่านมา มีทั้งสิ้น 54,348 เรื่อง โดยปัญหาที่มีการร้องเรียนมากที่สุดคือ ปัญหาซื้อขายทางออนไลน์ มีจำนวน 37,584 เรื่อง คิดเป็น 69% รองลงมาเป็นปัญหาเว็บไซต์ผิดกฎหมาย มีจำนวน 11,476 เรื่อง คิดเป็น 21% ตามมาด้วย ปัญหาอื่น ๆ และสอบถามข้อสงสัย มีจำนวน 3,200 เรื่อง คิดเป็น 6% ปัญหาภัยคุกคามไซเบอร์ มีจำนวน 1,667 เรื่อง คิดเป็น 3% และข้อสงสัยด้านกฎหมายไอซีที มีจำนวน 421 เรื่อง คิดเป็น 1% แสดงดังรูปที่ 3-18



รูปที่ 3-18 สัดส่วนเรื่องร้องเรียนผ่าน 1212 OCC

3.5.5 เว็บไซต์อื่น ๆ

นอกจากนี้ ทางคณะผู้วิจัยได้ทำการรวบรวมข้อมูลจากเว็บไซต์มาเป็นข้อมูลประกอบการพิจารณาเพื่อใช้ในการพัฒนาระบบให้มีประสิทธิภาพมากที่สุด โดยได้ทำการรวบรวมข้อมูลจากเว็บไซต์ต่าง ๆ ดังนี้

เว็บไซต์ Verme เป็นเว็บไซต์ที่มีการพัฒนามาเป็นแพลตฟอร์มเพื่อใช้ในการยืนยันตัวตนผู้ขายของออนไลน์ตาม Facebook, Line, Instagram, Twitter และเว็บบอร์ดต่าง ๆ เพื่อให้ผู้ซื้อมั่นใจว่าชำระเงินกับคนที่มีตัวตนจริง ๆ โดยผู้ขายจะมี บัตร VerME ในการยืนยันตัวตนว่าเป็นผู้ขายจริงไม่ใช่มิจฉาชีพทางฝั่งผู้ซื้อสามารถนำ ID บนบัตร VerME ของผู้ขายไปตรวจสอบได้เพื่อให้เกิดความมั่นใจในการซื้อขายกัน (Verme, 2565)

เว็บไซต์ Blacklistseller เป็นเว็บไซต์ที่ร่วมต้านภัยฉ้อโกงออนไลน์โดนผู้เสียหายที่โดนมิจฉาชีพออนไลน์โกงเงินสามารถนำข้อมูลเหล่านั้นมาสร้างเป็นรายงานและฐานข้อมูลเพื่อช่วยในการเตือนสังคมป้องกันไม่ให้มีผู้โดนหลอกเพื่อมากขึ้น (Blacklistseller, 2565)

เว็บไซต์เช็คคนโกง เป็นเว็บไซต์เว็บไซต์สำหรับเช็คคนโกง หลอกให้โอนเงินสำหรับการซื้อของออนไลน์ ผู้ใช้ควรเช็คก่อนโอนเงิน ผู้ที่โดนโกงสามารถโพส ใส่ข้อมูลไม่ครบถ้วน เช่น ชื่อ นามสกุล บัญชีที่

โอน วันที่โอน หลักฐานการแจ้งความ หรือข้อมูลการแชท ที่ช่วยให้ผู้ซื้อทำการเช็คคนโกงได้ก่อนการโอนเงิน โดยเช็คให้ชัวร์ก่อนโอน เช็คชื่อ เช็คเลขที่บัญชี เช็คเบอร์โทรศัพท์ เช็คทุกอย่างที่ทราบข้อมูล ลองค้นหาใน Google หรือ Facebook แม้กระทั่ง Twitter แล้วนำข้อมูลเหล่านั้นมาเช็คในเว็บคนโกง.com (เช็คคนโกง, 2565)

เว็บไซต์ Whoscheat เป็นเว็บไซต์สำหรับตรวจสอบข้อมูลมิจฉาชีออนไลน์เช่นกัน โดยในระบบมีการทำการตรวจสอบเลขบัญชีธนาคารของมิจฉาชีพ เบอร์โทรศัพท์มือถือ เลขประจำตัวประชาชน และชื่อ-นามสกุล ของมิจฉาชีพ เพื่อเป็นการป้องการให้ไม่โดนโกงเช่นกัน (Whoscheat, 2565)

เว็บไซต์ pantipmarket เป็นเว็บไซต์สำหรับซื้อขายของออนไลน์ซึ่งการซื้อขายของในหลายสินค้าและหมวดเช่นเดียวกัน ตัวอย่าง ซื้อ-ขายอสังหาริมทรัพย์ ซื้อ-ขายพระเครื่อง ซื้อ-ขายยานพาหนะ ซื้อ-ขายคอมพิวเตอร์ และอื่น ๆ มากมาย ซึ่งนอกจากเว็บไซต์ pantipmarket จะเป็นแพลตฟอร์มจะสร้างพื้นการซื้อ-ขายสินค้าต่าง ๆ ตัวระบบยังมีการสร้างรายการเลขที่บัญชีที่หลอกลวง และรายการสินค้าที่ถูกขโมย อีกด้วย

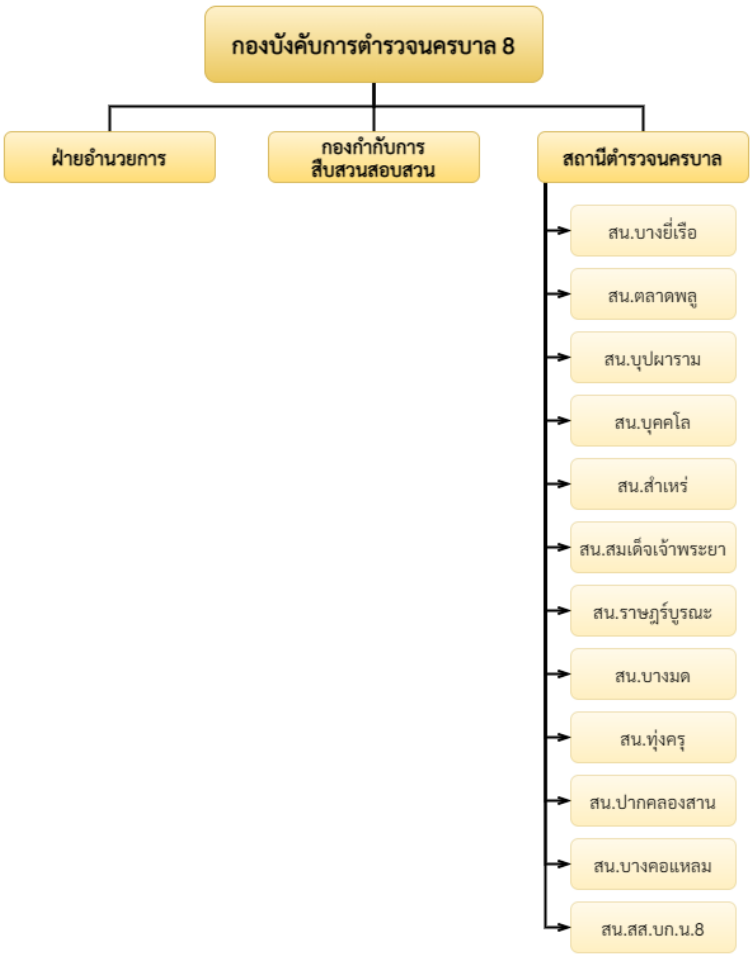
จากการรีวิวรวบรวมเว็บไซต์ต่าง ๆ ที่มีการให้ข้อมูลเกี่ยวกับมิจฉาออนไลน์ คนโกง คนหลอกลวง ผู้วิจัยได้ทำการเก็บข้อมูลต่าง ๆ เหล่ามาพัฒนาเป็นระบบเว็บไซต์ของฉลาดโอนเกิดขึ้นโดยใช้งานได้ทั้งบนคอมพิวเตอร์และมือถือ โดยตัวระบบของเว็บไซต์ฉลาดโอนสามารถตรวจสอบข้อมูลของผู้รับโอน ก่อนเชื่อก่อนโอนได้ซึ่งจะเช็ค ชื่อบัญชีธนาคาร เลขที่บัญชีธนาคาร/พร้อมเพย์/ทรูวอลเล็ต SMS หรือเบอร์โทร และเช็คตัวตนผู้ขาย อีกทั้งยังช่วยรวบรวมหลักฐานจากผู้โดนโกงเพื่อนำไปดำเนินคดีต่อไป

บทที่ 4
ผลการศึกษา และรวบรวมข้อมูลเกี่ยวกับกฎเกณฑ์ และระเบียบปฏิบัติของพนักงานสอบสวน

บทที่ 4 นี้ จัดทำขึ้นเพื่อแสดงรายละเอียดของผลการศึกษา และรวบรวมข้อมูลเกี่ยวกับกฎเกณฑ์และระเบียบปฏิบัติของพนักงานสอบสวน เพื่อใช้เป็นแนวทางและหลักเกณฑ์ ในการรวบรวมพยานหลักฐานและดำเนินคดีธุรกรรมออนไลน์ของมิจฉาชีพที่ไม่ระบุตัวตน โดยมีขอบเขตการศึกษาในพื้นที่กองบังคับการตำรวจนครบาล 8 (บก.น.8) สำหรับการศึกษาในระยะที่ 1

4.1 รายละเอียดของพื้นที่ที่ศึกษา

กองบังคับการตำรวจนครบาล 8 (บก.น. 8) มีหน่วยงานในสังกัดรวม 13 หน่วยงาน ประกอบด้วย ฝ่ายอำนวยการ กองกำกับการสืบสวนสอบสวน และสถานีตำรวจนครบาล โดยมีสถานีตำรวจในสังกัดจำนวน 11 แห่ง ดังนี้



รูปที่ 4-1 โครงสร้างหน่วยงานกองบังคับการตำรวจนครบาล 8

โดยสถานีตำรวจนครบาลแต่ละแห่ง มีผู้บังคับบัญชา แสดงรายชื่อดังตารางที่ 4-1

ตารางที่ 4-1 รายชื่อผู้บังคับบัญชาของสถานีตำรวจนครบาลแต่ละแห่ง

สถานีตำรวจนครบาล	ผู้บังคับบัญชา
สน.บางยี่เรือ	พ.ต.อ.ดุสิต วาลีประโคน
สน.ตลาดพลู	พ.ต.อ.ธนา มลิงาม
สน.บุปผาราม	พ.ต.อ.วิวัฒนชัย บุญญานุพงศ์
สน.บุคคโล	พ.ต.อ.สายชล ปัญจชัย
สน.สำเหร่	พ.ต.อ.ฉัฐกิตติ์ ผดุงจันทน์ธนัย
สน.สมเด็จเจ้าพระยา	พ.ต.อ.มหพล สายหยุด
สน.ราษฎร์บูรณะ	พ.ต.อ.ภัสพงษ์ บุตรไทย
สน.บางมด	พ.ต.อ.ปริญญา เหลืองอุทัย
สน.ทุ่งครุ	พ.ต.อ.ธีรศักดิ์ ภิญโญ
สน.ปากคลองสาน	พ.ต.อ.ต่อศักดิ์ ปานกลิ่นพุฒ
สน.บางคอแหลม	พ.ต.อ.ปิยะกรณ์ ศรีวันทา
สน.สส.บก.น.8	พ.ต.อ.นิภพล สุขนิยม

*ข้อมูล ณ วันที่ 10 ก.ค. 64

จากส่วนงานตามที่กล่าวมาดังรูปที่ 4-1 สามารถแจกแจงรายละเอียดหน้าที่และความรับผิดชอบของแต่ละส่วนงานได้ ดังนี้

1. ฝ่ายอำนวยการ

มีอำนาจหน้าที่และความรับผิดชอบ ดังนี้

(1) งานธุรการและงานสารบรรณ
(2) งานบริหารงานบุคคล
(3) งานคดีและวินัย
(4) งานนโยบายและแผน และงานยุทธศาสตร์
(5) งานการเงินและงานบัญชี
(6) งานงบประมาณ
(7) งานส่งกำลังบำรุง
(8) งานสวัสดิการ
(9) งานช่วยอำนวยการและงานเลขานุการ
(10) งานเทคโนโลยีสารสนเทศและการสื่อสาร
(11) งานประชาสัมพันธ์และเผยแพร่ข้อมูลข่าวสาร
(12) งานศึกษาอบรม
(13) งานการข่าว
(14) งานบันทึก ตรวจสอบ ควบคุม และรายงานข้อมูลสถานภาพกำลังพลของข้าราชการตำรวจในสังกัด รวมทั้งตรวจสอบดังกล่าวกับฐานข้อมูลกำลังพลกลางของสำนักงานตำรวจแห่งชาติ

และดำเนินการเพื่อให้ข้อมูลสถานภาพกำลังในความรับผิดชอบเป็นไปอย่างถูกต้องและเป็นปัจจุบัน

(15) งานคณะกรรมการตรวจสอบและติดตามการบริหารงานตำรวจ

(16) งานศูนย์รวมข่าวสารทั้งทางวิทยุ โทรศัพท์ โทรสาร โทรพิมพ์ และติดต่อประสานการข่าวระหว่างกองบังคับการตำรวจนครบาลกับกองบัญชาการตำรวจนครบาล สถานีตำรวจนครบาล สำนักงานตำรวจแห่งชาติ รวมทั้งส่วนราชการและหน่วยงานต่าง ๆ ที่เกี่ยวข้อง

(17) งานศูนย์ควบคุม สั่งการ ตรวจสอบ รับและส่งข้อมูล รับแจ้งเหตุด่วนเหตุร้าย เหตุสัญญาณและแจ้งภัยต่าง ๆ ให้กับสายตรวจ รวมทั้งรายงานคดีอาญาตามที่ระเบียบกำหนดให้ผู้บังคับบัญชาและส่วนราชการที่เกี่ยวข้องทราบ

(18) งานจัดทำรหัสสัญญาณเรียกขานทางวิทยุประจำตัวข้าราชการตำรวจชั้นสัญญาบัตร หน่วยงาน และชุดปฏิบัติการ รวมตลอดถึงยานพาหนะในสังกัด

(19) ดำเนินการเกี่ยวกับงานเทคโนโลยีสารสนเทศ โดยการปรับปรุงพัฒนาให้มีความทันสมัยและใช้งานได้อย่างมีประสิทธิภาพ

(20) ดำเนินการเกี่ยวกับการนำระบบเทคโนโลยีสารสนเทศมาประยุกต์ใช้ในการสนับสนุนงานป้องกันและปราบปรามอาชญากรรม รวมทั้งงานสืบสวนสอบสวนคดีอาญา

(21) เป็นศูนย์กลางรวบรวมข้อมูลต่าง ๆ ด้วยระบบคอมพิวเตอร์เพื่อใช้สนับสนุนการจัดการป้องกันและปราบปรามอาชญากรรมของกองบังคับการตำรวจนครบาล โดยรวบรวมข้อมูลที่มีอยู่มาใช้ในการประมวลผล เพื่อให้ได้สารสนเทศที่สามารถใช้ในการวางแผน การควบคุม และการประเมินผลการปฏิบัติงานของเจ้าหน้าที่ตำรวจ และให้บริการแก่หน่วยงานที่เกี่ยวข้องหรือส่วนราชการต่าง ๆ ที่สอบถามข้อมูล

(22) วางระเบียบ ข้อบังคับที่เกี่ยวกับการจัดการส่งข้อมูล การปรับปรุงข้อมูลและการแก้ไขข้อมูลทั้งทางเอกสารและเครือข่ายคอมพิวเตอร์ ของกองบังคับการตำรวจนครบาล

(23) ประสานงาน อำนวยการ และเร่งรัดหน่วยงานต่าง ๆ ที่มีหน้าที่จัดส่งข้อมูลทั้งหมดทางเอกสารและทางเครือข่ายคอมพิวเตอร์ ให้จัดส่งข้อมูลและจัดการข้อมูลตามระเบียบที่กำหนด

(24) ประมวลเหตุการณ์ประจำวันและเหตุการณ์พิเศษที่เกิดขึ้นในเขตพื้นที่กองบังคับการตำรวจนครบาล

(25) รวบรวมทำบัตรดรรชนีบุคคลพ้นโทษและกู้ภัยท้องถิ่น เพื่อประโยชน์ในการประสานงานกับสถานีตำรวจนครบาลพื้นที่ในการสอดส่องพฤติการณ์

(26) รวบรวมประวัติและวิธีการประทุษกรรมของคนร้ายบางประเภทในเขตพื้นที่รับผิดชอบของกองบังคับการตำรวจนครบาล เพื่อประโยชน์ในการสืบสวนจับกุม

(27) รวบรวมดรรชนีบุคคลอันธพาลที่สถานีตำรวจนครบาลส่งมา โดยแยกเก็บไว้ตามระบบดรรชนี

(28) รวบรวมภาพถ่ายของคนร้ายบางประเภทพร้อมทั้งดรรชนีไว้เพื่อประโยชน์ในการสืบสวนจับกุม

(29) ปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือที่ได้รับมอบหมาย

(30) งานอื่น ๆ ที่เกี่ยวข้องหรือมิได้อยู่ในหน้าที่ของฝ่ายใดโดยเฉพาะ

(31) งานอื่น ๆ ที่ผู้บังคับบัญชามอบหมาย

2. กองกำกับการสืบสวนสอบสวน

มีอำนาจหน้าที่และความรับผิดชอบเกี่ยวกับงานสืบสวนสอบสวนคดีอาญาตามประมวลกฎหมายวิธีพิจารณาความอาญาและกฎหมายอันเกี่ยวกับความผิดอาญาทั้งหลาย ในเขตอำนาจการรับผิดชอบของกองบังคับการตำรวจนครบาล รวมทั้งปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือที่ได้รับมอบหมาย

3. สถานีตำรวจนครบาล

มีอำนาจหน้าที่และความรับผิดชอบ ดังนี้

(1) ดำเนินการในการถวายความปลอดภัยสำหรับองค์พระมหากษัตริย์ พระราชินี พระรัชทายาท ผู้สำเร็จราชการแทนพระองค์ พระบรมวงศานุวงศ์ ผู้แทนพระองค์ พระราชอาคันตุกะและบุคคลสำคัญอื่น ๆ ในเขตอำนาจการรับผิดชอบ

(2) งานสืบสวนสอบสวนคดีอาญา ตลอดจนดำเนินการตามขั้นตอนต่าง ๆ ตามประมวลกฎหมายวิธีพิจารณาความอาญาและกฎหมายอื่นอันเกี่ยวกับความรับผิดอาญาทั้งหลายในเขตอำนาจการรับผิดชอบ

(3) งานป้องกันและปราบปรามอาชญากรรม การรักษาความสงบเรียบร้อย การให้ความปลอดภัยแก่ประชาชน และการให้บริการช่วยเหลือประชาชนในรูปแบบต่าง ๆ

(4) งานส่งเสริมและสนับสนุนให้ท้องถิ่นหรือชุมชนมีส่วนร่วมในกิจกรรมตำรวจ เพื่อป้องกันและปราบปรามการกระทำความผิดอาญา รักษาความสงบเรียบร้อยและรักษาความปลอดภัยของประชาชนตามความเหมาะสมและความต้องการของแต่ละพื้นที่

(5) งานจัดการจราจรในเขตอำนาจการรับผิดชอบ

(6) ให้การสนับสนุนการบรรเทาสาธารณภัยในเขตอำนาจการรับผิดชอบ

(7) ควบคุม ดูแลร้านค้าของเก่าให้ปฏิบัติตามกฎหมาย

(8) ควบคุม ดูแล และสอดส่องการเรี่ยไรให้เป็นไปตามกฎหมายเป็นเจ้าหน้าที่ทะเบียนคนต่างด้าวตามกฎหมายว่าด้วยการทะเบียนคนต่างด้าว

(9) งานคณะกรรมการตรวจสอบและติดตามการบริหารงานตำรวจ

(10) งานอื่น ๆ ที่ผู้บังคับบัญชามอบหมาย

4.2 หลักเกณฑ์และระเบียบปฏิบัติที่ใช้ในปัจจุบัน เมื่อเกิดคดีฉ้อโกงออนไลน์

เมื่อเกิดเหตุกรณีฉ้อโกงออนไลน์ขึ้น ผู้เสียหายจะต้องเข้าแจ้งความกับเจ้าหน้าที่ตำรวจ ณ สถานีตำรวจท้องที่ที่เกิดเหตุฉ้อโกงออนไลน์ขึ้น ภายในระยะเวลา 3 เดือน นับจากวันที่ทราบเรื่อง โดยเตรียมหลักฐานต่าง ๆ อย่างน้อย ดังนี้

(1) รูปภาพของผู้ขายสินค้า

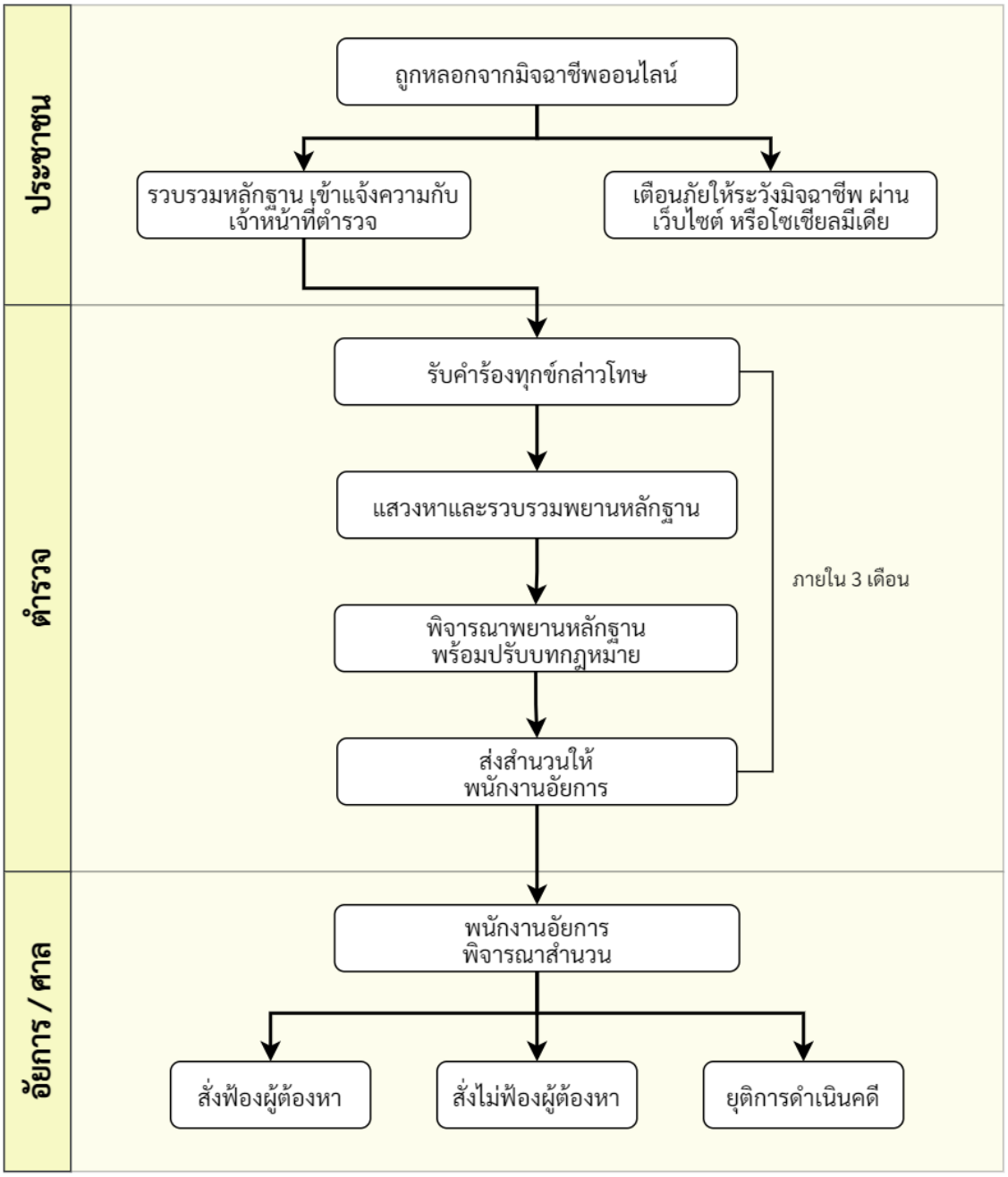
(2) โพสต์ประกาศซื้อหรือขายสินค้า

(3) ข้อความการพูดคุยระหว่างผู้ซื้อและผู้ขาย

(4) ชื่อบัญชีและเลขบัญชีธนาคารที่โอนเงินไป

(5) สลิปหรือภาพหลักฐานการโอนเงินชำระค่าสินค้า

จากนั้นพนักงานสอบสวนประจำสถานีตำรวจจะดำเนินการตามขั้นตอนตั้งแต่ รับเรื่อง สืบสวน พิจารณาหลักฐาน และส่งสำนวนต่อให้อัยการเพื่อพิจารณาสั่งฟ้องหรือสั่งไม่ฟ้องต่อไป แสดงขั้นตอนการดำเนินการของเจ้าหน้าที่ตำรวจ ดังรูปที่ 4-2



รูปที่ 4-2 ขั้นตอนการแจ้งความเมื่อถูกฉ้อโกง

การดำเนินการ ในส่วนของเจ้าหน้าที่ตำรวจเกี่ยวกับคดีฉ้อโกงออนไลน์ มี 4 ขั้นตอน ได้แก่

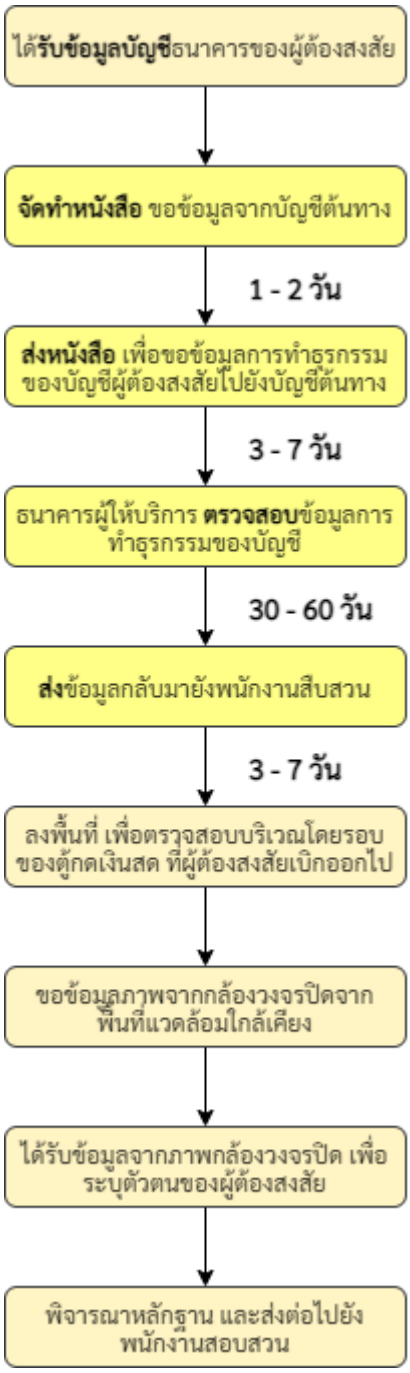
1. รับคำร้องทุกข์กล่าวโทษ

พนักงานสอบสวนเวร จะปฏิบัติหน้าที่เพื่อรับคำร้องทุกข์หรือคำกล่าวโทษ เมื่อดำเนินการแล้วจะลงบันทึกประจำวัน เป็นหลักฐานเอาไว้ ในขั้นตอนนี้ จะมีข้อพิจารณาเบื้องต้น เช่น (1) กรณีที่ได้รับแจ้ง

เป็นคดีอาญาหรือไม่, (2) ผู้แจ้งเป็นผู้เสียหายหรือผู้กล่าวโทษหรือไม่, (3) อยู่ในเขตอำนาจสอบสวนหรือไม่ เป็นต้น โดยเมื่อพนักงานสอบสวนเวรได้ข้อสรุปเบื้องต้นแล้ว ก็จะดำเนินการในขั้นตอนถัดไป

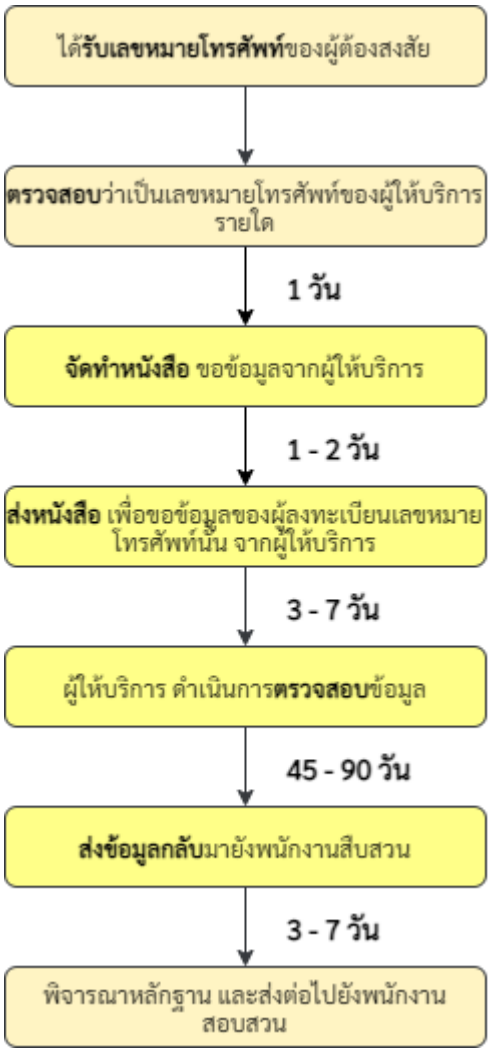
2. แสวงหาและรวบรวมพยานหลักฐาน

ขั้นตอนนี้เป็นขั้นตอนสำคัญของการสืบสวนเพื่อพิสูจน์ตัวตนของผู้กระทำความผิด ของคดีฉ้อโกงออนไลน์ โดยมิจฉาชีพจะใช้เครื่องมือหลัก ๆ ในการดำเนินการฉ้อโกงออนไลน์ ได้แก่ ช่องทางการชำระสินค้า ซึ่งจะอยู่ในรูปแบบของบัญชีเงินฝากธนาคาร หรือกระเป๋าสตางค์อิเล็กทรอนิกส์ (E-Wallet) เพราะเป็นช่องทางให้ผู้เสียหายชำระสินค้ามายังมิจฉาชีพได้ กรณีที่เป็นบัญชีเงินฝากของธนาคาร จะถือว่าเป็นช่องทางมีที่มาตรฐานความปลอดภัยระดับหนึ่ง มีธนาคารพาณิชย์อันเป็นสถาบันการเงินตามกฎหมายเป็นผู้รับผิดชอบ โดยมีธนาคารแห่งประเทศไทยเป็นผู้ควบคุมดูแล และผู้ที่จะเปิดบัญชีเงินฝากกับธนาคารพาณิชย์ต้องยืนยันตัวตนอย่างชัดเจน ธนาคารพาณิชย์ซึ่งเป็นผู้รับผิดชอบบัญชีเงินฝากเหล่านั้น จึงต้องปฏิบัติตามที่พนักงานสอบสวนสั่งการในอำนาจตามกฎหมายเสมอ และการดำเนินการต่าง ๆ ของธนาคารนั้นสามารถทำการตรวจสอบได้ ส่วนกระเป๋าสตางค์อิเล็กทรอนิกส์นั้น ผู้ให้บริการกระเป๋าสตางค์อิเล็กทรอนิกส์บางรายไม่ได้มีการตรวจสอบหรือให้ผู้เข้ารับบริการเปิดบัญชีต้องยืนยันตัวตนอย่างละเอียด และผู้ให้บริการบางรายยังไม่ได้ผ่านการรับรองหรือตรวจสอบการดำเนินงานจากธนาคารแห่งประเทศไทย จึงทำให้ยากต่อการตรวจสอบหลักฐานการดำเนินการต่างๆจากพนักงานสอบสวนอย่างยิ่ง โดยกระบวนการตรวจสอบข้อมูลจากบัญชีเงินฝากธนาคาร แสดงดังรูปที่ 4-3 และกระบวนการตรวจสอบข้อมูลจากกระเป๋าสตางค์อิเล็กทรอนิกส์ แสดงดังรูปที่ 4-4



รูปที่ 4-3 กระบวนการตรวจสอบข้อมูล กรณีเป็นบัญชีเงินฝากธนาคาร

จากรูป 4-3 แสดงขั้นตอนการตรวจสอบข้อมูลจากบัญชี เริ่มจากพนักงานสอบสวนได้รับข้อมูลบัญชีธนาคารของผู้ต้องสงสัย จากนั้นส่งเรื่องขอข้อมูลการทำธุรกรรมของบัญชีผู้ต้องสงสัย ไปยังธนาคารต้นทาง รอให้ทางธนาคารแจ้งข้อมูลของเจ้าของบัญชีผู้ต้องสงสัย และเส้นทางการทำธุรกรรมของบัญชีผู้ต้องสงสัย กลับมายังพนักงานสืบสวน ซึ่งโดยส่วนใหญ่จะใช้ระยะเวลาประมาณ 45 - 90 วัน จากนั้นพนักงานสืบสวนจะลงพื้นที่ เพื่อตรวจสอบสถานที่ ที่ผู้ต้องสงสัยได้เบิกเงินออกไป หลังจากนั้นระบุตัวตนของผู้ต้องสงสัยโดยขอข้อมูลจากกล้องวงจรปิดในพื้นที่ใกล้เคียง แล้วจึงส่งหลักฐานทั้งหมดไปยังพนักงานสอบสวน



รูปที่ 4-4 กระบวนการตรวจสอบข้อมูล กรณีเป็นกระเป๋าสตางค์อิเล็กทรอนิกส์

จากรูป 4-4 แสดงขั้นตอนการตรวจสอบข้อมูล กรณีผู้ต้องสงสัยทำธุรกรรมผ่านกระเป๋าสตางค์อิเล็กทรอนิกส์ พนักงานสืบสวน จะใช้เลขหมายโทรศัพท์ที่ได้จากกระเป๋าสตางค์อิเล็กทรอนิกส์ มาสืบหาข้อมูลว่าเป็นเลขหมายของผู้ให้บริการรายใด แล้วจึงสอบถามข้อมูลผู้ลงทะเบียนที่เป็นเจ้าของเลขหมายไปยังผู้ให้บริการโทรศัพท์ โดยจะใช้เวลาประมาณ 4 - 5 เดือน จึงจะได้รับข้อมูลกลับมาจากผู้ให้บริการโทรศัพท์ จากนั้นดำเนินการพิจารณาหลักฐานและส่งต่อไปยังพนักงานสอบสวน

อีกหนึ่งเครื่องมือในการจำหน่ายสินค้าผ่านระบบอิเล็กทรอนิกส์ คือ ช่องทางการขายสินค้า สามารถแบ่งออกเป็นสองกลุ่มใหญ่ ๆ ได้แก่

(1) เว็บไซต์หรือแอปพลิเคชันที่เป็นสื่อกลางในการขายสินค้า โดยผู้ที่จะมาขายสินค้าในเว็บไซต์เหล่านี้ จะต้องมีการลงทะเบียนเพื่อยืนยันตัวตนก่อนเข้าใช้งานระบบ อาจมีการใช้เลขบัตรประจำตัวประชาชนหรือเลขหมายโทรศัพท์สำหรับการลงทะเบียนยืนยันตัวตน สำหรับช่องทางนี้ ผู้ซื้อจะเลือกซื้อสินค้าผ่านเว็บไซต์ เมื่อมีการตกลงซื้อสินค้าแล้ว การชำระสินค้าจะใช้วิธีการชำระผ่านระบบกลางของเว็บไซต์หรือแอปพลิเคชัน เนื่องจากการใช้บริการเว็บไซต์ประเภทนี้ อาจมีค่าธรรมเนียมเพื่อเป็นรายได้ของเว็บไซต์ จึงไม่เป็นที่นิยมของมิจฉาชีพ และ

หากพบว่ามีการทุจริตในการซื้อขายแล้ว ผู้ซื้ออาจขอข้อมูลผู้ขายจากผู้ดูแลเว็บไซต์ระบบกลางเหล่านี้ได้

(2) แอปพลิเคชันเครือข่ายสังคมออนไลน์ (Social Network) สื่อกลางติดต่อระหว่างผู้ซื้อกับผู้ขาย โดยผู้ขายจะต้องเปิดบัญชีผู้ใช้กับเว็บไซต์เหล่านั้นก่อน จึงจะทำการนำเสนอสินค้าของตนผ่านบัญชีผู้ใช้ในต่าง ๆ ได้ เมื่อมีผู้ซื้อสนใจ จะติดต่อกับผู้ขายโดยตรง และชำระสินค้าผ่านบัญชีเงินฝากของธนาคารหรือกระเป๋าสตางค์อิเล็กทรอนิกส์ หากผู้ขายเป็นมิจฉาชีพ เมื่อได้รับเงินแล้ว อาจจะไม่ส่งสินค้าไปให้ผู้ซื้อตามที่กำหนด และปิดบัญชีผู้ใช้งานของบัญชีนั้น ๆ ทำให้ผู้ซื้อไม่สามารถติดต่อกับผู้ขายได้ มิจฉาชีพจึงใช้ช่องว่างของการสมัครสมาชิกบนแอปพลิเคชันต่าง ๆ ที่ไม่ต้องมีการยืนยันตัวตน ในการฉ้อโกงจากผู้ซื้อหลาย ๆ คน โดยปัญหาใหญ่ของบัญชีผู้ใช้เหล่านี้คือ มีฐานข้อมูลอยู่ที่ต่างประเทศทั้งสิ้น เช่น Facebook, Line, Instagram จึงทำให้พนักงานสอบสวนติดตามขอเบาะแสข้อมูลของบัญชีผู้ใช้ต่าง ๆ ได้ยากลำบาก ไม่สามารถเชื่อมโยงเส้นทางการจราจรของข้อมูลทางอินเตอร์เน็ตได้อย่างชัดเจน จึงไม่สามารถค้นหาไอพีแอดเดรสซึ่งเป็นที่ตั้งของการทำธุรกรรมผ่านระบบอินเตอร์เน็ต ว่าผู้ต้องหาก่อเหตุอยู่ที่ใด และถึงแม้จะรู้ไอพีแอดเดรสที่แท้จริงของที่ตั้งที่ผู้ต้องหาใช้ทำการแล้ว ก็ไม่อาจพิสูจน์ได้ชัดเจนว่า ผู้ใดเป็นผู้ป้อนข้อมูลและกระทำการอยู่ในเวลาเกิดเหตุ

3. พิจารณาพยานหลักฐานพร้อมปรับบทกฎหมาย

การพิจารณาพยานหลักฐานของเจ้าหน้าที่สอบสวน มีขั้นตอนดังนี้

(1) ข้อเท็จจริงที่เกี่ยวกับการกระทำ

การพิจารณาจากพยานหลักฐานที่รวบรวมมา

(2) กฎหมายที่เกี่ยวข้องกับการกระทำ

การนำข้อเท็จจริงที่เกิดขึ้นในคดีมาปรับกับตัวบทกฎหมายและวินิจฉัยชี้ขาดว่าข้อเท็จจริงนั้นมีผลทางกฎหมายอย่างไร การกระทำเหล่านั้นเป็นความผิดอย่างไร ฐานใด ชอบด้วยกฎหมายมีสิทธิตามกฎหมายที่จะกระทำได้หรือไม่ เป็นต้น

(3) ความเห็นทางคดีของพนักงานสอบสวน

พนักงานสอบสวนผู้รับผิดชอบ สรุปสำนวนการสอบสวนโดยต้องประกอบด้วยข้อเท็จจริงและความเห็นในข้อเท็จจริงที่ได้จากพนักงานเจ้าหน้าที่

(4) เสนอผู้บังคับบัญชาพิจารณา

พนักงานสอบสวนผู้รับผิดชอบ เสนอสำนวนสอบสวนต่อผู้บังคับบัญชา เพื่อพิจารณาเสนอพนักงานอัยการต่อไป

4. ส่งสำนวนให้พนักงานอัยการ

ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 140-144 พนักงานสอบสวนจะต้องทำความเห็นหลังจากรวบรวมหลักฐานแล้ว ว่าเห็นควร อย่างไร "เห็นควรสั่งฟ้อง" "เห็นควรสั่งไม่ฟ้อง" ในคดีที่ไม่ทราบตัวผู้กระทำความผิด ให้มีความเห็น "เห็นควรงดการสอบสวน" จากนั้นดำเนินการส่งเรื่องต่อไปยังพนักงานอัยการเพื่อให้ลงความเห็นต่อไป

4.3 ผลการศึกษาระบบสารสนเทศที่มีความเกี่ยวข้องกับโครงการ

ในปัจจุบัน สำนักงานตำรวจแห่งชาติต้องทำงานร่วมกับข้อมูลจำนวนมาก จึงจำเป็นอย่างยิ่งที่จะใช้เทคโนโลยีสารสนเทศมาประยุกต์ใช้ในการทำงาน จึงมีการพัฒนาระบบเทคโนโลยีสารสนเทศเพื่อสนับสนุนการทำงานของเจ้าหน้าที่ตำรวจ ทางคณะผู้วิจัยจึงได้ศึกษาระบบสารสนเทศที่มีความเกี่ยวข้องกับโครงการจะช่วยในการควบคุมอาชญากรรมในสังคมดิจิทัล

4.3.1 ระบบสารสนเทศที่ตำรวจใช้ในปัจจุบัน

ชื่อระบบ	คำอธิบาย	พิจารณาข้อมูลและความเกี่ยวข้องกับโครงการ
1. ระบบสารสนเทศของสำนักงานตำรวจแห่งชาติ		
1.1 ระบบสารสนเทศสำหรับผู้ใช้งานระดับสถานีตำรวจ		
1.1.1 ระบบสารสนเทศ ตร. (Police Information System : POLIS)	โครงการพัฒนาศูนย์ข้อมูลข้อสนเทศ (Police Information System : POLIS) มีระบบงาน 6 กลุ่ม ประกอบด้วย 26 ฐานข้อมูล	
กลุ่มที่ 1 ระบบสารสนเทศอาชญากรรม (Crime Information System : CIS)	ประกอบด้วยระบบงานย่อย 12 ฐานข้อมูล	
1) ระบบฐานข้อมูลทะเบียนยานพาหนะ	เป็นระบบงานบริการสอบถามข้อมูลเกี่ยวกับทะเบียนยานพาหนะ และข้อมูลที่เกี่ยวข้องกับรถที่จดทะเบียน ซึ่งสำนักงานตำรวจแห่งชาติได้ทำบันทึกข้อตกลง (MOU) กับกรมการขนส่งทางบก กระทรวงคมนาคม โดยพัฒนาระบบสอบถามข้อมูลทะเบียนยานพาหนะให้ข้าราชการตำรวจที่มีหน้าที่ที่เกี่ยวข้องใช้ในการสืบสวน สอบสวนและป้องกันปราบปรามอาชญากรรม เบื้องต้นเป็นการทำสำเนา (Copy) ข้อมูลจากกรมการขนส่งทางบกมาเก็บไว้ที่เครื่องแม่ข่ายของระบบ POLIS และส่งข้อมูลเฉพาะที่มีการปรับปรุงมาเก็บในทุก ๆวัน แต่ปัจจุบันได้ใช้รูปแบบ Web Service หมายถึง	มีความเกี่ยวข้องกับระบบที่พัฒนาขึ้น ซึ่งจะกล่าวในบทต่อไป

ชื่อระบบ	คำอธิบาย	พิจารณาข้อมูลและความเกี่ยวข้องกับโครงการ
	การสอบถามข้อมูลจากเครื่องคอมพิวเตอร์	
2) ระบบฐานข้อมูลใบอนุญาตขับรถ	เป็นระบบงานบริการสอบถามข้อมูลใบอนุญาตขับรถและใบอนุญาตผู้ประจำรถ มีลักษณะการทำงานเช่นเดียวกับข้อ 1	มีความเกี่ยวข้องกับระบบที่พัฒนาขึ้น ซึ่งจะกล่าวในบทต่อไป
3) ระบบฐานข้อมูลทะเบียนอาวุธปืน	เป็นระบบงานบันทึก/แก้ไข/สอบถามข้อมูลใบอนุญาตให้มีและใช้อาวุธปืน ข้อมูลการโอนย้ายทะเบียนอาวุธปืน	ไม่มีความเกี่ยวข้อง
4) ระบบฐานข้อมูลใบอนุญาตพกพาอาวุธปืน	เป็นระบบงานบริการบันทึก/แก้ไข/สอบถามข้อมูลเกี่ยวกับใบอนุญาตพกพาอาวุธปืน	ไม่มีความเกี่ยวข้อง
5) ระบบฐานข้อมูลบุคคลผู้กระทำผิดกฎหมาย (รวมเด็กและเยาวชน)	เป็นระบบการบันทึก/แก้ไข/สอบถามข้อมูลประวัติผู้กระทำผิดกฎหมาย ข้อมูลแผนประทุษกรรมและประวัติผู้ต้องหา ข้อมูลผลคดีผู้ต้องหาและรายงานที่เกี่ยวข้องซึ่งกองทะเบียนประวัติจะเป็นผู้รับผิดชอบในการดำเนินการ	มีความเกี่ยวข้องกับระบบที่พัฒนาขึ้น ซึ่งจะกล่าวในบทต่อไป
6) ระบบฐานข้อมูลสถิติคดีอาชญากรรม	เป็นระบบที่นำข้อมูลจากระบบฐานข้อมูลติดตามผลคดีมาจัดทำเป็นรายงาน สถิติ เพื่อให้หน่วยงานระดับบริหารใช้ในการวิเคราะห์วางแผนปฏิบัติการสำหรับการป้องกันปราบปราม	มีความเกี่ยวข้องกับระบบที่พัฒนาขึ้น ซึ่งจะกล่าวในบทต่อไป
7) ระบบฐานข้อมูลอุบัติเหตุจราจร	เป็นระบบการบันทึกข้อมูล/แก้ไข/สอบถามข้อมูลรายละเอียดเกี่ยวกับคดีจราจรทั้งในส่วนที่เป็นอุบัติเหตุจราจรทางบก และไม่เป็นอุบัติเหตุจราจรทางบก ตั้งแต่รับคดีจนถึงผลการตัดสินคดีจากชั้นศาล	ไม่มีความเกี่ยวข้อง
8) ระบบฐานข้อมูลทรัพย์หาย	เป็นระบบการบันทึก/แก้ไข/สอบถามข้อมูลรถยนต์หาย รถหายได้คืน รถหายเบื้องต้น พิมพ์	ไม่มีความเกี่ยวข้อง

ชื่อระบบ	คำอธิบาย	พิจารณาข้อมูลและความเกี่ยวข้องกับโครงการ
	ประกาศ ถอนประกาศรถหาย รวมถึงทรัพย์หาย ฯลฯ ซึ่งกองทะเบียนประวัติจะเป็นผู้รับผิดชอบในการดำเนินการ	
9) ระบบฐานข้อมูลบุคคลพลัดหลง	เป็นการเก็บข้อมูลโดยกระบวนการทำงานเริ่มตันสถานีตำรวจส่งตำหนิรูปพรรณรายละเอียดพร้อมภาพถ่ายตามแบบแจ้งรูปพรรณบุคคลพลัดหลงมายังกองทะเบียนประวัติอาชญากร เพื่อจัดพิมพ์ประกาศสืบหาบุคคลพลัดหลงและในกรณีที่ได้บุคคลพลัดหลงคืนให้สถานีตำรวจส่งข้อมูลมาบันทึกปรับปรุงข้อมูลเพื่อพิมพ์ประกาศถอนการสืบค้นบุคคลพลัดหลงต่อไป	ไม่มีความเกี่ยวข้อง
10) ระบบฐานข้อมูลประกาศสืบจับ	เป็นระบบการบันทึก/แก้ไข/สอบถามประกาศสืบจับ พิมพ์ประกาศ ถอนประกาศ ซึ่งกองทะเบียนประวัติจะเป็นผู้รับผิดชอบในการดำเนินการ	มีความเกี่ยวข้องกับระบบที่พัฒนาขึ้น ซึ่งจะกล่าวในบทต่อไป
11) ระบบฐานข้อมูลบุคคลพ้นโทษ	เป็นระบบการบันทึก/แก้ไข/สอบถามข้อมูลประวัติอาชญากร/ที่อยู่/ตำหนิรูปพรรณรูปถ่าย/ประวัติการต้องโทษ/การพันโทษ ฯลฯ ซึ่งกองทะเบียนประวัติจะเป็นผู้รับผิดชอบในการดำเนินการ	มีความเกี่ยวข้องกับระบบที่พัฒนาขึ้น ซึ่งจะกล่าวในบทต่อไป
12) ระบบฐานข้อมูลบุคคลผู้มีพฤติการณ์ในทางมิชอบ (บุคคลน่าสนใจ)	จัดเก็บข้อมูลบุคคลที่ต้องคอยสอดส่องพฤติการณ์และติดตามความเคลื่อนไหวของบุคคลนั้น ๆ เพื่อใช้ในการสืบสวนสอบสวนคดี	มีความเกี่ยวข้องกับระบบที่พัฒนาขึ้น ซึ่งจะกล่าวในบทต่อไป
กลุ่มที่ 2 ระบบสารสนเทศเพื่อการ	ประกอบด้วยระบบงานย่อย ๔ ฐานข้อมูล ได้แก่	
1) ระบบฐานข้อมูลเงินเดือน	เป็นระบบการบันทึก/แก้ไข/สอบถามข้อมูลเงินเดือนข้าราชการตำรวจ ข้าราชการบำนาญ และ	ไม่มีความเกี่ยวข้อง

ชื่อระบบ	คำอธิบาย	พิจารณาข้อมูลและความเกี่ยวข้องกับโครงการ
	ลูกจ้าง ฯลฯ	
2) ระบบฐานข้อมูลกำลังพล	เป็นระบบการบันทึก/แก้ไข/สอบถามข้อมูลกำลังพลตำรวจ ประวัติ การแต่งตั้ง โอนย้าย เลื่อนเงินเดือน เลื่อนตำแหน่ง ฯลฯ	ไม่มีความเกี่ยวข้อง
3) ระบบฐานข้อมูลแผนงานและงบประมาณ	เป็นระบบการบันทึก/แก้ไข/สอบถามข้อมูลที่เกี่ยวข้องกับงบประมาณของสำนักงานตำรวจแห่งชาติ ทั้งการจัดตั้งและจัดสรรงบประมาณรายจ่ายประจำปี เพื่อประโยชน์ในการบริหารควบคุมและการกำกับดูแลงบประมาณรายจ่ายตลอดจนติดตามและประเมินผลการใช้จ่ายงบประมาณตามแผนงานโครงการของแต่ละหน่วยงานในสังกัดสำนักงานตำรวจแห่งชาติ	ไม่มีความเกี่ยวข้อง
4) ระบบฐานข้อมูลส่งกำลังบำรุง	เป็นระบบการบันทึก/แก้ไข/สอบถามข้อมูลเกี่ยวกับวัสดุครุภัณฑ์ การเบิกจ่าย การบำรุงรักษาและค่าใช้จ่ายในการซ่อม ฯลฯ	ไม่มีความเกี่ยวข้อง
กลุ่มที่ 3 ระบบสารสนเทศเพื่อความมั่นคง (Security Information System : SIS)	ประกอบด้วยระบบงานย่อย ๒ ฐานข้อมูล ได้แก่	
1) ระบบฐานข้อมูลทะเบียนกลางสันติบาล	เป็นระบบการบันทึก/แก้ไข/สอบถามข้อมูลเรื่องราวและเหตุการณ์ที่เกิดขึ้นในอดีตและปัจจุบัน ข้อมูลประวัติบุคคลที่มีพฤติการณ์ประวัติกลุ่มบุคคล หรืออาชญากร ฯลฯ	ไม่มีความเกี่ยวข้อง
2) ระบบฐานข้อมูลคนร้ายข้ามชาติ	เป็นระบบการบันทึก/แก้ไข/สอบถามข้อมูลประวัติคนร้ายข้ามชาติ และรายละเอียดประวัติคนร้ายซึ่งได้รับข้อมูลจากตำรวจสากลหรือหน่วยงานตำรวจในต่างประเทศ	ไม่มีความเกี่ยวข้อง

ชื่อระบบ	คำอธิบาย	พิจารณาข้อมูลและความเกี่ยวข้องกับโครงการ
	โดยจะเชื่อมโยงกับระบบเครือข่ายสืบสวนสอบสวน	
กลุ่มที่ 4 ระบบสารสนเทศเพื่อการบริการสังคม (Social Service Information System : sSIS)	ประกอบด้วยระบบงานย่อย ๒ ฐานข้อมูล ได้แก่	
1) ระบบฐานข้อมูลจราจร	เป็นระบบการบันทึก/แก้ไข/สอบถามข้อมูล เพื่อควบคุมการรับ-เบิกจ่ายใบสั่งให้กับหน่วยปฏิบัติ รวมทั้งการยกเลิกใบสั่งที่เบิกไปแล้ว โดยสามารถตรวจสอบยอดใบสั่งคงเหลือในคลังได้	ไม่มีความเกี่ยวข้อง
2) ระบบฐานข้อมูลนิติเวช	เป็นระบบการบันทึก/แก้ไข ข้อมูลตามแบบรายงานการตรวจพิสูจน์ศพของสถาบันนิติเวชวิทยา และสามารถสอบถามข้อมูลคนตายไม่ทราบชื่อเมื่อมีญาติของผู้ตายมาติดต่อขอดูศพ และสามารถพิมพ์รายงานการตรวจศพ เพื่อส่งให้พนักงานสอบสวนเจ้าของคดีหรือบริษัทประกันชีวิตได้	ไม่มีความเกี่ยวข้อง
กลุ่มที่ 5 ระบบข้อมูลอื่นเพื่อสนับสนุนงานด้านป้องกันปราบปรามอาชญากรรม Service Crimes Information System : SCIS)	ประกอบด้วยระบบงานย่อย 2 ฐานข้อมูลได้แก่	
1) ระบบข้อมูลโครงข่ายการสืบสวนสอบสวนดดี	เป็นระบบสอบถามข้อมูลจากระบบงานต่าง ๆ ที่พัฒนาขึ้น เช่น ระบบฐานข้อมูลผู้กระทำผิดกฎหมาย ระบบสถิติคดีอาชญากรรมระบบภาพถ่าย เพื่อให้เกิดความเชื่อมโยงและต่อเนื่องกัน เป็นระบบที่ช่วยให้เจ้าหน้าที่สืบสวนปฏิบัติงานได้คล่องตัวขึ้น เช่น สอบถามข้อมูลคดีอุกฉกรรจ์ คดี	มีความเกี่ยวข้องกับระบบที่พัฒนาขึ้น ซึ่งจะกล่าวในบทต่อไป

ชื่อระบบ	คำอธิบาย	พิจารณาข้อมูลและความเกี่ยวข้องกับโครงการ
	สะเทือนขวัญ คดีฉ้อฉล และคดีฆาตกรรมได้ นอกจากนี้ยังสามารถใช้ในการวิเคราะห์เหตุการณ์และความสัมพันธ์อย่างต่อเนื่องกับบุคคล องค์การและแสดงผลลัพธ์ต่าง ๆ ทางจอภาพในแบบของข้อความและรูปภาพ ๆ ได้	
2) ระบบฐานข้อมูลภาพถ่าย	เป็นระบบการบันทึก/แก้ไข/สอบถามข้อมูลบุคคลและเหตุการณ์ที่เกี่ยวข้องกับอาชญากรรม เป็นระบบฐานข้อมูลเพื่อสนับสนุนระบบฐานข้อมูลอื่นในลักษณะการเชื่อมโยงข้อมูลกัน ช่น ระบบ บุคคลผู้กระทำผิดกฎหมาย ระบบทรัพย์หาย ระบบบุคคลพลัดหลง ระบบประกาศสืบจับ บุคคลพันโทษ ฯลฯ เป็นต้น โดยการนำเข้าข้อมูลในรูปแบบภาพถ่ายต้องใช้อุปกรณ์สแกนเนอร์และกล้องถ่ายรูปซึ่งกองทะเบียนประวัติจะเป็นผู้รับผิดชอบในการดำเนินการ	ไม่มีความเกี่ยวข้อง
กลุ่มที่ 6 ระบบสารสนเทศสถานีตำรวจ (Police Station Information System : PSIS)	ประกอบด้วยระบบงานย่อย 4 ฐานข้อมูล ได้แก่	
1) ระบบงานบริหารภายในสถานีตำรวจ (หน่วยงานย่อย)	เป็นระบบรวบรวมข้อมูลการบริหารงานในสถานีตำรวจ เช่น ประวัติบุคลากรในสถานีตำรวจ ข้อมูลการเงิน ข้อมูล	ไม่มีความเกี่ยวข้อง
2) ระบบฐานข้อมูลติดตามผลดีดำ	เป็นระบบที่เก็บรวบรวมข้อมูลรายละเอียดเกี่ยวกับคดีอาญา คดีอุกฉกรรจ์และสะเทือนขวัญ ตั้งแต่รับคดีจนถึงผลการดำเนินคดีจากชั้นศาลเชื่อมโยงข้อมูลจากระบบสถิติคดีอาชญากรรม เช่น ค้นหาข้อมูลเลขคดี หน่วยงาน เพื่อนำมาบันทึก	มีความเกี่ยวข้องกับระบบที่พัฒนาขึ้น ซึ่งจะกล่าวในบทต่อไป

ชื่อระบบ	คำอธิบาย	พิจารณาข้อมูลและความเกี่ยวข้องกับโครงการ
	ผลของคดีนั้น ๆ ไว้ใช้ในการติดตามความคืบหน้าของผลคดีที่ยังไม่สิ้นสุด นอกจากนี้ยังเชื่อมโยงข้อมูลกับระบบฐานข้อมูลอุบัติเหตุจราจร หมายจับ ทรัพย์หาย คนหายพลัดหลง (กรณีถูกลักพาตัว เรียกค่าไถ่) นิติเวช เครือข่ายสืบสวนประวัติผู้กระทำผิด	
3) ระบบงานข้อมูลจราจร	เป็นระบบการบันทึก/แก้ไข/สอบถามข้อมูลการออกใบสั่ง (สีเหลือง) การบันทึกคะแนน และการชำระค่าปรับ	ไม่มีความเกี่ยวข้อง
4) ระบบฐานข้อมูลป้องกันปราบปรามอาชญากรรม	จัดเก็บข้อมูลบุคคลและสถานที่ตามประเภทกลุ่มข้อมูลต่าง ๆ เพื่อใช้ในการสืบสวนและการป้องกันปราบปรามชื่อโครงการพัฒนาศูนย์ข้อมูลข่อสนเทศ (Police Information System : POLIS) มีการใช้งานในหลากหลายชื่อ เช่น ระบบ POLIS, ระบบสารสนเทศหลัก ตร. (โครงการ POLIS), ระบบสารสนเทศ ตร. (POLIS) ซึ่งในปัจจุบันสำนักงานตำรวจแห่งชาติก็ยังไม่ได้มีชื่อที่ระบุชัดเจน เป็นลายลักษณ์อักษรเพียงแต่ใช้กันทั่วไปในหนังสือราชการว่า "ระบบสารสนเทศ ตร. (POLIS)" และใช้อย่างไม่เป็นทางการว่า "ระบบ POLIS"	มีความเกี่ยวข้องกับระบบที่พัฒนาขึ้น ซึ่งจะกล่าวในบทต่อไป
1.1.2 ระบบสารสนเทศสถานีตำรวจ (Criminal Record and Information Management Enterprise System : CRIMES)	CRIMES คือ ระบบสารสนเทศที่รวบรวมข้อมูลการรับแจ้ง ข้อมูลเกี่ยวกับคดีเพื่อเป็นเครื่องมือช่วยในการสืบสวน สอบสวน ป้องกันปราบปรามอาชญากรรม อันเป็นระบบที่อำนวยความสะดวกให้กับ	ข้อมูลที่เกี่ยวกับผู้ถูกกล่าวหา ผู้ถูกออกหมายเรียก และผู้ถูกออกหมายจับ จะเป็นประโยชน์ในการสอบสวน และสืบสวน ทั้งในส่วนของการรับพิจารณษเพื่อดำเนินคดี

ชื่อระบบ	คำอธิบาย	พิจารณาข้อมูลและความเกี่ยวข้องกับโครงการ
	เจ้าหน้าที่ผู้ปฏิบัติงาน โดยเป็นจุดศูนย์กลางสู่การเชื่อมต่อไปยังฐานข้อมูลของหน่วยงานต่างๆ ทั้งในสำนักงานตำรวจแห่งชาติและหน่วยงาภายนอก นอกจากนั้นยังเป็นระบบที่รองรับการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานในกระบวนการยุติธรรม ซึ่งถือว่าระบบนี้ช่วยให้ประชาชนที่มาติดต่อสถานีตำรวจ ได้รับการอำนวยความสะดวกและความยุติธรมได้อย่างโปร่งใสและรวดเร็ว	ทดแทนการลงบันทึกประจำวัน และสามารถนำข้อมูลมาใช้ในระบบตรวจสอบข้อมูลผู้กระทำความผิด เพื่อป้องกันไม่ให้เกิดการกระทำผิดกับผู้เสียหายรายอื่นต่อไป
1.1.3 ระบบประชุมวิดีทัศน์ทางไกล สำนักงานตำรวจแห่งชาติ (Video Conference System)	ระบบประชุมวดีทัศน์ทางไกล สำนักงานตำรวจแห่งชาติ (Video Conference System) คือ การนำเทคโนโลยีต่าง ๆ มาใช้สำหรับการประชุมที่ผู้เข้าร่วมประชุมอยู่คนละสถานที่	ไม่มีความเกี่ยวข้อง
1.1.4 ศูนย์รับแจ้งเหตุฉุกเฉิน 191	โดยไม่จำกัดระยะทาง สามารถประชุมร่วมกันและมีปฏิสัมพันธ์โต้ตอบกันได้ สามารถส่งทั้งภาพและเสียงไปยังสถานที่ต่าง ๆ ได้ ปัจจุบันหน่วยงานต่าง 1 ของสำนักงานตำรวจแห่งชาติได้มีการติดตั้งใช้งานระบบ ระบบประชุมวีดิทัศน์ทางไกล แบบฮาร์ดแวร์หลายหน่วยงาน	ไม่มีความเกี่ยวข้อง
1.1.5 ระบบบริหารจัดการใบสั่งออนไลน์ (Police Ticket Management : PTM)	ศูนย์รับแจ้งเหตุฉุกเฉิน 191 หรือ "ระบบ 191"หรือ "Call Center 190" เกิดขึ้นในกรมตำรวจประมาณปี 2520 ในขณะนั้นใช้ผู้รับโทรศัพท์เพียง 20 คู่สาย งาน 191 อยู่ในกองกำกับการศูนย์รวมข่าวของกองบัญชาการตำรวจนครบาล ต่อมาในปี 2523 กองตำรวจสื่อสาร	ไม่มีความเกี่ยวข้อง

ชื่อระบบ	คำอธิบาย	พิจารณาข้อมูลและความเกี่ยวข้องกับโครงการ
	ได้เขียนโครงการของบจากประเทศญี่ปุ่น ในปี 2532 ประเทศญี่ปุ่นได้ให้งบมาพัฒนาศูนย์ 191 ประมาณ 250 ล้านบาท ต่อมาในปี 2535 กรมตำรวจ ได้นำเทคโนโลยี C๓I มาใช้ในระบบของศูนย์ 191 กองบัญชาการตำรวจนครบาลใช้งบประมาณ 250 ล้านบาท ดำเนินการพัฒนาระบบของศูนย์ 191 ในปี 2539-2544 คณะรัฐมนตรี ในคราวประชุมเมื่อ 1 เม.ย. 2546 ได้มีมติเห็นชอบให้ส่วนราชการและหน่วยงานของรัฐที่มีหน้าที่บริการประชาชนไปพิจารณาความเหมาะสมและเป็นไปได้ในการจัดตั้งศูนย์บริการประชาชนขึ้นในหน่วยงาน ในส่วนของสำนักงานตำรวจแห่งชาติจึงได้กำหนดแนวทางการพัฒนาศูนย์บริการประชาชน (Call Center) โดยการปรับปรุงระบบสารสนเทศและการสื่อสาร โทรศัพท์สายด่วน 191 เรียกว่า "ศูนย์รับแจ้งเหตุฉุกเฉิน 191" ของตำรวจภูธรจังหวัดในแต่ละจังหวัดเพียงแห่งเดียว	
1.2 ระบบสารสนเทศอื่นที่ใช้ในหน่วยงานภายในสำนักงานตำรวจแห่งชาติ		
1.2.1 ระบบสารสนเทศสำนักงานตรวจคนเข้าเมือง (Personal Identification and Blacklist Immigration Control System : PIBICS)	เป็นระบบสารสนเทศที่ทางสำนักงานตรวจคนเข้าเมืองพัฒนาขึ้นโดยมีบริษัท คอนโทรล ดาตา (ประเทศไทย) จำกัด เป็นบริษัทคู่สัญญา เพื่อรวบรวมข้อมูลประวัติการเดินทางเข้า-ออกราชอาณาจักรไทย สามารถเชื่อมโยงข้อมูลต่างๆ	ไม่มีความเกี่ยวข้อง

ชื่อระบบ	คำอธิบาย	พิจารณาข้อมูลและความเกี่ยวข้องกับโครงการ
	ได้ เช่น ข้อมูลการขออยู่ต่อการตรวจสอบบัญชีเฝ้าดู การตรวจสอบเปรียบเทียบกับภาพบุคคลกับผู้ที่มีแบล็กลิสต์ และใบหน้าคนที่เคยเข้ามาในราชอาณาจักร หรือรูปที่อยู่ในพาสสปอร์ต รวมทั้งประวัติที่เคยเข้ามาในอดีตเพื่อป้องกันการสวมรอย ป้องกันการปลอมพาสปอร์ตซึ่งด่านต่าง ๆ ของสำนักงานตรวจคนเข้าเมืองมีอยู่ทั่วราชอาณาจักร สามารถเชื่อมโยงข้อมูลถึงกันได้ ระบบโครงข่ายส่วนตัวเสมือน (Virtual Private Network : VPN) ทำให้ข้อมูลมีความทันสมัยและทันต่อเหตุการณ์ การดำเนินการนี้อยู่ภายในกำกับดูแลของศูนย์เทคโนโลยีสารสนเทศ สำนักงานตรวจคนเข้าเมือง (ศทส.ตม.) ทำหน้าที่เป็น "แอดมิน" หรือผู้ดูแลระบบ มีหน้าที่คอยควบคุมและออกแบบระบบให้มีประสิทธิภาพ ระบบ PIBICSจะช่วยในการบูรณาการข้อมูล ถือว่าเป็นกระดูกสันหลังเป็นคลังข้อมูลของสำนักงานตรวจคนเข้าเมืองทั้งนี้ ข้อมูลเปรียบเสมือนอาวุธการจะรบกันในยุคของฐานข้อมูล (Knowledge Base) จำเป็นต้องมีข้อมูลในปริมาณที่มากและทันสมัยถึงจะรบชนะ ซึ่งการบริหารงานแบบใช้ข้อมูลเป็นการเสริมการทำงานให้กับทีมสอบสวนของ สตม.ด้วย	
1.2.2 ระบบตรวจสอบลายพิมพ์นิ้วมืออัตโนมัติ(Automated Fingerprint Identification :	เป็นการนำเทคโนโลยีคอมพิวเตอร์มาใช้งานร่วมกับหลักวิชาพิมพ์นิ้วมือโดยในขั้นตอนการทำงานนั้น	ไม่มีความเกี่ยวข้อง

ชื่อระบบ	คำอธิบาย	พิจารณาข้อมูลและความเกี่ยวข้องกับโครงการ
AFIS)	ลายพิมพ์นิ้วของอาชญากรทั่วประเทศจะถูกส่งมาตรวจสอบและเก็บในฐานข้อมูลระบบ AFIS ของกองทะเบียนประวัติอาชญากร Software ของระบบ AFIS จะอ่านและแยกประเภทของลายพิมพ์นิ้วมือแต่ละนิ้วว่าเป็นลายประเภทใด เช่น ประเภทโค้ง ประเภทมัดหวาย ประเภทก้นหอย เป็นต้น และแสดงจุดใจกลางของลายเส้นในลายนิ้วมือและจุดสำคัญลักษณะพิเศษของลายเส้นแล้วคำนวณค่าสัมพันธ์ของจุดต่าง ๆ ดังกล่าวเป็นค่าทางคณิตศาสตร์โดยอัตโนมัติจากนั้นระบบจะนำค่าที่ได้ไปค้นหาเปรียบเทียบข้อมูลในระบบ AFIS หากพบข้อมูลที่ตรงกันก็แสดงว่าผู้นั้นเคยมีประวัติการกระทำความผิดมาก่อน ระบบ AFIS จะเชื่อมโยงไปยังระบบฐานข้อมูลประวัติอาชญากร เพื่อที่จะแสดงรายละเอียดและยืนยันประวัติของผู้ต้องหา ตำหนิรูปพรรณ แผนประทุษกรรมและภาพถ่าย ใช้เป็นข้อมูลและหลักฐานในการดำเนินคดีกับผู้ต้องหาได้อย่างแม่นยำ	
1.2.3 ระบบฐานข้อมูลอาชญากรรม (Criminal Database System : CDS)	เป็นระบบที่รวบรวมข้อมูลเกี่ยวกับประวัติอาชญากรมาจัดเก็บเช่นเดียวกับระบบสารสนเทศอาชญากรรม (ระบบ CIS) ซึ่งปัจจุบันกองทะเบียนประวัติอาชญากรเป็นผู้ดูแล ผู้บันทึกและใช้งานข้อมูล แต่ระบบ CDS หน่วยงานศูนย์พิสูจน์หลักฐานต่าง " ทั่วประเทศเป็นผู้บันทึกข้อมูลและใช้	มีความเกี่ยวข้องกับระบบที่พัฒนาขึ้น ซึ่งจะกล่าวในบทต่อไป

ชื่อระบบ	คำอธิบาย	พิจารณาข้อมูลและความเกี่ยวข้องกับโครงการ
	งานข้อมูล ความสามารถของระบบ CDS สามารถสืบค้นจากชื่อ-นามสกุล ตำหนิรูปพรรณวิธีการกระทำความผิด ลักษณะเช่นนี้ในพื้นที่ใกล้เคียงกันมีกี่คดี และในแต่ละคดีมีบุคคลใดเป็นผู้ต้องสงสัย จึงทำให้งานสืบสวนสามารถทราบข้อมูลของอาชญากรรมที่ต้องการได้อย่างรวดเร็ว	
1.2.4 การใช้คอมพิวเตอร์สเก็ตช์และประกอบภาพใบหน้าคนร้าย	เป็นเทคนิคการบอกเล่าเหตุการณ์ที่ผู้พบเห็นภาพใบหน้า ลักษณะตำหนิรูปพรรณการสวมเสื้อผ้า ของผู้ต้องสงสัยออกมาเป็นรูปภาพวาดเพื่อนำไปสู่การออกหมายจับ หรือกระบวนสืบสวนหาผู้กระทำความผิดผ่านเทคโนโลยีที่ทันสมัยในยุคปัจจุบันโดยไม่มีการใช้โปรแกรมประยุกต์ที่ตายตัว เป็นเลือกใช้เทคโนโลยีที่เหมาะสม ผสมผสานกับความเชี่ยวชาญของเจ้าหน้าที่กองทะเบียนประวัติอาชญากร ที่ฝึกฝนจนเกิดความชำนาญเชี่ยวชาญ ในวิชาการสเก็ตช์ภาพผู้ต้องสงสัยส่วนลำดับขั้นตอนการวาดภาพสเก็ตช์คนร้ายนั้น ผู้เสียหายต้องมาคัดเลือกชิ้นส่วนต่างๆ ของใบหน้าเช่น โครงหน้า คิ้ว คาง ปาก จมูก ฯลฯ จากสมุดแฟ้มภาพสเก็ตช์อาชญาก โดยจดหมายเลขรหัสใต้รูปนำไปให้เจ้าหน้าที่ประกอบรูปคนร้าย ทำให้หลาย ๆ คดีคลี่คลายจนดำเนินการจับตัวผู้กระทำความผิดมาดำเนินคดีได้	ไม่มีความเกี่ยวข้อง
1.2.5 ระบบฐานข้อมูล	สำนักงานตำรวจแห่งชาติเป็นหน่วย	ไม่มีความเกี่ยวข้อง

ชื่อระบบ	คำอธิบาย	พิจารณาข้อมูลและความเกี่ยวข้องกับโครงการ
อาชญากรรมข้ามชาติ (Case Management Intelligence System : CMIS)	รับผิดชอบและเป็นหน่วยงานเจ้าภาพในกรอบความร่วมมือว่าด้วยอาชญากรรมข้ามชาติของอาเซียนได้มีการจัดทำความตกลงแลกเปลี่ยนข่าวกรองมีความร่วมมือระหว่างกัน และมีความร่วมมือในด้านอื่น ๆ เช่น อนุสัญญาอาเซียนว่าด้วยการต่อต้านการก่อการร้าย นอกจากนี้ยังมีกรอบความร่วมมือภายใต้สนธิสัญญาอาเซียนว่าด้วยการให้ความช่วยเหลือซึ่งกันและกันทางอาญา (Mutual Legal Assistance Treaty : MLAT) อีกกรอบหนึ่ง ที่จะใช้ในอนาคตและได้จัดตั้งศูนย์ประสานงานปราบปรามอาชญากรรมข้ามชาติ (Transnational Crime Coordination Center (TCCC)) (ศอปช.) แบ่งเป็นระดับสำนักงานตำรวจแห่งชาติ (ศอปช.ตร.) กองบัญชาการ (อปช.ภ.) กองบังคับการ (ศอปช.ภ.จว.) ขึ้นมา เพื่อดำเนินการประสานการปฏิบัติ การสืบสวน ปราบปราม จับกุม และดำเนินคดีกับอาชญากร กลุ่มองค์กรอาชญากรรมข้ามชาติที่มีลักษณะเป็นกระบวนการและเป็นเครือข่ายทั้งในประเทศและต่างประเทศผ่านระบบฐานข้อมูลอาชญากรรมข้ามชาติ (Case Management Intelligence System : CMIS) เป็นระบบที่รวบรวมข้อมูลข่าวสารเกี่ยวกับตัวบุคคลและกลุ่มบุคคลหรือองค์กรที่มีลักษณะเป็นเครือข่ายมีพฤติการณ์กระทำผิด	

ชื่อระบบ	คำอธิบาย	พิจารณาข้อมูลและความเกี่ยวข้องกับโครงการ
	เกี่ยวกับอาชญากรรมข้ามชาติเพื่อนำไปสู่การจับกุมและตรวจยึดหรืออายัดทรัพย์ของผู้กระทำผิด รวมทั้งประชาสัมพันธ์รูปแบบแผนประทุษกรรมของกลุ่มอาชญากรโดยกองการต่างประเทศ (ตท.) เป็นผู้ดูแลระบบ หน่วยงานระดับกองบัญชาการ (กองบังคับการกองกำกับการสืบสวน) และกองบังคับการ (กองกำกับการสืบสวน) เป็นผู้บันทึกข้อมูลอาชญากรรมข้ามชาติและความผิดอาญาที่เข้าข่ายอาชญากรรมข้ามชาติลงในระบบและใช้ข้อมูลร่วมกัน	
1.2.6 ระบบกล้องอ่านหมายเลขป้ายทะเบียนรถอัตโนมัติ (License Plate)	สืบเนื่องจากจุดตรวจ/ด่านตรวจต่าง ๆ มีเจ้าหน้าที่ทำการตรวจบริการการเดินทางของประชาชนเป็นบางเวลา ไม่ต่อเนื่อง ทำให้เป็นช่องว่างในการที่กลุ่มคนร้ายลำเลียงยาเสพติดและก่ออาชญากรรมต่าง ๆ ได้ สำนักงานตำรวจแห่งชาติจึงได้หาวิธีการนำเทคโนโลยีเพื่อรักษาความปลอดภัย สืบสวน ป้องกันและปราบปรามอาชญากรรมต่างๆ ในปี พ.ศ.2555 ผู้บัญชาการตำรวจแห่งชาติสมัยนั้น จึงได้จัดตั้งศูนย์สกัดกั้นการลำเลียงยาเสพติดขึ้น เพื่อสกัดกั้นการลำเลียงยาเสพติด ที่มีแหล่งผลิตภายนอกประเทศ มิให้เข้าสู่พื้นที่ตอนในของประเทศ รวมทั้ง ป้องกันและปราบปรามอาชญากรรมต่าง ๆ โดยใช้ระบบกล้องวงจรปิดที่สามารถนำภาพที่เห็นมาแปลงเป็นข้อมูลหรือเรียกว่าอ่านป้ายแผ่นทะเบียน แล้วทำการ	ไม่มีความเกี่ยวข้อง

ชื่อระบบ	คำอธิบาย	พิจารณาข้อมูลและความเกี่ยวข้องกับโครงการ
	บันทึกข้อมูลจำนวนรถที่ผ่านเส้นทางจุดนั้นๆ ทำให้เจ้าหน้าที่ตำรวจสามารถนำข้อมูลนั้น ๆ มาใช้ในการคัดแยกรถ ตรวจสอบรถ แจ้งเตือนภัยรถกรณีรถต้องสงสัยซึ่งจุดติดตั้งระบบกล้องอ่านแผ่นป้ายทะเบียน มีอยู่ทั่วทุกภาคทั่วประเทศทั้งหมด 376 จุดประสิทธิภาพของระบบกล้องอ่านป้ายทะเบียนสามารถใช้ได้กับยานพาหนะรถยนต์รถบรรทุก ทำงานได้ทั้งเวลากลางวันและกลางคืน จากนั้นข้อมูลที่ถูกแปลงแล้วจากด่านตรวจจำนวนมากทั้งประเทศ จะถูกส่งขึ้นมาที่ศูนย์ควบคุมส่วนกลาง ที่กองบังคับการสกัดกั้นการลำเลียงยาเสพติด กองบัญชาการตำรวจปราบปรามยาเสพติด ในทันที ในส่วนศูนย์ควบคุมสั่งการฯ ได้ดำเนินการจัดทำเว็บบริการ สำหรับข้าราชการตำรวจที่เกี่ยวข้อง ให้สามารถข้าถึงข้อมูลโดยมีรหัสลับในการเข้าถึงข้อมูลเพื่อที่จะสามารถใช้บริการในการตรวจสอบสืบค้นหาและดูข้อมูลสถานที่ตั้งของกล้อง หมายเลขทะเบียนรถ ประเภทรถภาพถ่ายรถ วันและเวลาที่ถูกต้อง อีกทั้งสามารถเรียกดูภาพและประวัติการใช้เส้นทางย้อนหลังของยานพาหนะและเชื่อมโยงเส้นทางของยานพาหนะ ทั้งก่อนหน้า และหลังใช้เส้นทาง ได้อย่างรวดเร็วโดยอัตโนมัติและมีประสิทธิภาพสูง เจ้าหน้าที่จึงต้องศึกษาเพื่อให้เข้าถึงหลักการทำงานและนำข้อมูลมา	

ชื่อระบบ	คำอธิบาย	พิจารณาข้อมูลและความเกี่ยวข้องกับโครงการ
	วิเคราะห์ สืบสวนประกอบกับเทคโนโลยีอื่น ๆ	
1.2.7 Application CRIME ON MOBILE	เป็นโปรแกรมที่พัฒนาขึ้นโดยข้าราชการตำรวจในสังกัด ศูนย์เทคโนโลยีสารสนเทศกลาง สำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อบูรณาการข้อมูลในระบบ CRIMESให้เกิดประโยชน์สูงสุดแก่สำนักงานตำรวจแห่งชาติ รองรับระบบปฏิบัติการ (Operating System : OS) ของโทรศัพท์เคลื่อนที่ (Smart Phone) ทั้ง iOS และ Android โดยดาวน์โหลดโปรแกรมจาก Play Store สำหรับ iOS และ App Store สำหรับ Android เพื่อติดตั้งบนโทรศัพท์ที่ต้องการ ในปี ๒๕๖๐ ระบบสามารถดำเนินการได้แล้วดังนี้ 1. ทะเบียนราษฎร์ (ต้องทำการเสียบบัตรยืนยัน PIN CODE ที่เครื่อง CRIMES ก่อน 1 ครั้งและสามารถดำเนินงานอย่างต่อเนื่องถึงเที่ยงคืนยกเว้นการออกจากระบบ (Log out)) 2. ทะเบียนรถ 3. ใบขับขี่ 4. หมายจับ 5. ผู้ต้องหาในคดีอาญา 6. บุคคลพ้นโทษ 7. บริษัทจดทะเบียน 8. แรงงานต่างด้าว (อยู่ระหว่างพัฒนา) 9. สิทธิ์ประกันสุขภาพถ้วนหน้า (อยู่ระหว่างพัฒนา)	ข้อมูลนี้ สามารถเชื่อมโยงแลกเปลี่ยนกับระบบที่พัฒนาขึ้นได้ และ/หรือแนะนำให้พนง. สอบสวน และพนง. สืบสวน ใช้ร่วมระบบที่พัฒนาขึ้น ประกอบการพิจารณาดำเนินคดีได้ ข้อมูลที่เกี่ยวข้องกับผู้ถูกกล่าวหา ที่ระบบสามารถค้นหาได้นั้น จะเป็นประโยชน์ในการสอบสวน และสืบสวน ทั้งในส่วนของการรับพิจารณษเพื่อดำเนินคดี และสามารถนำข้อมูลมาใช้ในระบบตรวจสอบข้อมูลผู้กระทำความผิด เพื่อป้องกันไม่ให้เกิดการกระทำผิดกับผู้เสียหายรายอื่นต่อไป

ชื่อระบบ	คำอธิบาย	พิจารณาข้อมูลและความเกี่ยวข้องกับโครงการ
	10. ประกันสังคม 11. นักโทษที่ถูกคุมขัง(อยู่ระหว่างพัฒนา)	
1.4 การรับแจ้งความทางออนไลน์คดีอาชญากรรมทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ	ทางสำนักงานตำรวจแห่งชาติ จึงได้มีการจัดตั้งศูนย์รับแจ้งความออนไลน์ ในคดีทางเทคโนโลยีโดยเฉพาะ โดยให้บริการตั้งแต่วันที่ 1 มี.ค. 65 หลังจากที่สำนักงานตำรวจแห่งชาติได้ทำบันทึกตกลงความร่วมมือ (MOU) กับสมาคมสถาบันทางการเงินของรัฐ สมาคมธนาคารไทยและสมาชิก รวม 21 ธนาคาร ในคดีที่เกี่ยวกับอาชญากรรมทางเทคโนโลยี เมื่อวันที่ 28 ก.พ. 65 ขั้นตอนการแจ้งความออนไลน์ 1. เข้าไปที่เว็บไซต์ www.thaipoliceonline.com 2. ลงทะเบียนผู้ใช้งาน และยืนยันตัวตน 3. หลังจากลงทะเบียนแล้ว กดยอมรับเงื่อนไขการใช้งาน 4. กรอกรายละเอียดข้อมูลทางคดี 5. ผู้แจ้งจะได้รับเลขรับแจ้งความออนไลน์ 6. จากนั้นรอนัดหมายจากเจ้าหน้าที่ส่วนกลาง สำหรับนัดพบพนักงานสอบสวน เพื่อสอบปากคำเพิ่มเติม	

4.3.2 ระบบสารสนเทศจากหน่วยงานภายนอก

4.3.2.1 ระบบตรวจสอบข้อมูลผู้ลงทะเบียน

ระบบตรวจสอบข้อมูลผู้ลงทะเบียน เป็นระบบของสำนักงาน กสทช. ที่ร่วมกับผู้ให้บริการเครือข่ายโทรศัพท์มือถือ เพื่อใช้ตรวจสอบประวัติผู้เป็นเจ้าของเลขหมายโทรศัพท์เคลื่อนที่

4.3.2.2 ระบบแจ้งอายัดบัญชีธนาคาร

ระบบแจ้งอายัดบัญชีธนาคาร เกิดจากความร่วมมือระหว่างสมาคมธนาคารไทย สถาบันเพื่อการยุติธรรมแห่งประเทศไทย และกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี เป็นระบบที่ให้อำนาจตามกฎหมายกับพนักงานสอบสวน ในการอายัดเงินในบัญชีของคนร้ายด้วยการส่งหนังสือโดยใช้วิธีการทางอิเล็กทรอนิกส์ และมีการเข้ารหัสข้อมูลด้วย Public Key และ Private Key เพื่อเพิ่มความปลอดภัยของข้อมูล

4.3.2.3 ตรวจสอบข้อมูลบัตรประชาชนผ่านระบบเว็บเซอร์วิส

การให้บริการตรวจสอบข้อมูลทะเบียนประวัติบุคคลสัญชาติไทย และบุคคลซึ่งไม่มีสัญชาติไทยจากฐานข้อมูลทะเบียนกลาง โดยการกำกับของกรมการปกครอง กระทรวงมหาดไทย

4.3.2.4 ระบบศูนย์กลางการตรวจสอบคนโกงออนไลน์ เว็บไซต์ Blacklistseller.com

เว็บไซต์ blacklistseller เป็นเว็บไซต์ศูนย์กลางการตรวจสอบคนโกงออนไลน์ มีไว้สำหรับตรวจสอบชื่อและเลขบัญชีก่อนโอนเงิน เพื่อป้องกันการโดนโกง โดยมีผู้เสียหายที่ถูกมิจฉาชีพฉ้อโกงไป เป็นผู้ให้ข้อมูลเพื่อเตือนภัย โดยทางเว็บไซต์ได้เริ่มเปิดให้ประชาชนเข้ามาร้องเรียนตั้งแต่ 2558 และยังดำเนินการเปิดใช้งานจนถึงปีปัจจุบัน

4.3.2.5 ระบบยื่นคำฟ้องอิเล็กทรอนิกส์สำหรับประชาชน (e-Filing)

ในปัจจุบันการซื้อขายออนไลน์เป็นที่นิยมกันอย่างมากเนื่องจากสะดวกและรวดเร็ว ประกอบกับช่วงของการแพร่ระบาดของไวรัสโควิด-19 ทำให้ผู้บริโภคปรับเปลี่ยนพฤติกรรมจากการซื้อสินค้าผ่านห้างสรรพสินค้าหรือร้านค้าต่าง ๆ เป็นการสั่งซื้อสินค้าทางออนไลน์แทน ซึ่งเป็นเหตุทำให้เกิดข้อพิพาทตามมาเป็นจำนวนมาก เช่น สั่งซื้อสินค้าแล้วไม่ได้รับสินค้า ได้รับของไม่ตรงปก หรือถูกหลอกลวง เป็นต้น โดยปกติแล้วผู้เสียหายสามารถนำคดีมายื่นฟ้องศาล เพื่อให้มีการชดใช้ได้ แต่ในการยื่นฟ้องคดีแพ่งตามหลัก จะต้องยื่นฟ้องต่อศาลในภูมิลำเนาของผู้ขายที่จะเป็นจำเลย หรือที่มูลคดีเกิด ขณะที่การซื้อขายออนไลน์ นอกจากนี้อาจมีกรณีที่ว่าความเสียหายเป็นเงินจำนวนไม่มาก หลักร้อยหลักพันบาท จึงทำให้คดีเหล่านี้มาไม่ถึงศาล เพราะมองว่าจะต้องเสียเวลา ค่าใช้จ่ายในการดำเนินคดี อาจไม่คุ้มค่าที่จะไปยื่นฟ้องศาล รวมถึงความยุ่งยากในขั้นตอนการดำเนินคดี แต่เมื่อปัจจุบันข้อพิพาทในการซื้อสินค้าออนไลน์ในสังคมมีมากขึ้นเรื่อย ๆ หากปล่อยปัญหานี้ไปก็จะกระทบถึงความน่าเชื่อถือของระบบการซื้อขายออนไลน์ในประเทศ และผู้บริโภคที่ซื้อของทางออนไลน์มีโอกาสที่จะถูกหลอกโดยที่ไม่ได้รับการเยียวยา ขณะที่ผู้ขายซึ่งก่อให้เกิดปัญหาจะยังคงไปสร้างความเดือดร้อนให้แก่ผู้บริโภครายอื่นได้อีก ศาลยุติธรรมจึงได้ดำเนินการการจัดตั้งแผนกคดีซื้อขายออนไลน์ในศาลแพ่ง และได้มีการเปิดตัวเมื่อวันที่ 27 มกราคม 2565 ซึ่งจะมุ่งส่งเสริมการดำเนินคดีเพื่อยกระดับการคุ้มครองผู้บริโภคให้ครอบคลุมถึงการบริโภควิถีใหม่ เช่น กลุ่มการซื้อขายสินค้าออนไลน์ โดยให้ใช้ระบบศาลอิเล็กทรอนิกส์เต็มรูปแบบในทุกขั้นตอนของกระบวนการพิจารณา เพื่อให้ผู้บริโภคที่คิดว่าจะใช้สิทธิทางศาลฟ้องคดี ได้รับความสะดวก เพื่อยกระดับการให้บริการแก่ประชาชนได้ครอบคลุมและรวดเร็วขึ้น สามารถเข้ายื่นคำฟ้องอิเล็กทรอนิกส์ได้ที่ https://efiling3.coj.go.th/eFiling

4.4 ข้อเสนอแนะในการปรับปรุง หลักเกณฑ์และระเบียบปฏิบัติ

จากผลการวิเคราะห์ข้อมูลเกี่ยวกับหลักฐานที่จะใช้ประกอบคดีฉ้อโกงออนไลน์ ซึ่งวิธีพิจารณาของพนักงานสอบสวนในการที่จะรับเป็นคดีประเภทแจ้งความเพื่อดำเนินคดีนั้น ส่วนใหญ่จะพิจารณาจากคดีที่เป็นคดีที่มีการฉ้อโกงประชาชนเป็นหลัก หรือเรียกคดีฉ้อโกงประชาชน ซึ่งเป็นความผิดความประมวลกฎหมายอาญา มาตรา 343 และเป็นคดีที่ยอมความกันไม่ได้ และมีผู้เสียหายมากกว่า 1 รายโดยไม่ได้พิจารณาจากมูลค่าความเสียหาย หรือมูลค่ารวมของความเสียหายจากผู้เสียหายทุกคนรวมกัน

ปัญหาโดยส่วนใหญ่ของการพิจารณารับเป็นการแจ้งความดำเนินคดีในขั้นตอนดังที่กล่าวมานั้น คือไม่สามารถพิจารณาความเป็นไปได้ในการดำเนินการจนถึงขั้นตอนการออกหมายเรียก หรือการออกหมายจับได้โดยง่าย เนื่องจากหลักฐานที่ทางผู้เสียหายนำมาใช้ประกอบนั้นส่วนใหญ่เป็นการติดต่อผ่านทางช่องทางที่ไม่สามารถพิสูจน์ว่าเป็นบุคคลใดที่ติดต่อด้วย หรือขั้นตอนการพิสูจน์ยืนยันตัวตนผู้กระทำความผิด ซึ่งผู้เสียหายมักจะเข้าใจว่าหลักฐานหลักที่สำคัญคือการได้ทราบชื่อเจ้าของบัญชีธนาคาร ซึ่งมักจะปรากฏภายหลังว่าเป็นบัญชีที่ได้มาจากการรับจ้างเปิดบัญชีโดยที่ผู้รับจ้างไม่ทราบหรือยอมเสี่ยงหากมีการออกหมายเรียกหรือหมายจับในอนาคต และคิดว่าตนเองจะหลุดพ้นจากคดีดังกล่าวในที่สุด ซึ่งการประสานงานกับทางธนาคารเพื่อแจ้งอายัด และ/หรือขอหลักฐานการโอนต่อไปจนถึงการเบิกถอนเงินจากธนาคารหรือตู้เอทีเอ็ม ตลอดไปจนถึงการขอหลักฐานจากกล้องโทรทัศน์วงจรปิด และนำมาหาข้อมูลต่อไปนั้นเป็นไปได้ยาก เนื่องจากส่วนใหญ่จะอยู่นอกพื้นที่ที่ดูแลและใช้เวลานานในการประสานงานกับธนาคารต่าง ๆ โดยข้อมูลที่ได้รับจากธนาคารเกี่ยวกับบัญชีธนาคารของผู้ต้องสงสัย แบ่งข้อมูลออกเป็น 2 ส่วน ได้แก่

(1) ข้อมูลพื้นฐานเกี่ยวกับบัญชีธนาคาร หมายถึง ข้อมูลของผู้เป็นเจ้าของบัญชี ชื่อ นามสกุล ที่อยู่ หมายเลขโทรศัพท์ รวมถึงวันเวลาที่เปิดบัญชี สาขาที่เปิดบัญชี เป็นต้น

(2) ข้อมูลเกี่ยวกับการทำธุรกรรมของบัญชี หมายถึง ข้อมูลการฝากเงิน ถอนเงิน หรือโอนเงิน เส้นทางการทำธุรกรรมของบัญชีที่เกี่ยวข้อง เป็นต้น

ข้อมูลส่วนนี้ พนักงานสอบสวนจะใช้เพื่อตรวจสอบและระบุตัวตนของผู้ต้องสงสัย หรือผู้ที่มีส่วนเกี่ยวข้อง รวมถึงข้อมูลเกี่ยวกับเส้นทางการทำธุรกรรมของบัญชีนี้ ว่ามีการทำธุรกรรมระหว่างผู้เสียหายและผู้ต้องสงสัยเกิดขึ้นจริงหรือไม่ นอกจากนี้ยังใช้สำหรับการตรวจสอบว่ามีการโอนเงินไปยังบัญชีใด หรือถอนเงินออกจากบัญชีที่ตู้กดเงินสดบริเวณใด เพื่อตรวจสอบและยืนยันตัวตนของผู้กระทำความผิด จากกล้องวงจรปิดในพื้นที่ใกล้เคียงที่มีการถอนสดเงินออกมา

ส่วนหลักฐานที่ผู้เสียหายบางรายมักจะได้มาพร้อมกันคือเลขหมายโทรศัพท์เคลื่อนที่ ซึ่งในปัจจุบันเป็นหลักฐานสำคัญในการสืบสวนไปยังข้อมูลอื่น ๆ ต่อไป โดยการขอความร่วมมือกับผู้ให้บริการโทรศัพท์เคลื่อนที่ที่ได้รับใบอนุญาตจากสำนักงาน กสทช โดยข้อมูลที่ได้รับจากผู้ให้บริการโทรศัพท์เคลื่อนที่ จะเป็นข้อมูลเกี่ยวกับเลขหมายโทรศัพท์ของผู้ต้องสงสัย ข้อมูลการลงทะเบียนของเจ้าของเลขหมายโทรศัพท์จากบัตรประจำตัวประชาชน และภาพถ่ายใบหน้าของเจ้าของเลขหมายโทรศัพท์ พื้นที่ที่ซื้อซิม วิธีการชำระเงินค่าโทรศัพท์ ตลอดทั้งพื้นที่ที่เลขหมายใช้ในวันเวลาดังกล่าว พร้อมหลักฐานการติดต่อกับผู้เสียหาย เพื่อนำสืบไปยังหลักฐานประกอบอื่นๆ ได้ต่อไป

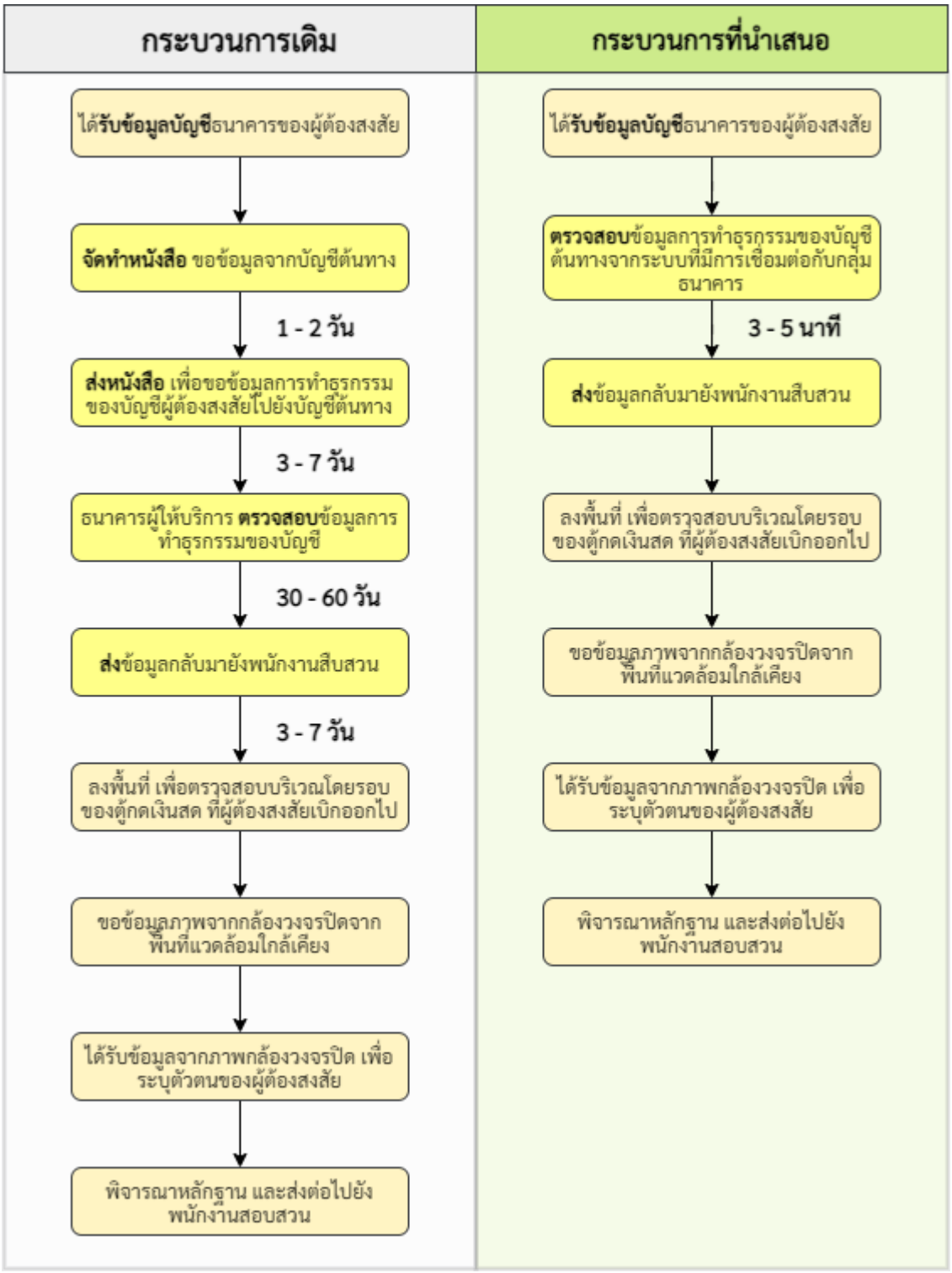
ข้อสรุปในเบื้องต้นจากการจากรวบรวมและวิเคราะห์ข้อมูล และผลการประชุมร่วมกับพนักงานสอบสวนสืบสวน เจ้าหน้าที่ตำรวจที่เกี่ยวข้องถึงแนวทางการพัฒนาระบบต้นแบบเพื่อสนับสนุนงานป้องกันและปราบปรามมิจฉาชีพออนไลน์ที่ไม่ระบุตัวตน สามารถกำหนดได้ว่า การยืนยันตัวตนได้นั้น

หมายถึงการที่สามารถค้นหาข้อมูลประกอบอื่นๆ จากเลขหมายโทรศัพท์เคลื่อนที่ และเจ้าของบัญชีธนาคารพร้อมกัน โดยในโครงการนี้ จะเรียกระบบต้นแบบที่พัฒนาขึ้นว่า **“ระบบป้องกันและปราบปรามมิจฉาชีพออนไลน์ที่ระบุตัวตนไม่ได้ (Unidentified Scammer Prevention and Suppression)”** จะแบ่งระบบงานหลักเป็น 2 ส่วนหลักดังนี้

1) ระบบป้องกันการถูกหลอกจากมิจฉาชีพออนไลน์ที่ไม่สามารถระบุตัวตนได้ สำหรับให้ประชาชนในเขตพื้นที่ศึกษาสามารถใช้ระบบนี้ในการยืนยันตัวตนระหว่างกันก่อนการทำธุรกรรมทางออนไลน์ และการตรวจสอบประเมินความเสี่ยงก่อนการทำธุรกรรม
2) ระบบปราบปรามมิจฉาชีพออนไลน์ที่ไม่สามารถระบุตัวตนได้ สำหรับให้ผู้เสียหายแจ้งความดำเนินคดีผ่านทางออนไลน์กับทางพนักงานสอบสวนพิจารณาก่อนเข้าส่งมอบหลักฐานจริง และติดตามสถานะของคดี พร้อมทั้งระบบที่อำนวยความสะดวกให้กับพนักงานสอบสวนในการค้นหาคดีที่เกี่ยวข้องในพื้นที่อื่นๆ และระบบย่อยในการขอพยานหลักฐานจากผู้ให้บริการโทรศัพท์เคลื่อนที่ และธนาคารที่ให้ความร่วมมือ

โดยในส่วนระบบงานสำหรับพนักงานสอบสวน จะเป็นการรวบรวมข้อมูลและช่วยประเมินความเป็นไปได้ในการรับพิจารณาคดีให้เป็นการแจ้งความเพื่อดำเนินคดี โดยการลดขั้นตอนการแสวงหาพยานหลักฐานจากการขอข้อมูลจากหน่วยงานภายนอก เช่น ผู้ให้บริการโทรศัพท์เคลื่อนที่ ธนาคารพาณิชย์ และระบบอื่นๆ ที่กระบวนการทำงานในปัจจุบันจะใช้ระยะเวลาค่อนข้างมาก ส่งผลให้การสืบสวนมีความล่าช้า มิจฉาชีพอาจไหวตัวทัน ทำให้การจับกุมเป็นไปได้ยากมากขึ้น ส่งผลให้เกิดการไม่รับพิจารณาคดีซึ่งเป็นปัญหาหลักสำหรับผู้เสียหายในปัจจุบัน

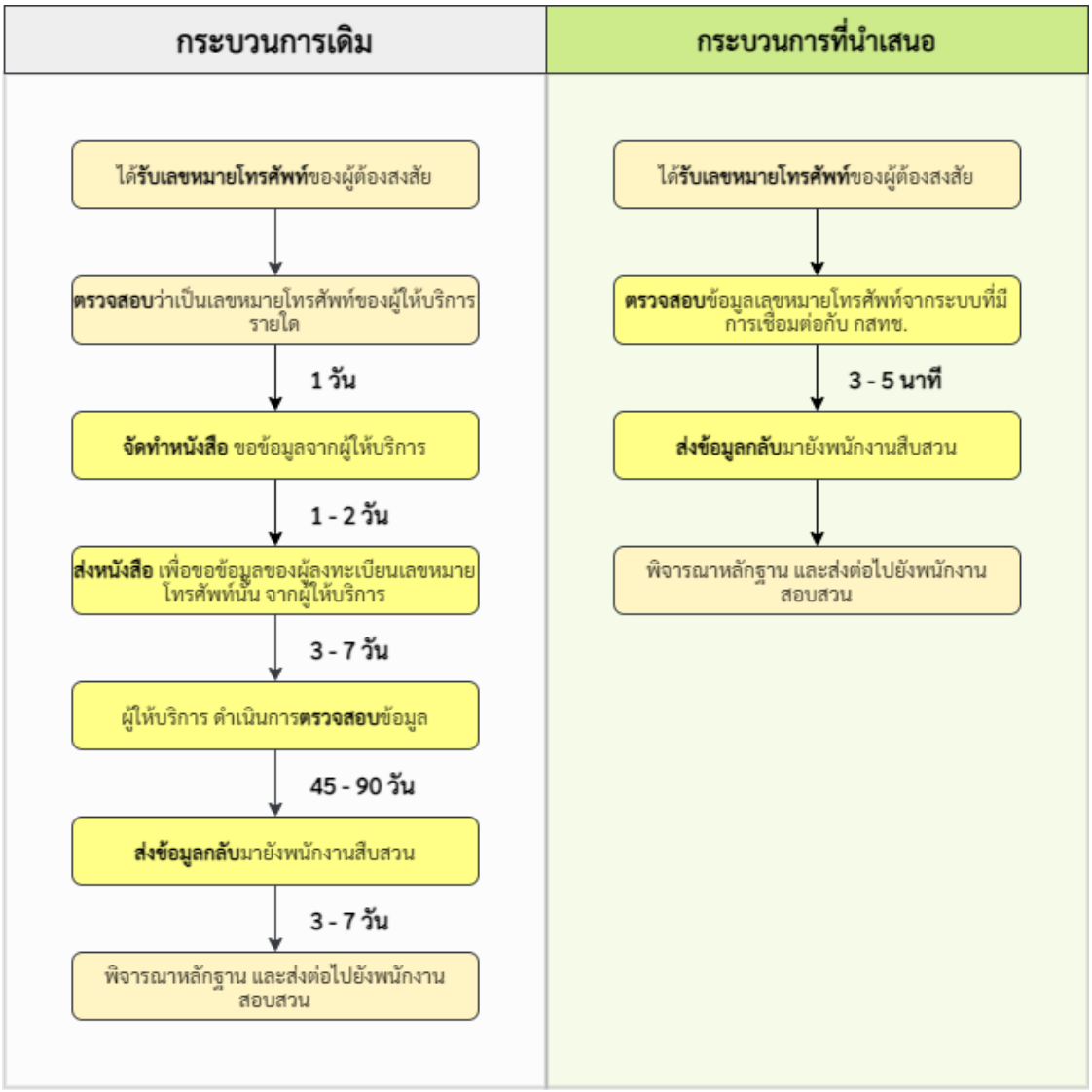
ทางคณะผู้วิจัยได้มีแนวทางการปฏิบัติที่จะช่วยแก้ไขปัญหากระบวนการตรวจสอบข้อมูลที่มีความล่าช้าดังต่อไปนี้



รูปที่ 4-5 กระบวนการขอข้อมูลบัญชีธนาคาร

จากรูปที่ 4-5 จากกระบวนการเดิม เมื่อพนักงานสืบสวนได้รับข้อมูลบัญชีของผู้ต้องสงสัยแล้ว จะต้องดำเนินการทำหนังสือเพื่อขอข้อมูลไปยัง ธนาคารพาณิชย์ผู้ให้บริการ เพื่อตรวจสอบข้อมูลพื้นฐานและข้อมูลเกี่ยวกับการทำธุรกรรมของบัญชีผู้ต้องสงสัย ซึ่งกระบวนการนี้จะใช้ระยะเวลาประมาณ 37 - 76 วัน แต่สำหรับกระบวนการที่ทางคณะผู้วิจัยนำเสนอ หากสามารถตรวจสอบข้อมูลการทำธุรกรรมของ

บัญชีผู้ต้องสงสัยได้จากระบบที่มีการเชื่อมต่อกับกลุ่มธนาคาร จะช่วยลดระยะเวลาการดำเนินการเหลือเพียง 3 - 5 นาที เท่านั้น ซึ่งคาดว่าจะช่วยทำการการนำจับผู้ต้องสงสัยของเจ้าหน้าที่ตำรวจ เป็นไปด้วยความรวดเร็วและสะดวกยิ่งขึ้น



รูปที่ 4-6 กระบวนการขอข้อมูลหมายเลขโทรศัพท์

จากรูปที่ 4-6 จากกระบวนเดิมเมื่อพนักงานสืบสวนได้รับเลขหมายโทรศัพท์ของผู้ต้องสงสัย ต้องดำเนินการหาข้อมูลว่าเลขหมายโทรศัพท์ที่ได้มาเป็นของผู้ให้บริการรายใด จากนั้นจึงทำหนังสือเพื่อขอข้อมูลไปยังผู้ให้บริการโทรศัพท์ และรอผู้ให้บริการโทรศัพท์ส่งข้อมูลกลับมา โดยกระบวนการนี้จะใช้เวลาทั้งสิ้นประมาณ 53 - 107 วัน แต่สำหรับกระบวนการที่ทางคณะผู้วิจัยนำเสนอ หากสามารถตรวจสอบข้อมูลเลขหมายโทรศัพท์จากระบบที่มีการเชื่อมต่อกับ กสทช. จะทราบข้อมูลภายใน 3 - 5 นาที ซึ่งจะช่วยให้การยืนยันตัวตนผู้กระทำความผิดเป็นด้วยความรวดเร็ว ส่งผลให้การสืบสวนของตำรวจกระทำได้อย่างทันท่วงที สามารถเข้าจับกุมผู้ต้องสงสัยได้ทันเวลา

บทที่ 5
ผลการรวบรวมข้อมูลจากการประชุมแต่ละกลุ่ม

บทที่ 5 นี้ จัดทำขึ้นเพื่อสรุปข้อมูลที่ได้จากการประชุมกับหน่วยงานต่าง ๆ รวมทั้งสรุปผลจากการจัดงานเสวนาวิชาการกลุ่มย่อย (Focus Group) ครั้งที่ 1 และครั้งที่ 2 และการจัดประชุมแถลงผลการดำเนินงาน

5.1 การประชุมกับหน่วยงานต่าง ๆ

ทางคณะผู้วิจัย ได้ร่วมประชุมเพื่อหาแนวทางในการออกแบบและพัฒนาระบบต้นแบบเพื่อสนับสนุนงานป้องกันและปราบปรามมิจฉาชีพออนไลน์ โดยมีรายละเอียดดังต่อไปนี้

5.1.1 ตารางการประชุมกับหน่วยงานภายนอก

ตารางที่ 5.1 ตารางการประชุมกับหน่วยงานภายนอก

วันที่	ประเด็น	ส่วนงาน	ผู้เข้าประชุม
24 มิ.ย. 64	งานเสวนาวิชาการกลุ่มย่อย (Focus Group) เรื่อง “มิจฉาชีพออนไลน์ : ภาพรวมปัญหาและแนวทางป้องกันและปราบปราม” และ “การออกแบบระบบต้นแบบเพื่อสนับสนุนงานป้องกันและปราบปรามมิจฉาชีพออนไลน์”		รายละเอียดผู้เข้าร่วมแสดงดังข้อ 5.2
16 ก.ย. 64	แนวทางความร่วมมือในการสนับสนุนการปฏิบัติงานของเจ้าหน้าที่ตำรวจ	เว็บไซต์ Blacklistseller	- ผู้ดูแลเว็บไซต์ Blackliseller
4 ต.ค. 64	แนวทางในการดำเนินคดีบนโลกออนไลน์	กองบังคับการสืบสวนสอบสวน กองบัญชาการตำรวจนครบาล 1-9	- พล.ต.ต.โชคชัย งามวงศ์ (รอง ผบช.น.) - พ.ต.อ. นิภพล สุขนิยม (ผู้กำกับการสืบสวน บก.น.8) - พ.ต.อ.ดร. ปราโมทย์ จันทร์บุญแก้ว (ผู้กำกับการฝ่ายตรวจสอบสำนวนคดีฎีกา) - รอง ผกก. จาก กก. สส.บก.น.1-9

วันที่	ประเด็น	ส่วนงาน	ผู้เข้าประชุม
6 ต.ค. 64	แนวทางการแก้ไขปัญหามิจฉาชีพออนไลน์	กรมการปกครอง กระทรวงมหาดไทย	- พ.ต.อ.ดร. ปราโมทย์ จันทร์บุญแก้ว (ผู้กำกับการฝ่ายตรวจสอบสำนวนคดีฎีกา) - เจนภพ ชะด้าบู้ (เจ้าหน้าที่จากกรมการปกครอง กระทรวงมหาดไทย)
8 ต.ค. 64	แนวทางการสืบสวนปราบปรามมิจฉาชีพออนไลน์ที่ไม่ระบุตัวตน	ธนาคารแห่งประเทศไทย	
18 ต.ค. 64	แนวทางการแก้ไขปัญหามิจฉาชีพออนไลน์	สำนักงานตำรวจแห่งชาติ สำนักงาน กสทช. และผู้ให้บริการโทรศัพท์เคลื่อนที่	- พล.ต.ต.โชคชัย งามวงศ์ (รองผบช.น. หัวหน้างานสืบสวน (สส.)) - พ.ต.อ. นิภพล สุขนิยม (ผู้กำกับการสืบสวน บก.น.8) - พ.ต.อ.ดร. ปราโมทย์ จันทร์บุญแก้ว (ผู้กำกับการฝ่ายตรวจสอบสำนวนคดีฎีกา) - นางสาวอรวรี เจริญพร (ผู้อำนวยการสำนัก. สำนักบริหารและจัดการเลขหมายโทรคมนาคม) - นายศุภกาญจน์ บุญจันทร์ (ผู้อำนวยการส่วน ส่วนพัฒนางานดิจิทัลและการระบุตัวตนทางดิจิทัล) - เจ้าหน้าที่จากผู้ให้บริการโทรศัพท์เคลื่อนที่ 7 ราย
19 ต.ค. 64	แนวทางการแก้ไขปัญหา	สำนักงานพัฒนา	

วันที่	ประเด็น	ส่วนงาน	ผู้เข้าประชุม
	มิจฉาชีพออนไลน์	ธุรกรรมทางอิเล็กทรอนิกส์	
21 ต.ค. 64	แนวทางการพัฒนาฐานข้อมูล Blackistseller.com (BLS)	เว็บไซต์ Blacklistseller	- ผู้ดูแลเว็บไซต์ Blackliseller - ที่ปรึกษาเว็บไซต์ Blackliseller
18 ก.พ. 65	งานเสวนาวิชาการกลุ่มย่อย (Focus Group) เรื่อง “การนำเสนอผลการออกแบบและพัฒนาระบบต้นแบบเพื่อสนับสนุนงานป้องกันและปราบปรามมิจฉาชีพออนไลน์และรับฟังความคิดเห็น”	มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร	รายละเอียดผู้เข้าร่วมแสดงดังข้อ 5.3
17 มี.ค. 65	ประชุมแถลงผลโครงการ	สมาพันธ์ชมรมคุ้มครองผู้บริโภคกรุงเทพฯ	สมาชิกสมาพันธ์ชมรมคุ้มครองผู้บริโภคกรุงเทพฯ

5.1.2 ผลสรุปประเด็นสำคัญจากการประชุมทั้ง 7 ครั้ง

5.1.2.1 ประเด็นที่ได้จากการประชุมกับ Blacklistseller ครั้งที่ 1

(1) แนวทางความร่วมมือในการแลกเปลี่ยนข้อมูล

ทางคณะผู้วิจัยได้แจ้งให้ผู้ดูแลเว็บไซต์ Blacklistseller ทราบถึงที่มาของโครงการ ประโยชน์ของข้อมูลในเว็บไซต์ฯ รวมถึงตัวอย่างการร่วมมือกับหน่วยงานตำรวจ พร้อมมีมติเห็นชอบในการพัฒนาความร่วมมือระหว่างกัน

คณะผู้วิจัย เสนอให้มีการดึงข้อมูลจากหน้าเว็บไซต์ที่เปิดเผยต่อสาธารณะมาใช้ (Web scrape) เพื่อทดสอบระบบที่คณะผู้วิจัยกำลังพัฒนาขึ้น ซึ่งทางเว็บไซต์กำลังอยู่ในขั้นตอนการพัฒนา Webservice/API โดยทั้งสองฝ่ายมีมติเห็นชอบสำหรับร่างแนวทางการเชื่อมโยงข้อมูล

5.1.2.2 ประเด็นที่ได้จากการประชุมกับ Blacklistseller ครั้งที่ 2

(1) การพัฒนาระบบของ Blacklistseller เพื่อเชื่อมต่อข้อมูล

คณะผู้วิจัยและผู้จัดทำเว็บไซต์ Blacklistseller สอบทานความเข้าใจเกี่ยวกับข้อเสนอขอบเขตการดำเนินการและค่าใช้จ่าย สำหรับการพัฒนาระบบฐานข้อมูล Blacklistseller.Com (BLS) สำหรับโครงการจัดทำแนวทางพัฒนาระบบต้นแบบ เพื่อสนับสนุนงานป้องกันและปราบปรามมิจฉาชีพออนไลน์ที่ไม่สามารถระบุตัวตน โดยคณะผู้วิจัย จะนำข้อเสนอที่ได้ไปเสนอต่อสำนักงานตำรวจ หรือกองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะ อีกครั้งหนึ่ง

(2) การดำเนินการของเว็บไซต์ Blacklistseller

หน้าที่หลักของเว็บไซต์ Blacklistseller คือ การเปิดเผยบัญชีของผู้กระทำความผิด ดังนั้น แนวทางการลงประกาศของเว็บไซต์ Blacklistseller สามารถยกเลิกประกาศนั้น ๆ เองได้ โดยจะขึ้นอยู่กับดุลยพินิจของเว็บไซต์เอง หรือหากมีการรับผิดชอบ หรือไกล่เกลี่ยกับคู่กรณีเป็นที่เรียบร้อยแล้ว ก็จะสามารถยกเลิกประกาศนั้นได้

ในกรณีที่มีผู้เสียหาย แจ้งผู้ขายโกงผ่านทางเว็บไซต์แล้วปรากฏว่าเป็นเท็จ กรณีนี้ จะเป็นความรับผิดชอบของผู้กล่าวหา ตาม พรบ. คอมพิวเตอร์ มาตรา 14 ที่ถูกเรียกว่าความผิดฐาน “นำเข้าข้อมูลคอมพิวเตอร์อันเป็นเท็จ”

5.1.2.3 ประเด็นที่ได้จากการประชุมกับกรมการปกครอง

(1) แนวทางความร่วมมือในการแลกเปลี่ยนข้อมูล

- คณะผู้วิจัยได้แจ้งความสงค์ในการเชื่อมต่อระบบกับเพื่อตรวจสอบสถานะของบัตรประชาชนว่ายังใช้งานอยู่หรือไม่ และเพื่อตรวจสอบข้อมูลและการยืนยันตัวตน

- ผู้เชี่ยวชาญฯ จากกรมการปกครอง ได้ให้ข้อมูลว่าระบบที่จะพัฒนานี้สามารถเชื่อมต่อกับฐานข้อมูลของกรมการปกครองได้ในรูปแบบใดบ้าง สามารถแลกเปลี่ยนข้อมูลอะไรได้บ้าง และให้ชื่อผู้ติดต่อทั้งทางเทคนิคและทางเอกสาร

(2) แนวทางอื่น ๆ

- กรมการปกครองได้ให้ข้อมูลเกี่ยวกับสิ่งที่ทางกรมกำลังดำเนินการ ได้แก่ D.DOPA และแผนการพัฒนาระบบ Digital ID

- กรมการปกครองให้ มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร ทำการตรวจสอบว่า ได้เคยลงนามในหนังสือความร่วมมือในการเชื่อมต่อระบบสำหรับการตรวจสอบข้อมูลนักศึกษาหรือไม่ ถ้ามีจะต้องทำการสืบค้นเพื่อหาเอกสารดังกล่าว

5.1.2.4 ประเด็นที่ได้จากการประชุมกับกองบัญชาการตำรวจนครบาล และผู้แทนจากธนาคารแห่งประเทศไทย

แนวทางความร่วมมือในการแลกเปลี่ยนข้อมูล

- คณะผู้วิจัยนำเสนอที่มาและความสำคัญของโครงการให้ผู้แทนจาก ธปท. ได้รับทราบและได้แจ้งความประสงค์ในการเชื่อต่อข้อมูล
- มีการอภิปรายร่วมกันในประเด็นที่เกี่ยวกับข้อกฎหมาย และอำนาจหน้าที่ของตำรวจ
- ผู้แทนจาก ธปท. ได้ให้มุมมองที่เกี่ยวข้องกับต้นทุนของธนาคารหากมีการเชื่อมต่อระบบ
- ผู้แทนจาก ธปท. ได้ให้แนะนำให้ทาง บช.น. และ บก.น.8 ไปศึกษาแนวทางการเชื่อมต่อจาก ป.ป.ส. และ ป.ป.ง. เนื่องจาก 2 หน่วยงานนั้น ได้มีการเชื่อมต่อและแลกเปลี่ยนข้อมูลกับ ธปท./ธนาคาร แล้ว

5.1.2.5 ประเด็นที่ได้จากการประชุมกับ สำนักงาน กสทช. และผู้ให้บริการโทรศัพท์เคลื่อนที่ (2 ครั้ง)

(1) แนวทางความร่วมมือในการแลกเปลี่ยนข้อมูล

- ผู้ให้บริการโทรศัพท์เคลื่อนที่เสนอให้ใช้ Mobile ID ที่ผู้ให้บริการโทรศัพท์เคลื่อนที่กำลังดำเนินการ สำหรับการสมัครและยืนยันตัวตน
- ในการเข้าถึงข้อมูลต้องมีระบบการรักษาความปลอดภัยที่ระบุและกำหนดว่าระดับการเข้าถึงหรือสิทธิ์ของผู้ใช้ผ่านตัวตน (Authorization)
- มีการอภิปรายกันในประเด็นเรื่องอำนาจหน้าที่ และขอบเขตความรับผิดชอบของทางตำรวจหรือหน่วยงานที่ต้องการเข้าถึงข้อมูลของผู้ใช้งานโทรศัพท์
- นอกจากนี้ ยังมีข้อเสนอว่า ต้องมีข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA) เพื่อให้การดำเนินการแล้วเสร็จภายในเวลา 3 วัน
- ต้องการให้มีการรับรองฐานอำนาจในการเชื่อมต่อข้อมูล และการขอข้อมูลที่ชัดเจน
- การขอข้อมูลในกรณี Fasttrack ซึ่งอาจมีค่าใช้จ่าย ตัวแทนผู้ให้บริการโทรศัพท์เคลื่อนที่ให้ความเห็นว่าไม่จำเป็น
- ผู้แทนจาก สคบ. ได้ร่วมให้ความเห็นด้วย โดยเฉพาะประเด็นที่ทางคณะผู้วิจัยเสนอว่าเสนอว่า ผู้เสียหายควรมีสิทธิ์ขอตรวจสอบข้อมูลโดยไม่มีค่าใช้จ่ายแค่ครั้งเดียว ไม่ควรถูกโกงบ่อยและขอตรวจสอบข้อมูลผ่านระบบบ่อย ๆ

(2) แนวทางอื่น ๆ

ผู้แทนของตำรวจขอให้ตั้งกลุ่มไลน์ (LINE) สำหรับการประสานงานระหว่าง กสทช. ตำรวจ ผู้ให้บริการโทรศัพท์เคลื่อนที่ ในระหว่างการพัฒนาระบบและการเชื่อมต่อฐานข้อมูลต่าง ๆ

5.1.2.6 ประเด็นที่ได้จากการประชุมกับฝ่ายให้คำปรึกษา สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA)

แนวทางความร่วมมือและการหารือในประเด็นที่เกี่ยวข้อง

- สำนักงานฯ มีการทำความร่วมมือกับหน่วยงานต่างๆ ที่เกี่ยวข้องเพื่อร่วมกันพัฒนาระบบที่ทำหน้าที่เป็นตัวกลางในการเชื่อมต่อและแลกเปลี่ยนข้อมูล โดยในระยะแรกนี้เป็นการพัฒนาและทดสอบในระบบ Sandbox หาก มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร ต้องการเชื่อมต่อให้ประสานเข้ามาในภายหลัง

- ผู้แทนของสำนักงานฯ ได้ให้ข้อมูลและอธิบายเกี่ยวกับ Mobile ID, NDID, Digital ID และ DBD Verified ที่ทางสำนักงานมีบทบาท

- คณะผู้วิจัยได้สอบถามเกี่ยวกับศูนย์รับเรื่องร้องเรียน (OCC 1212) ที่ได้รับการจัดตั้งขึ้นเพื่อคุ้มครองผู้บริโภคออนไลน์ และได้สอบถามเกี่ยวกับความเป็นไปได้ในการเชื่อมต่อและแลกเปลี่ยนข้อมูล แต่เจ้าหน้าที่ของสำนักงานฯ ได้แสดงความกังวลในประเด็น พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล PDPA แล้วแนะนำให้ประสานเพื่อหารือเพิ่มเติมในประเด็นดังกล่าวต่อไปในอนาคต

5.2 งานเสวนาวิชาการกลุ่มย่อย ครั้งที่ 1

ทางผู้วิจัย ได้จัดงานเสวนาวิชาการกลุ่มย่อย (Focus Group) เรื่อง “มิจฉาชีพออนไลน์ : ภาพรวมปัญหาและแนวทางป้องกันและปราบปราม” และ “การออกแบบระบบต้นแบบเพื่อสนับสนุนงานป้องกันและปราบปรามมิจฉาชีพออนไลน์” ในวันพฤหัสบดีที่ 24 มิถุนายน 2564 ณ โรงแรม รามาการ์เด้นส์ กรุงเทพฯ โดยมีรายละเอียดของงาน ดังนี้

5.2.1 รายชื่อผู้เข้าร่วมงานประชุมเสวนาวิชาการกลุ่มย่อย

5.2.1.1 รายชื่อผู้ทรงคุณวุฒิฯ

1) พ.ต.อ. นิภพล สุขนิยม กองบังคับการตำรวจนครบาล 8

2) พ.ต.อ.ดร. ปราโมทย์ จันทร์บุญแก้ว สำนักงานกฎหมายและคดี สำนักงานตำรวจแห่งชาติ

3) คุณศรัณย์ ทองคำ จากกองป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

4) คุณจุฑาธัช คูเกษมรัตน์ จากสถาบันเพื่อการยุติธรรมแห่งประเทศไทย

5) คุณธนะชัย สุนทรเวช จากสถาบันเพื่อการยุติธรรมแห่งประเทศไทย

6) คุณรังสรรค์ วิริยะวารี จากบริษัทเบสท์ เอ็นเตอร์ไพรส์ จำกัด

7) คุณปรเมศร์ เพียรสกุล จากบริษัทเอซิสโปรเฟสชั่นนัล เซ็นเตอร์ จำกัด

8) คุณศุภกาญจน์ บุญจันทร์ จากสำนักบริหารและจัดการเลขหมายโทรคมนาคม กสทช.

9) คุณกษิดิศ กรสิทธิ์ จากสำนักอนุญาตประกอบกิจการโทรคมนาคม 2 กสทช.

10) คุณพิชิต แก้วมาคูณ จากบริษัท ดีแทค ไตรเน็ต จำกัด

11) พ.ต.ท. บดินทร วิยาภรณ์ สำนักงานป้องกันและปรามการฟอกเงิน

12) พ.ต.อ.ณัทกฤช พรหมจันทร์ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

13) คุณอาริยา อาขุบุตร จากบริษัท บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (ประชุมทางไกล)

หมายเหตุ

คณะผู้วิจัยได้ทำหนังสือเชิญผู้แทนจาก บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) บริษัท ทรูมูฟ เอช ยูนิเวอร์แซล คอมมิวนิเคชัน จำกัด และธนาคารกรุงไทย จำกัด (มหาชน) ด้วย แต่ผู้แทนไม่ได้เดินทางเข้าร่วมประชุมในวันดังกล่าว เนื่องจากบางท่านติดภารกิจอื่น

5.2.2 ภาพบรรยากาศการ Focus Group ครั้งที่ 1

รูปที่ 5-1 ประธานในพิธีกล่าวเปิดงาน

รูปที่ 5-2 พิธีกรกล่าวแนะนำผู้ทรงคุณวุฒิ

รูปที่ 5-3 ผู้เข้าร่วมการประชุมเสวนาวิชาการกลุ่มย่อย (Focus Group)

รูปที่ 5-4 ผู้ดำเนินรายการระหว่างการประชุมเสวนาฯ

รูปที่ 5-5 การประชุมเสวนาฯ (1)

รูปที่ 5-6 การประชุมเสวนาฯ (2)

5.2.3 บันทึกการประชุมเสวนา

เวลา 9:00 น. ดร.ณัฐวรพล รัชสิริวัชรบุล รักษาการแทนอธิการบดี มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร ประธานในพิธี ได้กล่าวเปิดงาน โดยได้กล่าวถึงที่มาของโครงการและสภาพปัญหาภัยคุกคามจากผู้ไม่ประสงค์ดีที่อาศัยช่องโหว่ ทั้งจากคน ระบบ และกระบวนการ ตลอดจนข้อกฎหมายที่ยังมีจุดอ่อน และข้อจำกัดต่างๆ ที่กลายเป็นช่องทางให้มิจฉาชีพแอบแฝงเข้ามาหาผลประโยชน์ด้วยกลโกงรูปแบบต่าง ๆ โดยใช้การเปลี่ยนเลขหมายโทรศัพท์มือถือไปเรื่อย ๆ และใช้เครือข่ายอินเทอร์เน็ตสาธารณะเป็นเครื่องมือหลักในการกระทำความผิดเพื่อหลอกเหยื่อซึ่งอาจเป็นผู้ซื้อหรือผู้ขายที่ไม่ได้ทำการตรวจสอบตัวตนจริงของบุคคลที่ทำธุรกรรมด้วยอย่างละเอียดถี่ถ้วน นอกจากนี้ยังมีปัจจัยร่วมอื่น คดีเหล่านี้ส่วนใหญ่เป็นคดีความที่มีมูลค่าความเสียหายน้อย ทำให้ผู้เสียหายไม่อยากเสียเวลาในการแจ้งความดำเนินคดี ทั้งที่มิจฉาชีพเหล่านี้ได้กระทำความผิดกับผู้เสียหายเป็นจำนวนมาก และมีมูลค่ารวมมหาศาลแต่ไม่ถูกดำเนินคดี

เมื่อสิ้นสุดพิธีเปิด ดร.เทอดพงษ์ แดงสี หัวหน้าโครงการฯ ได้บรรยายถึงที่มา และวัตถุประสงค์ในการจัดโครงการฯ โดยได้กล่าวถึงการทำธุรกรรมออนไลน์ในปัจจุบัน ที่มีแนวโน้มที่เติบโตขึ้นเรื่อย ๆ ด้วยการพัฒนาเทคโนโลยีจากต่างประเทศ ธุรกิจอีคอมเมิร์ซ (E-commerce) ในประเทศ และความสะดวกในการทำธุรกรรมทางการเงิน ซึ่งทำให้ประชาชนทั่วไปสามารถจะเป็นผู้ซื้อ-ผู้ขายได้เนื่องจากติดต่อซื้อขายกันได้ง่ายขึ้นผ่านเครือข่ายอินเทอร์เน็ต เช่น การซื้อขายออนไลน์ สั่งซื้ออาหารออนไลน์ สั่งสินค้าแบบชำระเงินล่วงหน้า (Pre-order) รวมไปถึงการสมัครขอสินเชื่อดอกเบี้ยต่ำ การซื้อขายตามเว็บไซต์ การประกาศขายสินค้าผ่านช่องทางสังคมสื่อออนไลน์ Facebook, Instagram, LINE หรือ การทำธุรกรรมอื่นๆ ทางออนไลน์ ในเนื้อหาการบรรยาย ได้ระบุว่า นอกจากการที่ประชาชนในประเทศให้ความสนใจ ซื้อขาย หรือทำธุรกรรมต่างๆ ผ่านช่องทางสื่อ และสังคมออนไลน์ จะทำให้เกิดผลประโยชน์ให้เชิงบวกแล้ว การซื้อขาย หรือทำธุรกรรมต่างๆ ผ่านช่องทางสื่อ และสังคมออนไลน์ ยังทำให้เกิดผลกระทบในด้านลบ ซึ่งเป็นภัยคุกคามที่มาจากมิจฉาชีพออนไลน์ ที่มักจะมีกลโกงที่แอบแฝงมาในรูปแบบต่าง ๆ เพื่อหลอกหรือล่อลวงผู้ที่ซื้อขายหรือทำธุรกรรมออนไลน์ ที่ไม่ได้มีการตรวจสอบข้อมูลในการยืนยันตัวตนที่แท้จริงของบุคคลเหล่านี้โดยละเอียด ซึ่งมิจฉาชีพเหล่านี้มักจะมีการใช้วิธีการในการฉ้อโกงโดยการใช้หมายเลขโทรศัพท์มือถือ และเครือข่ายอินเทอร์เน็ตเป็นเครื่องมือหลักในการกระทำความผิด สำนักงาน กสทช. จึงต้องการศึกษาระบบการติดตาม ป้องกัน และต่อต้านการกระทำความผิดของมิจฉาชีพออนไลน์ ทั้งในและต่างประเทศ โดยได้คัดเลือกให้คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร ดำเนินการโครงการ พัฒนาระบบต้นแบบเพื่อสนับสนุนงานป้องกัน และปราบปรามมิจฉาชีพออนไลน์ ที่ไม่ระบุตัวตน (ระยะที่ 1) เพื่อพัฒนาเป็นระบบต้นแบบสำหรับช่วยในการติดตามหาผู้ประทำความผิดมาดำเนินคดี

จากนั้นผู้ดำเนินรายการได้เชิญให้ผู้ทรงคุณวุฒิซึ่งเป็นผู้แทนจากหน่วยงานต่าง ๆ ร่วมกันแสดงความคิดเห็น และร่วมกันให้ข้อมูลที่คาดว่าจะเป็นประโยชน์ต่อการดำเนินโครงการ ซึ่งสรุปสาระสำคัญได้ดังนี้

1) พ.ต.อ. ดร.ปราโมทย์ จันทร์บุญแก้ว ผู้กำกับการฝ่ายตรวจสอบสำนวนคดีฎีกา ส่วนตรวจสอบสำนวนคดีอุทธรณ์และฎีกา สำนักงานตำรวจแห่งชาติ ได้ชี้แจงและให้ความคิดเห็นเกี่ยวกับปัญหาที่เกิดขึ้นในการปฏิบัติหน้าที่ ทั้งปัญหาในการติดตาม และจับกุมผู้กระทำความผิดเพื่อนำมารับโทษที่ใช้เวลาในการดำเนินงานเป็นระยะเวลานาน อันเนื่องมาจากการเข้าถึงข้อมูลที่ทำได้ยาก และขาด

เครื่องมือในการติดตามที่รวดเร็ว จึงทำให้ผู้กระทำความผิดก่อเหตุหรือก่อคดีซ้ำกับผู้เสียหายรายอื่น ทางเจ้าหน้าตำรวจจึงขอความร่วมมือไปยังผู้ที่เกี่ยวข้อง เพื่อหาวิธีการในการลดเวลาในการติดตามจับกุมผู้กระทำความผิดมารับโทษ และป้องกันความเสียหายที่อาจเกิดขึ้นกับเหยื่อรายอื่น โดยการสนับสนุนให้เจ้าหน้าที่สามารถทำการจับกุมผู้กระทำความผิดให้ได้อย่างทันท่วงที และสามารถคืนทรัพย์สินให้ผู้เสียหายได้ ซึ่งจะเกิดประโยชน์อย่างยิ่ง นอกจากนี้ พ.ต.ท.ดร.ปราโมทย์ จันทร์บุญแก้ว ยังได้ให้ข้อเสนอแนะเพิ่มเติมโดยอ้างถึงองค์ประกอบในการเกิดอาชญากรรมว่าประกอบด้วย 3 องค์ประกอบ คือ ผู้เสียหาย ผู้กระทำความผิด และช่องโอกาส จาก 3 องค์ประกอบนี้ ทางหน่วยงานตำรวจสามารถดำเนินการในส่วนข้อมูลของผู้กระทำความผิดได้โดยตรง จากการเก็บข้อมูลหลักฐานในการกระทำความผิดนั้น และทำการตรวจสอบเบื้องต้นในกรณีที่เกิดการทำผิดซ้ำ จากข้อมูลในระบบทางเจ้าหน้าที่ตำรวจสามารถจะดำเนินการจากแบล็คลิสได้ทันที แต่ในส่วนของผู้เสียหายจะไม่ทราบเข้าถึงข้อมูลนี้ จึงอยากให้มีการพัฒนาระบบที่เป็นศูนย์ข้อมูลกลาง เช่น ข้อมูลเบอร์โทรศัพท์ของผู้กระทำความผิด เพื่อให้ประชาชนที่ยังไม่ตกเป็นเหยื่อเข้าไปตรวจสอบข้อมูลได้ นอกจากนี้ท่านยังได้กล่าวเสริมว่า ต้องการให้เกิดความร่วมมือกันระหว่างตำรวจ ผู้ให้บริการเครือข่ายโทรศัพท์มือถือและหน่วยงานที่เกี่ยวข้อง ที่ร่วมมือกันในการแก้ปัญหามิจฉาชีพออนไลน์ให้ลดน้อยลง แม้ไม่สามารถแก้ปัญหาได้ทั้งหมดก็ตาม ก็ยังถือว่าเป็นสิ่งดี

2) คุณรังสรรค์ วิริยะวารี Project Director ผู้แทน Best Enterprise Co., Ltd. ผู้พัฒนาระบบของธนาคาร (และเคยเป็นผู้บริหารในธนาคารแห่งหนึ่ง) ได้ชี้แจงและให้ความคิดเห็นว่า ปัญหาที่พบมากที่สุดในส่วนของการทำงานและการพัฒนาระบบหลังบ้านของธนาคาร และกล่าวว่า ธนาคารมีระบบการทำงาน และการเก็บข้อมูลที่แตกต่างกัน ในบางธนาคารก็มีระบบการจัดเก็บข้อมูลที่เป็นระบบสามารถตรวจสอบข้อมูลได้อย่างระเอียดและสมบูรณ์ แต่ในบางธนาคารก็ไม่ได้ให้ความสำคัญในการเก็บข้อมูลที่มีมูลค่าน้อย แต่มุ่งเน้นไปในการเก็บข้อมูลที่มีมูลค่ามาก จึงอาจทำให้การติดตามข้อมูลในส่วนที่มีมูลค่าน้อย (ซึ่งในที่นี้หมายถึงข้อมูลที่ใช้ในการตรวจสอบการเคลื่อนไหวของบัญชี หรือตรวจสอบเส้นทางการเงิน เมื่อเป็นคดีความหรือเมื่อตำรวจร้องขอ) ค่อนข้างที่จะใช้เวลา นอกจากนี้ คุณรังสรรค์ วิริยะวารี ยังได้กล่าวเสริมว่า ธนาคารโดยส่วนใหญ่มีข้อมูลการทำธุรกรรมทางการเงินของลูกค้าอยู่แล้ว ฉะนั้นสิ่งที่ธนาคารควรจะให้ความสำคัญ คือการพัฒนาระบบการยืนยันตัวตนของลูกค้า ซึ่งจะเป็นระบบที่ตรวจสอบความผิดปกติในการทำธุรกรรมของลูกค้า และสามารถโทรแจ้งลูกค้าของทางธนาคารได้เมื่อเกิดความผิดปกติ โดยได้ยกตัวอย่างกรณีที่ลูกค้าถูกล่อลวงให้ทำการโอนเงินออกจากบัญชีเป็นจำนวนมากผิดปกติเมื่อเปรียบเทียบจากสถิติเดิม ถ้าระบบของทางธนาคารเป็นระบบที่ถูกออกแบบไว้อย่างดี ในระบบจะมีการแจ้งเตือนและทางธนาคารสามารถทำการโทรแจ้งลูกค้าเกี่ยวกับความผิดปกติที่เกิดขึ้นโดยด่วน เพื่อระงับเหตุให้รวดเร็วที่สุด อย่างไรก็ดี การติดต่อลูกค้าของธนาคารไม่ควรใช้วิธีการส่ง SMS ในการแจ้งเหตุ

3) คุณศรัณย์ ทองคำ ผู้แทนจากกองป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้ให้ข้อมูลเกี่ยวกับปัญหาในการปฏิบัติงานที่เป็นเหตุให้ทางกระทรวงฯ ให้ทำการงานและจัดการข้อมูลได้ล่าช้า ในการณีที่มีผู้ร้องขอข้อมูลจากกระทรวง หรือขอให้ทางกระทรวงช่วยดึงข้อมูลที่ต้องการ อันเนื่องมาจากการไม่ระบุความต้องการของข้อมูล ที่จะใช้เป็นพยานพิสูจน์หลักฐานทางคดีอาชญากรรมออนไลน์ จึงนำเสนอในที่ประชุมว่า ผู้ที่เกี่ยวข้องหรือผู้พัฒนาระบบ ควรดำเนินการแก้ไขปรับปรุงในส่วนของรายละเอียดการขอข้อมูลจากกระทรวงดิจิทัล โดยให้ระบุความต้องการที่ชัดเจนว่ามีความต้องการข้อมูลในส่วนใดบ้าง และควรเป็นการขอข้อมูลที่เฉพาะเจาะจงที่ต้องการนำไปใช้ในการดำเนินการสอบสวนสืบสวนจริง นอกจากนี้ คุณศรัณย์

ทองคำ ยังได้มีการแสดงความคิดเห็นเพิ่มเติมว่า ในการเกิดอาชญากรรมออนไลน์นอกจากจะเกิดจากผู้ก่อเหตุหาช่องว่างในการซื้อขายหรือทำธุรกรรมออนไลน์หรือแฝงตัวมาเพื่อทำการฉ้อโกงแล้ว สาเหตุอีกประการหนึ่ง มาจากการที่ประชาชนหรือบริษัทขนาดเล็กหรือ SME ไม่มีความรู้ที่ถูกต้องในการซื้อขายหรือทำธุรกรรมออนไลน์ทั้งในและต่างประเทศ จึงให้ความคิดเห็นว่า ควรมีการให้ความรู้ประชาชนทั่วไปให้เข้าถึงข้อมูลด้านการซื้อขายหรือทำธุรกรรมออนไลน์ ที่อัปเดตรอบด้าน และครบถ้วน โดยผ่านระบบการเก็บข้อมูลส่วนกลาง

4) คุณปรเมศร์ เพียรสกุล ผู้แทนจากบริษัทเอซิสโปรเฟสชั่นนัล เซ็นเตอร์ จำกัด ซึ่งเชี่ยวชาญด้านการดูแลรักษาความมั่นคงปลอดภัยทางไซเบอร์ ได้แสดงความคิดเห็นว่า ปัญหาของการเกิดอาชญากรรมออนไลน์ สาเหตุหลักที่พบ เกิดจากการไม่ระบุตัวตนที่แท้จริงในการทำธุรกรรมหรือการซื้อขายออนไลน์ และได้กล่าวว่าสื่อสังคมออนไลน์ที่ทำให้เกิดอาชญากรรม ในการฉ้อโกงออนไลน์มากที่สุด ก็คือ Facebook แต่เนื่องด้วย Facebook เป็นแพลตฟอร์มขนาดใหญ่และไม่ได้มีเงื่อนไขผูกมัดหรืออยู่ภายใต้การดูแลของประเทศไทย จึงค่อนข้างที่จะเป็นเรื่องยากในการเข้าไปควบคุม ทั้งนี้ คุณปรเมศร์ ได้ให้ข้อเสนอแนะในการแก้ไขการเกิดอาชญากรรมเบื้องต้นเอาไว้ดังนี้

- ขอความร่วมมือจากทุกฝ่ายหรือทุกภาคส่วนที่เกี่ยวข้อง ในการรวบรวมข้อมูลการเกิดอาชญากรรม หรือการฉ้อโกงออนไลน์จากการใช้งาน Facebook ในประเทศ และให้ผู้นำหรือรัฐบาลเป็นสื่อกลางในการเจรจาเพื่อให้แพลตฟอร์มทราบซึ่งปัญหาที่เกิด และให้ความร่วมมือในการแก้ไข
- เข้มงวดในการดำเนินการลงทะเบียนผู้ค้าหรือผู้ที่ซื้อขายออนไลน์ทั้งหมด และจะต้องมีการเสียภาษีให้กรมสรรพากรอย่างถูกต้อง เพื่อยื่นยันตัวตนที่แท้จริงและง่ายต่อการตรวจสอบข้อมูล

5) พ.ต.ท. บดินทร วิยาภรณ์ สำนักงานป้องกันและปรามการฟอกเงิน (ปปง.) ได้ให้ข้อคิดเห็นและข้อเสนอเอาไว้ว่า การเกิดเหตุอาชญากรรมออนไลน์เป็นปัญหาเรื้อรัง ดังนั้นควรมีการนำเสนอข้อเท็จจริงให้ประชาชนทั่วไปได้รับทราบ โดยนำเสนอข้อมูลเกี่ยวกับคดีที่เกิดขึ้นจริง เพื่อให้ผู้ที่ยังไม่ตกเป็นเหยื่อได้ทราบถึงข้อมูลที่เป็นจริง นอกจากนี้ควรจัดให้มีหน่วยงานที่รับผิดชอบในการประสานงานและประชาสัมพันธ์ข้อมูลอาชญากรรมออนไลน์โดยตรง เพื่อให้ทำหน้าที่ติดตาม ประสานงานระหว่างหน่วยงานที่มีส่วนร่วมในการดำเนินการจับกุมผู้ก่อเหตุ และอัปเดตข้อมูล ตลอดจนการประชาสัมพันธ์ให้ประชาชนเป็นทราบเป็นระยะ เพื่อป้องกันการเกิดการก่อเหตุซ้ำ นอกจากนี้ ในช่วงท้ายท่านได้เสริมว่า ทาง ปปง. มีระบบที่สามารถร้องขอข้อมูลจากทางธนาคารหรือสถาบันการเงินได้อย่างรวดเร็ว เนื่องจากมีกฎหมายที่บังคับให้ทุกธนาคารจะต้องส่งข้อมูลให้ ปปง. หากเกี่ยวข้องกับการฟอกเงิน

6) พ.ต.อ. นิภพล สุขนิยม กองบังคับการตำรวจนครบาล 8 ได้ท้าวความถึงความเป็นมาของโครงการ และได้กล่าวขอบคุณทาง กสทช. ที่ให้การสนับสนุนโครงการนี้ จากนั้นท่านได้เล่าถึงสภาพปัญหาที่เกิดขึ้น ไม่ว่าจะเป็นประเด็นปัญหาที่ ตำรวจไม่ค่อยอยากจะรับแจ้ง เนื่องจากเป็นคดีเล็กน้อย และยอมความได้ ในขณะที่ตำรวจก็มีปัญหาในการสืบสวนและเข้าถึงข้อมูลได้ยาก หรือในบางกรณีคนร้ายใช้บัญชีนอมินีในการทำธุรกรรม การจับเจ้าของบัญชี จึงมักจะไม่ใช่คนร้ายตัวจริง และท่านได้ชี้ให้เห็นถึงปัญหาในการเข้าถึงข้อมูลของคนร้าย และขอความร่วมมือจากผู้เกี่ยวข้องเพื่อให้ตำรวจสามารถเข้าถึงข้อมูลได้ง่ายขึ้น เพื่อให้สามารถนำคนร้ายเข้าสู่กระบวนการยุติธรรม และเยียวยาผู้เสียหายหรือสามารถช่วยเหลือประชาชนที่ถูกหลอกได้ นอกจากนี้ยังได้ให้ข้อมูลเกี่ยวกับคดีโรแมนซ์สแกมเอาไว้ด้วย

7) พ.ต.อ.ณัทกฤช พรหมจันทร์ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ได้อธิบายให้ผู้เข้าร่วมประชุมได้ทราบถึง ลำดับการเก็บข้อมูล เพื่อใช้เป็นพยานหลักฐานในการจับกุมผู้ก่อเหตุ ซึ่งประกอบด้วย

- ข้อมูลต้นทาง ซึ่งหมายถึงข้อมูลของผู้สียหายที่ใช้เป็นหลักฐานในการในการร้องทุกข์ เช่น เลขหมายโทรศัพท์ บัญชีธนาคาร หรือหลักฐานการจากหน้าจอในขณะสนทนาข้อความกับผู้ก่อเหตุ
- ข้อมูลระหว่างทาง ซึ่งเป็นข้อมูลที่อยู่ในหน่วยงานที่ให้บริการ อันเกิดจากการแลกเปลี่ยนข้อมูล เช่น ธนาคาร เครือข่ายโทรศัพท์ หรือเว็ปไซต์ เป็นต้น
- ข้อมูลปลายทาง ซึ่งหมายถึงข้อมูลของผู้ก่อเหตุ และเป็นส่วนที่สำคัญที่สุด เมื่อเกิดเหตุ และมีการตรวจสอบข้อมูลจากข้อมูลต้นทาง และระหว่างทาง ถ้าข้อมูลปลายทางมีความสอดคล้องกัน ก็สามารถดำเนินคดีได้ตามกฎหมาย หากข้อมูลในส่วนปลายทางไม่มีความสอดคล้องกัน ไม่มีหลักฐานในการพิสูจน์ตัวตนของผู้ก่อเหตุ อาจทำให้เกิดการยกฟ้องเนื่องจากเอกสารหลักฐานไม่เพียงพอก็ได้

จากข้อมูลข้างต้น พ.ต.อ.ณัทกฤช พรหมจันทร์ จึงให้ข้อเสนอแนะว่า ควรจะมีการจัดเก็บข้อมูลให้เป็นมาตราฐานเดียวกันภายใต้กรอบของกฎหมาย และทำการพัฒนาช่องทางการปฏิบัติงานระหว่างผู้เกี่ยวข้องและเจ้าหน้าที่ตำรวจ โดยมีข้อมูลส่วนกลางเพื่อใช้ในการดำเนินการสืบสวน นอกจากนี้ ควรมีการจัดทำเช็คลิสต์ (Checklist) ที่ระบุความต้องการข้อมูล พยานหลักฐาน ให้เป็นไปในทิศทางเดียวกัน ป้องกันการสอบถามข้อมูลที่อาจพลาดตกหล่น และเป็นเครื่องมือที่ช่วยเจ้าหน้าที่ตำรวจให้สามารถทำการสอบถามง่ายขึ้น นอกจากนั้นแล้ว ควรมีการพัฒนาระบบใช้ฐานข้อมูลกลางระหว่างหน่วยงานที่จะใช้ดำเนินงาน และควรเปิดเป็นสาธารณะให้ประชาชนเข้าถึงได้ และประเด็นสุดท้าย ได้มีการเสนอแนะเกี่ยวกับการสร้างความสัมพันธ์ระหว่างหน่วยงานที่เกี่ยวข้อง เพื่อให้แต่ละหน่วยงานรับทราบปัญหาและการยอมรับร่วมกัน แล้วร่วมกันแก้ไขและพัฒนาระบบให้เป็นไปในทิศทางเดี่ยวกัน

8) คุณศุภกาญจน์ บุญจันทร์ สำนักบริหารและจัดการเลขหมายโทรคมนาคม ได้กล่าวถึงวิธีการที่มิจฉาชีพออนไลน์ใช้ในการล่อลวงผู้เสียหาย และได้ให้ข้อเสนอแนะว่า ในการดำเนินโครงการนี้ต้องการให้คณะผู้วิจัยที่ได้รับทุนในการพัฒนาระบบ ทำการติดต่อกับหน่วยงานที่เกี่ยวข้องกับการทำธุรกิจออนไลน์ เช่น กรมพัฒนาธุรกิจการค้า กระทรวงพานิชย์ เพื่อสร้างการรับรู้ที่ปลอดภัยและมีความน่าเชื่อถือโดยอาจผ่านการรับรองจากกระทรวงพาณิชย์ และมีการยืนยันตัวตนที่ชัดเจนและลดการก่อเหตุอาชญากรรมออนไลน์ นอกจากนี้ คุณศุภกาญจน์ บุญจันทร์ ยังได้ให้ข้อมูลว่า ทางสำนักงาน กสทช. มีระบบที่เชื่อมกับข้อมูลเลขหมายโทรศัพท์และข้อมูลของผู้ที่ลงทะเบียนเลขหมายโทรศัพท์ของผู้ให้บริการอยู่แล้ว ซึ่งทางโครงการสามารถดำเนินการเพื่อขอชื่อมต่อกับระบบดังกล่าวได้

9) คุณพิชิต แก้วมาคูณ ผู้แทนจากบริษัท ดีแทค ไตรเน็ต จำกัด ได้แจ้งให้ที่ประชุมทราบมีความยินดีให้ความร่วมมือและสนับสนุนหน่วยงานที่เกี่ยวข้อง ในการมอบหลักฐานหรือให้ข้อมูลจากบริษัททุกด้านภายใต้ข้อกฎหมายกำหนด โดยได้ชี้แจงประเด็นเรื่องความล่าช้าในการสืบค้นและให้ข้อมูลแก่ทางเจ้าหน้าที่ โดยยินดีที่จะให้ความร่วมมือเพื่อให้กระบวนการดังกล่าวรวดเร็วขึ้น นอกจากนี้ยังได้แสดงความคิดเห็นว่า ในส่วนของคู่ค้าของบริษัทที่มีการส่ง SMS เพื่อหลอกลวง บริษัทสามารถดำเนินการต่าง ๆ ได้แต่จะไม่สามารถดำเนินการได้ ถ้าหากการกระทำผิดเกิดขึ้นในระดับแพล็ตฟอร์ม

10) คุณอาริยา อาขุบุตร ผู้แทนจาก บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด ได้แจ้งให้ที่ประชุมทราบมีความยินดีให้ความร่วมมือ และสนับสนุนหน่วยงานที่เกี่ยวข้องในการตรวจสอบขอข้อมูลเสมอมา ซึ่งทางบริษัทเองก็ได้พยายามป้องกันปัญหาเหล่านี้อยู่แล้ว เช่น กรณีของการฟิชชิ่ง หากตรวจพบ

ก็จะทำการบล็อก สำหรับปัญหาเรื่องระยะเวลาในการค้นหาข้อมูล หากเป็นข้อมูลที่มีความสำคัญ ทางบริษัทจำเป็นที่จะต้องดำเนินการตามขั้นตอน อาจจะต้องใช้ระยะเวลามากกว่า ข้อมูลพื้นฐานปกติ แต่ก็จะรีบดำเนินการให้รวดเร็วที่สุด

11) ดร.ธริศร์ ทิมทอง ที่ปรึกษาโครงการได้เสนอว่า ควรมีการพัฒนาระบบที่สามารถเชื่อมต่อกับฐานข้อมูลของผู้ให้บริการ เพื่อเวลาที่ตำรวจมีการร้องขอข้อมูล จะได้ดำเนินการได้รวดเร็วขึ้น (ประเด็นนี้ผู้แทนจาก กสทช. ได้ให้ข้อเสนอแนะว่าให้เชื่อมต่อผ่านระบบของ กสทช.) นอกจากนี้ ดร.ธริศร์ ทิมทอง ได้เปิดประเด็น เกี่ยวกับการตรวจสอบไอพีแอดเดรสมิจฉาชีพแบบเรียบไทม์ด้วย (แต่ พ.ต.อ.ณัทกฤช พรหมจันทร์ ได้ตอบประเด็นนี้ว่า ในประเทศไทยยังไม่มีกฎหมายรองรับ ยกเว้นกรณีกฎหมายความมั่นคง เป็นต้น)

12) คุณธนะชัย สุนทรเวช ผู้แทนจากสถาบันเพื่อการยุติธรรมแห่งประเทศไทย ได้ให้ข้อมูลว่าเกี่ยวกับบทบาทหน้าที่ของหน่วยงานที่เกี่ยวข้องกับการดูแลผู้ต้องขัง งานระหว่างประเทศ และงานวิจัยและพัฒนาศักยภาพของบุคลากรของกระทรวงยุติธรรม และกล่าวว่าปัจจุบันผู้บริหารของทางสถาบันมีแนวคิดที่จะผลักดันงานในประเทศด้วย และท่านเองยินดีที่จะสนับสนุนโครงการนี้ เช่น ช่วยด้านประชาสัมพันธ์ และจะนำเสนอประเด็นเรื่องมิจฉาชีพออนไลน์นี้ให้กับทางผู้บริหารได้รับทราบด้วย

13) คุณจุฑาธัช คูเกษมรัตน์ ผู้แทนจากสถาบันเพื่อการยุติธรรมแห่งประเทศไทย ได้กล่าวเสริมว่า ทางสถาบันก็มีโครงการที่ขับเคลื่อนเกี่ยวกับการฉ้อโกงออนไลน์อยู่แล้วด้วย แต่เป็นการดำเนินการระหว่างตำรวจกับทางธนาคาร เพื่อให้สามารถระงับบัญชีได้รวดเร็วยิ่งขึ้นโดยอาศัย ซึ่งก็คล้ายกับแนวคิดของทางโครงการที่กำลังดำเนินการกับผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่

14) คุณกษิดิศ กรสิทธิ์ ผู้แทนจากสำนักอนุญาตประกอบกิจการโทรคมนาคม 2 กสทช. ได้กล่าวถึงการแก้ปัญหาแก๊งคอลล์เซ็นเตอร์ที่ทาง กสทช. ได้ร่วมมือกับไอเอสพี (หรือผู้ให้บริการอินเทอร์เน็ต) และผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ ในการให้ข้อมูลและให้ความรู้กับประชาชน ส่วนประเด็นเรื่องแพล็ตฟอร์มต่างๆ นั้น อาจต้องใช้วิธีขอความร่วมมือจากผู้ให้บริการแพล็ตฟอร์ม เนื่องจากอยู่นอกเหนืออำนาจของ กสทช.

15) ผศ.กร พวงนาค ผู้ช่วยอธิการบดีฝ่ายการเงินและทรัพย์สิน นักวิจัยและพัฒนาระบบ ได้แสดงความคิดเห็นว่า ต้องการให้คณะผู้วิจัยคำนึงถึงภาคประชาชนเป็นหลัก และได้กล่าวว่า การพัฒนาระบบแม้จะเป็นระบบที่มีประสิทธิภาพดีเพียงใด หากขาดประชาชนที่ผู้เป็นใช้งาน ก็ถือว่าระบบนั้นพัฒนาไม่สำเร็จ จึงเห็นควรให้ความมุ่งเน้นการพัฒนาว่าทำอย่างให้ให้ประชาชนรับรู้ และเกิดการใช้งาน

จากการประชุมเสวนาดังกล่าว ที่ประชุมมีมติร่วมกันคือ รับทราบและพร้อมที่จะให้ความร่วมมือและสนับสนุนโครงการนี้

5.3 งานเสวนาวิชาการกลุ่มย่อย ครั้งที่ 2

ทางผู้วิจัย ได้จัดงานเสวนาวิชาการกลุ่มย่อย (Focus Group) เรื่อง “การนำเสนอผลการออกแบบและพัฒนาระบบต้นแบบเพื่อสนับสนุนงานป้องกันและปราบปรามมิจฉาชีพออนไลน์ และรับฟังความคิดเห็น” ในวันศุกร์ที่ 18 กุมภาพันธ์ 2565 ผ่านระบบออนไลน์ โดยมีรายละเอียดของงาน ดังนี้

5.3.1 รายชื่อผู้เข้าร่วมงานประชุมเสวนาวิชาการกลุ่มย่อย

5.3.1.1 รายชื่อผู้ทรงคุณวุฒิ

1) พ.ต.อ. นิภพล สุขนิยม กองบังคับการตำรวจนครบาล 8

2) พ.ต.อ.ดร. ปราโมทย์ จันทร์บุญแก้ว ผู้กำกับการฝ่ายอำนวยการ 5 กองบังคับการอำนวยการ กองบัญชาการตำรวจนครบาล

3) พ.ต.ท.ณัทกฤช พรหมจันทร์ ผู้อำนวยการสำนักปฏิบัติการ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

4) นายศุภกาญจน์ บุญจันทร์ ผู้อำนวยการส่วนพัฒนางานดิจิทัลและการระบุตัวตนทางดิจิทัล สำนักบริหารและจัดการเลขหมายโทรคมนาคม สำนักงาน กสทช.

5) นายภควัต ทะสังขา วิศวกรปฏิบัติการระดับกลาง ส่วนพัฒนางานดิจิทัลและการระบุตัวตนทางดิจิทัล สำนักบริหารและจัดการเลขหมายโทรคมนาคม สำนักงาน กสทช.

6) พ.ต.ต.พิษณุ เอี่ยมสวัสดิ์ ผู้อำนวยการฝ่าย ผู้บริหารฝ่าย Investigation บมจ. ธนาคารกรุงไทย

7) นางดวงใจ กุศลฉันท์ ผู้อำนวยการฝ่ายกำกับการปฏิบัติงาน ธนาคารออมสิน

8) นางสาวภัควลัญชญ์ ติณวโรดม เหรัญญิกสมาคมสถาบันการเงินของรัฐ สมาคมสถาบันการเงินของรัฐ

9) นางไลวรรณ ปองเสงี่ยม เลขาธิการสมาคมสถาบันการเงินของรัฐ สมาคมสถาบันการเงินของรัฐ

10) นางสาวทานตะวัน วังชมภู ผู้ช่วยผู้อำนวยการสำนักจัดการและป้องกันการกระทำทุจริต ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร

11) นายวรณัฐ สุโฆษสมิต เจ้าหน้าที่ประสานงานโครงการ สถาบันเพื่อการยุติธรรมแห่งประเทศไทย

12) นายทรงวุฒิ ชินวัฒนกูล รักษาการหัวหน้าส่วนกำกับกฎเกณฑ์เทคโนโลยีสารสนเทศฯ ธนาคารอาคารสงเคราะห์ ฝ่ายกำกับการปฏิบัติงาน

13) นายจุฑาธัช คูเกษมรัตน์ เจ้าหน้าที่ประสานงานโครงการ สถาบันเพื่อการยุติธรรมแห่งประเทศไทย

14) นายธนชาติ พิมพ์สวัสดิ์ ผู้ช่วยเจ้าหน้าที่ประสานงานโครงการ สถาบันเพื่อการยุติธรรมแห่งประเทศไทย

15) นางสาวอโนชา บุญรัศมี ผู้ช่วยเจ้าหน้าที่ประสานงานโครงการ สถาบันเพื่อการยุติธรรมแห่งประเทศไทย

16) นางสาวพงศ์รวี ธัญญสิริ นักศึกษาฝึกงาน สถาบันเพื่อการยุติธรรมแห่งประเทศไทย

17) พ.ต.ต.ไกรทอง โพธิ์ตาด รองอัยการจังหวัดเชียงใหม่ สำนักงานอัยการสูงสุด

18) นายวรุณ กาญจนภู รองเลขาธิการสมาคมธนาคารไทย สมาคมธนาคารไทย

19) พ.ต.ต.วิณพ วงษ์อารักษ์ ผู้ตรวจสอบอาวุโส ฝนช. ธนาคารแห่งประเทศไทย
20) นายอนุภาค มาตรมูล ผู้ช่วยผู้อำนวยการ ฝตท. ธนาคารแห่งประเทศไทย
21) น.ส.ภาวิตา เฮงเจริญ ผู้ตรวจสอบอาวุโส ฝตท. ธนาคารแห่งประเทศไทย
22) นางนริศรา รวมศิริวัฒนกุล นิติกรอาวุโส (ควบ) ฝกม. ธนาคารแห่งประเทศไทย
23) นายเอกสิทธิ์ สุดแก้ว ผู้ช่วยผู้อำนวยการ ฝรภ. ธนาคารแห่งประเทศไทย
24) พ.ต.ต.เมธา โคตร์สันเทียะ ผู้ช่วยผู้อำนวยการ ฝรภ. ธนาคารแห่งประเทศไทย
25) นายณัฐพล พิพิธรัตน์ เจ้าหน้าที่สืบสวน ฝรภ. ธนาคารแห่งประเทศไทย
26) พ.ต.ท.ปริทัศน์ รัตนรักษ์ เจ้าหน้าที่สืบสวน ฝรภ. ธนาคารแห่งประเทศไทย
27) นายปรมัตถ์ ไวรักษ์ เจ้าหน้าที่สืบสวน ฝรภ. ธนาคารแห่งประเทศไทย
28) ร.ต.ท.หญิง วราภรณ์ ฉัตรเจริญมิตร เจ้าหน้าที่สืบสวน ฝรภ. ธนาคารแห่งประเทศไทย
29) ร.ต.อ.เตชินท์ บุญขันธ์ เจ้าหน้าที่สืบสวน ฝรภ. ธนาคารแห่งประเทศไทย
30) ร.ต.อ.ต่อตระกูล นาคผจญ เจ้าหน้าที่สืบสวน ฝรภ. ธนาคารแห่งประเทศไทย
31) พ.ต.ท. บดินทร วิยาภรณ์ สำนักงานป้องกันและปรามการฟอกเงิน

5.3.1.2 รายชื่อตัวแทนคณะผู้วิจัย

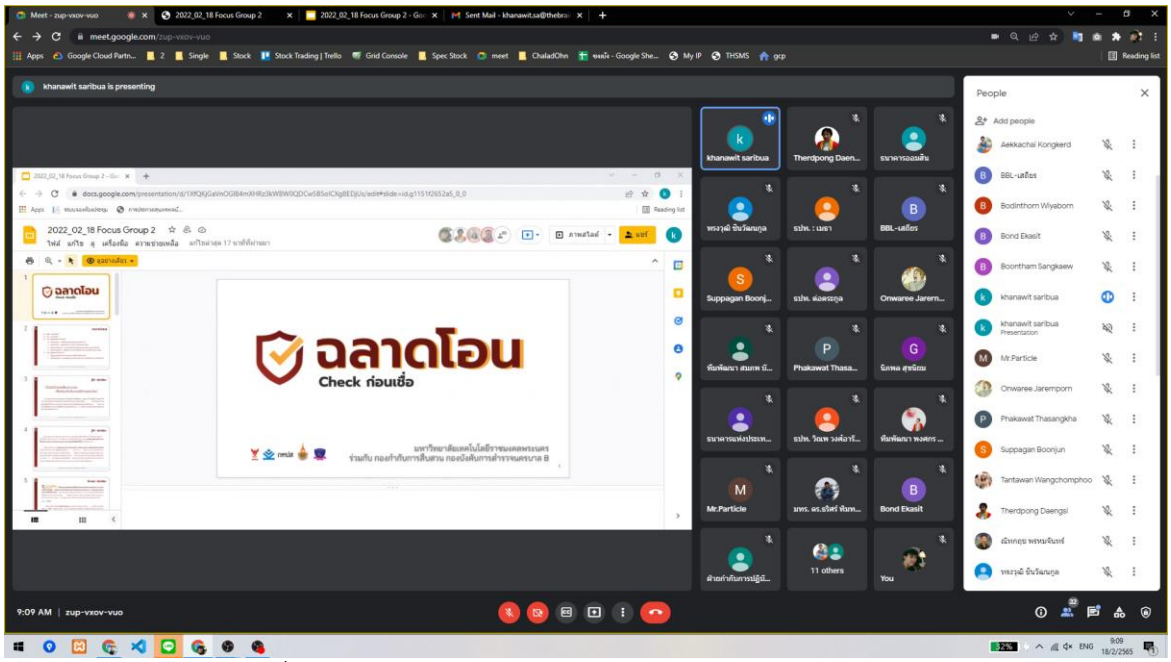
1) ดร.เทอดพงษ์ แดงสี หัวหน้าโครงการ มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร
2) ดร.ธริศร์ ทิมทอง ที่ปรึกษา

5.3.1.3 รายชื่อพิธีกรดำเนินรายการ

ดร.ณัฏฐ์ชยธร วัทธิกรสิริกุล มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร

5.3.2 ภาพบรรยากาศการ Focus Group ครั้งที่ 2

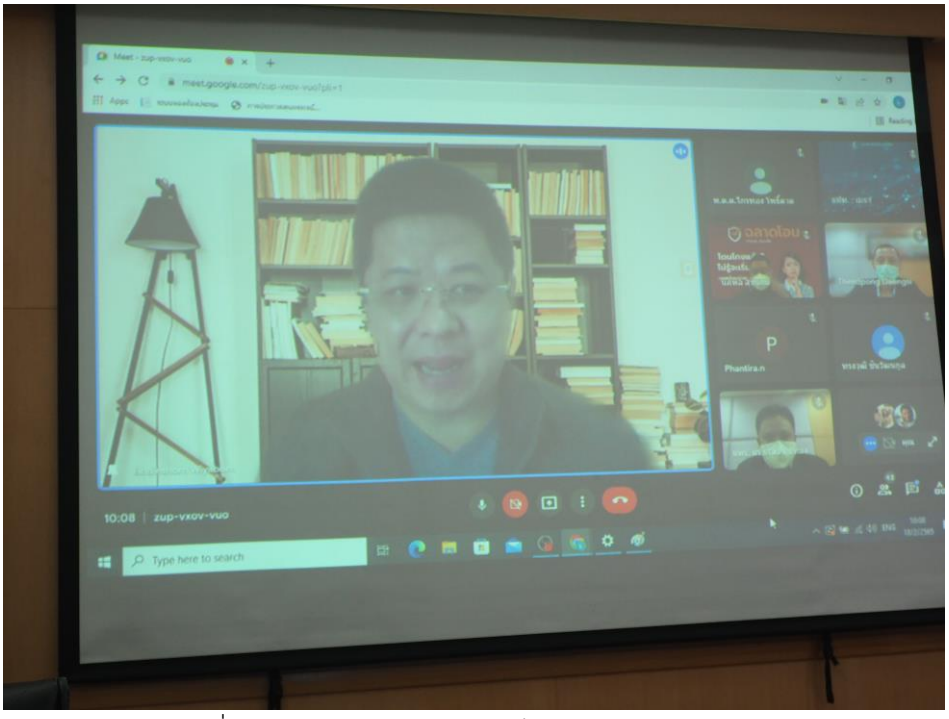
รูปที่ 5-7 ประธานกล่าวเปิดงาน



รูปที่ 5-8 การนำเสนอระบบฉลาดโอนโดย ดร.เทอดพงษ์ แดงสี

รูปที่ 5-9 ผู้เข้าร่วมประชุม Focus Group ครั้งที่ 2

รูปที่ 5-10 บรรยากาศการประชุม



รูปที่ 5-11 การแสดงความคิดเห็นจากผู้เข้าร่วมประชุม

5.3.3 บันทึกการประชุมเสวนา

ผู้ดำเนินรายการ เริ่มกล่าวนำเสนอการประชุมเสวนาวิชาการ กลุ่มย่อยครั้งที่ 2 ได้นำเสนอ ผลการออกแบบพัฒนาระบบต้นแบบเพื่อสนับสนุนการป้องกันและปราบปรามมิจฉาชีพออนไลน์ ประชุม ณ ตึกอธิการบดีชั้น 4 ห้องประชุมบัวม่วง สำนักงานอธิการบดีมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร และได้รับเกียรติจากท่านอธิการบดีกล่าวเปิดงาน

ดร.ณัฐวรพล รัชสิริวัชรบุล รักษาการแทนอธิการบดี มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร ประธานในพิธี ได้กล่าวเปิดงาน โดยกล่าวถึงเรื่อง การนำผลการออกแบบพัฒนาระบบต้นแบบเพื่อสนับสนุนการป้องกันและปราบปรามมิจฉาชีพออนไลน์ และเป็นการรับฟังความคิดเห็น จากผู้ทรงคุณวุฒิ ผู้แทนหน่วยงานและองค์กรที่เกี่ยวข้อง ตลอดจนผู้วิจัยและทีมงาน ซึ่งโครงการนี้ได้รับการสนับสนุนจากกองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมเพื่อประโยชน์สาธารณะ หรือ กทปส. เป็นงบประมาณประจำปี 2564 ซึ่งในปัจจุบันความก้าวหน้าและวิธีการสื่อสารต่าง ๆ กับอินเทอร์เน็ต ผนวกกับการระบาดของโรคโควิด-19 ทำให้มีการทำธุรกรรมออนไลน์เพิ่มขึ้นอย่างเป็นจำนวนมาก ทั้งในแง่ของการซื้อสินค้าออนไลน์ รวมถึงในการทำธุรกรรมอื่น ๆ มีแอปพลิเคชันและสื่อสังคมออนไลน์ต่าง ๆ ที่เติบโตขึ้นอย่างมาก ปัญหาที่ตามมาคือการคุกคามไม่ประสงค์ดีอาศัยช่องว่างต่าง ๆ รวมถึงช่องว่างทางกฎหมายที่ยังมีจุดอ่อนและข้อจำกัด เป็นช่องทางให้มิจฉาชีพเหล่านี้แฝงตัวเข้ามาหาผลประโยชน์ด้วยกลโกงรูปแบบต่าง ๆ สำนักงาน กทปส. ได้เล็งเห็นปัญหานี้และได้คัดเลือกให้คณะวิศวกรรมศาสตร์มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร ทำการศึกษาและพัฒนาระบบต้นแบบเพื่อป้องกันและปราบปรามปัญหาที่เกิดขึ้น โครงการนี้ได้รับความร่วมมือจาก กองบัญชาการตำรวจนครบาล กองกำกับการสืบสวน กองบังคับตำรวจนครบาล 8 และจึงเป็นที่มาของการจัดการประชุมออนไลน์ในครั้งนี้

เมื่อสิ้นสุดพิธีเปิด ดร.เทอดพงษ์ แดงสี หัวหน้าโครงการฯ ได้บรรยายถึงที่มาของเว็บไซต์ฉลาดโอน มีฟังก์ชันอะไรและสามารถช่วยตำรวจดำเนินการกับคนร้ายหรือจัดการกับมิจฉาชีพออนไลน์ได้อย่างไรบ้างและเว็บไซต์นี้สามารถช่วยประชาชนได้อย่างไร โดยได้กล่าวถึงแนวคิด ต้องการที่จะช่วยเหลือประชาชนเพื่อป้องกันภัยจากการฉ้อโกงออนไลน์ ด้วยความก้าวหน้าของเทคโนโลยีอินเทอร์เน็ตประชาชนสามารถทำธุรกรรม ผ่านโทรศัพท์มือถือ ผ่านแอปธุรกรรมต่าง ๆ ได้โดยไม่จำเป็นต้องไปธนาคาร ในช่วงการระบาดของเชื้อไวรัสโควิด-19 ทำให้ประชาชนมีพฤติกรรมใช้งานบริการต่าง ๆ ผ่านธุรกรรมออนไลน์เพิ่มมากขึ้น ด้วยนโยบายของธนาคารไม่มีการเก็บค่าธรรมเนียม ทำให้การทำธุรกรรมออนไลน์เป็นไปได้ง่ายขึ้น ถึงการทำธุรกรรมออนไลน์จะสะดวก แต่ก็แฝงไปด้วยภัยคุกคามจากมิจฉาชีพที่อาศัยช่องโหว่จากประชาชนผู้ซื้อขาย จากระบบ จากกระบวนการต่าง ๆ ตลอดจนข้อกฎหมายที่ยังมีช่องว่าง ทำให้มิจฉาชีพแอบแฝงเข้ามาหาผลประโยชน์ด้วยกลโกงรูปแบบต่างๆ ด้วยข้อจำกัดทำให้การจับกุมผู้กระทำผิดมาลงโทษได้ยาก ทำให้ปัญหาเหล่านี้เกิดขึ้นมาก จึงเป็นที่มาของโครงการนี้ ซึ่งเป็นระบบต้นแบบที่เป็นตัวกลางในการบูรณาการ แลกเปลี่ยนข้อมูลและความร่วมมือระหว่างหน่วยงานราชการและหน่วยงานเอกชนที่เกี่ยวข้อง เพื่อให้ประชาชนสามารถเข้ามาตรวจสอบคนโกงหรือมิจฉาชีพออนไลน์ได้ และได้มีการแนะนำฟังก์ชันของเว็บไซต์ฉลาดโอน ได้แก่ ฟังก์ชันแรก เช็คก่อนโอน ประชาชนสามารถเข้ามาตรวจสอบเลขบัญชี ชื่อบัญชีของผู้โอนก่อนตัดสินใจทำธุรกรรม แหล่งที่มาของข้อมูลจาก ข้อมูลของหน่วยงานทั้งภาครัฐ หน่วยงานเอกชนและข้อมูลจากประชาชนที่แจ้งเข้ามาในเว็บไซต์ฉลาดโอน ซึ่งกระบวนการนี้ผู้แจ้งจะต้องมีการยืนยันตัวตน ฟังก์ชันที่สอง แจ้งคนโกง การแจ้งข้อมูลคนโกงเพื่อป้องกันไม่ให้ประชาชนคนอื่นตกเป็น

เหยื่อ ข้อมูลผู้แจ้ง มีชื่อนามสกุล เบอร์โทรศัพท์และยืนยันตัวตน e-KYC เมื่อยืนยันตัวตนเสร็จสามารถใส่ข้อมูลคนโกง ได้แก่ชื่อนามสกุล ข้อมูลบัญชีธนาคาร หลักฐานการโอนเงินและหลักฐานการสนทนาส่งเข้ามาในระบบ ฟังก์ชันที่สาม ช่วยรวมหลักฐาน จะมีทีมงานแอดมิน คอยดูแลรับฟังปัญหา จัดการเอกสาร สรุปพฤติการณ์และสร้างไฟล์เอกสาร PDF เพื่อให้สะดวกและง่ายต่อผู้เสียหายในการแจ้งความดำเนินคดี ข้อมูลในการแจ้งความดำเนินคดีประกอบด้วย ข้อมูลผู้เสียหาย ข้อมูลคนโกง รายละเอียดพฤติการณ์ หลักฐานการโอนเงินและหลักฐานการสนทนา ฟังก์ชันที่สี่ เช็คตัวตนผู้ขาย เพื่อสร้างเครือข่ายผู้ขายที่สุจริต ซึ่งมีการยืนยันตัวตนของผู้ขายและตรวจสอบหลายชั้น ซึ่งการตรวจสอบมี 4 ชั้นได้แก่ 1.ตรวจสอบเลขหลังบัตรประชาชนมีการลิงค์กับกรมการปกครอง 2.ตรวจสอบเบอร์มือถือกับสำนักงาน กสทช. 3. ตรวจสอบใบหน้ากับรูปในบัตรประชาชนว่าเป็นคนเดียวกันหรือไม่ 4.ตรวจสอบชื่อบัญชีธนาคารกับชื่อในบัตรประชาชน ซึ่งสถิติการใช้งานช่วง 7 วันที่ผ่านมา บันทึกข้อมูลเมื่อวันที่ 15 กุมภาพันธ์ 2565 มีจำนวนรายการตรวจสอบมากกว่า 60,000 คน มีจำนวนผู้ที่ลงทะเบียนทั้งหมดเกือบ 4,000 คน และจำนวนการเพิ่มเพื่อน LINE เพื่อติดต่อ 2,798 คน การติดต่อผ่านช่องทางไลน์จากจำนวนเพื่อน 2,798 คน ซึ่งร้อยละ 61.81 ต้องการให้ช่วยรวบรวมหลักฐาน ร้อยละ 27.31 เป็นการเช็คคนโกง ร้อยละ 8.1 เป็นการแจ้งคนโกง และร้อยละ 2.77 เป็นการเช็คตัวตนผู้ขาย ผลการตอบรับจากประชาชนผ่านสื่อสังคมออนไลน์ มีทั้งชื่นชมและมีให้คำแนะนำ รวมถึงเว็บไซต์ต่าง ๆ มีการนำเว็บไซต์ฉลาดโอนไปเผยแพร่และขยายความต่อ สรุปฉลาดโอน ต้องการที่จะเป็นส่วนหนึ่งที่จะช่วยเหลือสังคม ร่วมสร้างสังคมออนไลน์ปลอดภัยและลดจำนวนผู้เสียหาย “เพื่อไม่ให้มีใครตกเป็นเหยื่อของมิจฉาชีพออนไลน์อีกต่อไป”

จากนั้นผู้ดำเนินรายการได้เชิญให้ผู้ทรงคุณวุฒิซึ่งเป็นผู้แทนจากหน่วยงานต่าง ๆ ร่วมกันแสดงความคิดเห็น และร่วมกันให้ข้อมูลที่คาดว่าจะเป็นประโยชน์ต่อการดำเนินโครงการ ซึ่งสรุปสาระสำคัญได้ดังนี้

1) คุณศุภกาญจน์ บุญจันทร์ จากสำนักบริหารและจัดการเลขหมายโทรคมนาคม กสทช. ได้ชี้แจงและให้ความคิดเห็นว่า ในอนาคตฉลาดโอนควรไปต่อยอดกับหน่วยงานอื่น ๆ ได้เพิ่มมากขึ้น ไม่ว่าจะเป็นธนาคารแห่งประเทศไทย หน่วยงานอื่นหรือค่ายโทรศัพท์มือถือ ที่อยู่ภายใต้การกำกับดูแลของ กสทช. ในเชิงของการบูรณาการ การร่วมมือในด้านธนาคาร และควรพัฒนาเป็นแอปพลิเคชันหรือมีระบบตรวจสอบอะไรเพิ่มเติม เพื่อเพิ่มศักยภาพของตัวระบบให้มีความทันสมัย และคุณศุภกาญจน์ บุญจันทร์ มีความคาดหวังว่าหากผู้ซื้อสามารถเช็คผู้ขายว่ามีตราประทับของฉลาดโอนเช่นเป็นใบรับรองมา น่าจะเป็นเรื่องที่ดี

2) คุณกนกศักดิ์ วิมลรัตน์ จากบริษัททรูมูฟเอช ยูนิเวอร์แซล คอมมิวนิเคชั่น จำกัด ได้แจ้งให้ที่ประชุมทราบมีความยินดีให้ความร่วมมือว่า ทางทรูมูฟเอชยินดีที่จะสนับสนุนให้เชื่อมต่อระบบ เพื่อตรวจสอบฐานข้อมูลจากหมายเลขโทรศัพท์ เพื่อให้สามารถยืนยันตัวตนได้ถูกต้องมากยิ่งขึ้น

3) พ.ต.ต. เมธา พจน์สันเทียะ ผู้ช่วยผู้อำนวยการ จากธนาคารแห่งประเทศไทย ได้ชี้แจงและให้ความคิดเห็นว่า ธปท. ได้มีการปรึกษาในการแก้ปัญหาเรื่องของการถูกฉ้อโกงออนไลน์เรื่องของบัญชีม้าจากหลาย ๆ หน่วยงาน ซึ่งไม่สามารถเดินเรื่องได้เร็วมาก เพราะเกี่ยวข้องกับหลายหน่วยงาน ซึ่งมีข้อกฎหมายที่แต่ละหน่วยงานดูแลอยู่ และคอนเซปที่ ธปท. เคยคิดไว้คือประชาสัมพันธ์เรื่องการหลอกลวง ซึ่งการประชาสัมพันธ์เป็นแบบวงกว้าง ไม่สามารถติดต่อไปที่เหยื่อได้โดยตรงเหมือนมิจฉาชีพได้ และขอให้พัฒนาต่อยอดเรื่อย ๆ และเก็บฐานข้อมูลได้เยอะ ๆ แต่ถ้าสามารถเชื่อมโยงกับระบบอื่นที่ตำรวจจัดทำได้ เช่นการแจ้งความออนไลน์ที่สำนักงานตำรวจแห่งชาติทำอยู่ ก็จะเป็นประโยชน์และเป็นความยั่งยืน

4) คุณวรุณ กาญจนภู รองเลขาธิการสมาคมธนาคารไทย จากสมาคมธนาคารไทย ได้ให้ข้อมูลและให้ความคิดเห็นว่า แบงค์ชาติมีการพูดถึงแอปพลิเคชัน ที่ให้สินเชื่อที่ได้รับอนุญาตจากแบงค์ชาติ แบงค์ชาติมีฐานข้อมูลว่า ผู้ที่ได้รับการอนุญาตมีใครบ้าง ซึ่งถ้าสามารถนำมาเชื่อมต่อกับฉลาดโอนได้ก็น่าจะเป็นประโยชน์กับฉลาดโอนมากยิ่งขึ้น

5) พ.ต.ต. ไกรทอง โพธิ์ตาด รองอัยการจังหวัดเชียงใหม่ สำนักงานอัยการสูงสุด ได้กล่าวชื่นชมเว็บไซต์ฉลาดโอนว่ามีประโยชน์ต่อประชาชนทั่วไปที่จะได้รับข้อมูลข่าวสารที่เป็นประโยชน์ในการที่จะตัดสินใจทำธุรกรรมทางออนไลน์ และได้ให้ข้อมูลและแสดงความคิดเห็นในเรื่องของการดำเนินคดีเกี่ยวกับการฉ้อโกงออนไลน์ จะมีปัญหาในเรื่องของการยืนยันตัวบุคคล ที่แสดงข้อความอันเป็นเท็จหรือนำเข้าข้อมูลอันเป็นเท็จเข้าสู่ระบบคอมพิวเตอร์ว่า บุคคลคนนั้นคือใคร ส่วนใหญ่แล้วพยานหลักฐานที่มีการรวบรวมโดยพนักงานสืบสวน จะเป็นหมายเลขบัญชีของผู้รับโอน สลิปโอนเงินของผู้เสียหายหรือหน้าโปรไฟล์ที่แคปหน้าจอออกมาที่ใช้เป็นพยานหลักฐาน และอยากให้มีการประสานงานในเรื่องของการยืนยันตัวบุคคลที่มีการนำข้อมูลอันเป็นเท็จเข้าสู่ระบบคอมพิวเตอร์ ว่าจะได้ข้อมูลของมิจฉาชีพออนไลน์ได้อย่างไรเพื่อเป็นพยานหลักฐานในการติดตามตัวผู้กระทำความผิดมาดำเนินคดี ในส่วนของบัญชีที่รับโอนเงินจากผู้เสียหายส่วนใหญ่แล้ว หมายเลขบัญชีที่รับการโอนเงินจะเป็นบัญชีม้าเป็นบัญชีของคนที่รับจ้างเปิดบัญชีน้อยที่จะเป็นบัญชีของผู้ที่กระทำความผิดเอง หากมีพยานหลักฐานในส่วนของบัญชีที่รับโอนเงินอย่างเดียวก็ยากที่จะดำเนินคดีกับมิจฉาชีพที่เป็นตัวการจริง ๆ ในการหลอกลวงผู้เสียหาย นอกจากจะมองในแง่มุมของการเป็นผู้ขายและมาหลอกขายของผู้ซื้ออยู่แล้ว แต่ก็มีบางเคสนอกจากจะเป็นผู้ขายที่หลอกขายให้กับผู้ซื้อแล้ว ยังมีผู้ซื้อที่หลอกผู้ขายด้วย เช่นมีการประกาศขายของผ่าน facebook marketplace มิจฉาชีพบางกลุ่มก็จะทำทีเป็นผู้ซื้อติดต่อไปยังผู้ขายสินค้าสนใจอยากซื้อสินค้าและขอให้ผู้ขายโอนเงินค่าธรรมเนียมในการจ่ายเงิน และอยากให้เพิ่มเติมในส่วนของวิธีการในการกระทำความผิดของมิจฉาชีพ

6) ดร.ณัฏฐ์ชยธร วัทธิกรสิริกุล ผู้ดำเนินรายการ มีประเด็นสอบถามผู้แทนจากหน่วยงานต่าง ๆ สามประเด็น ได้แก่

- ประเด็นที่หนึ่ง แบงค์ชาติมีขั้นตอนในการอายัดบัญชีอย่างไรและมีแนวทางอย่างไรเพื่อที่จะอายัดบัญชีให้รวดเร็วยิ่งขึ้นและเพื่อร่วมงานกับเว็บฉลาดโอน พ.ต.ต. เมธา พจน์สันเทียะ ได้ชี้แจงประเด็นเรื่องนี้ว่า ในเรื่องของบัญชีม้า ทาง ธปท. ได้มีการปรึกษากับ ปปง. กำลังดำเนินงานอยู่อย่างเรื่อย ๆ ซึ่งเกี่ยวข้องกับหลายหน่วยงาน หลายข้อกฎหมาย การแก้ปัญหาจึงจำเป็นต้องใช้เวลาและยังไม่สามารถตีกรอบปัญหาได้ทั้งหมด ส่วนของการอายัดบัญชี ในส่วนของธนาคารแห่งประเทศไทยไม่ได้มีข้อมูลลูกค้าของธนาคารพาณิชย์เก็บรักษาไว้และในเรื่องของการอายัดบัญชีที่เกี่ยวข้องกับมิจฉาชีพ ส่วนนี้ต้องใช้อำนาจตามกฎหมายต่าง ๆ ที่แต่ละหน่วยมีอำนาจ ซึ่งเป็นอำนาจเฉพาะตามกฎหมายที่กำหนดขึ้น

- ประเด็นที่สอง จากรูปแบบการรวบรวมหลักฐานที่ทีมงานฉลาดโอนดำเนินการมา เพียงพอต่อการดำเนินคดีในชั้นศาลหรือไม่ พ.ต.ต. ไกรทอง โพธิ์ตาด ได้ชี้แจงประเด็นเรื่องนี้ว่า จากพยานหลักฐานเท่าที่ปรากฏ จะติดขัดบุคคลคนที่นำข้อมูลอันเป็นเท็จเข้าสู่ระบบคอมพิวเตอร์ว่าเป็นใคร จะยากแก่การสืบสวนเอาตัวคนผิดมาดำเนินคดี ซึ่งหลักฐานในการดำเนินคดีของฉลาดโอนค่อนข้างน้อยมาก เพราะในการดำเนินคดีของประเทศไทยเป็นระบบกล่าวหา ในการที่จะดำเนินคดีกับมิจฉาชีพต้องมีการนำพยานหลักฐานเข้าสื่อ เพื่อให้ศาลเชื่อว่า ผู้ถูกกล่าวหามีส่วนร่วมในการฉ้อโกงว่านำข้อมูลอันเป็นเท็จเข้าสู่ระบบคอมพิวเตอร์ ซึ่งยากที่จะระบุว่าผู้รับโอนหรือเจ้าของบัญชี คือคนที่นำข้อมูลอันเป็นเท็จเข้าสู่ระบบคอมพิวเตอร์ ถ้าไม่สามารถที่จะพิสูจน์ได้ว่าบัญชีรับโอนคือคนที่นำข้อมูลอันเป็นเท็จเข้าสู่ระบบ

คอมพิวเตอร์ก็ยากที่จะลงโทษในข้อหาร่วมกันฉ้อโกงประชาชน แต่ถ้าบัญชีรับโอนรู้เห็นกับคนที่นำข้อมูลอันเป็นเท็จเข้าสู่ระบบคอมพิวเตอร์ ก็สามารถดำเนินคดีได้ หรือมีการเรียกบัญชีรับโอนเงินมาสอบสวน ถ้าบัญชีรับโอนเงินให้การสารภาพว่ามีส่วนร่วมในการกระทำความผิดโดยการแบ่งหน้าที่กันทำ ก็สามารถเป็นพยานหลักฐานที่จะลงโทษผู้กระทำความผิดได้

- ประเด็นที่สาม หลักฐานและเอกสารที่ฉลาดโอนรวบรวมมา สามารถนำไปพิจารณาในการประกอบคดีหรือการฟ้องร้องเหมาะสมหรือไม่ หรือต้องเพิ่มเติมอะไรหรือไม่ พ.ต.ต. ไกรทอง โพธิ์ตาด ได้ชี้แจงประเด็นเรื่องนี้และให้ความคิดเห็นว่า เป็นการรวบรวมพยานหลักฐานที่ดีมาก ในข้อมูลจะประกอบไปด้วยข้อมูลของผู้เสียหาย หลักฐานในการโอนเงิน บัญชีที่รับโอนเงิน และข้อความอันเป็นเท็จที่มิจฉาชีพได้หลอกลวงผู้เสียหาย ถือว่าเป็นข้อมูลที่สมบูรณ์ และอยากให้ผู้เสียหายลงลายมือชื่อ ในเอกสารที่เกี่ยวข้องทุกแผ่น หลังจาก พ.ต.ต. ไกรทอง โพธิ์ตาด กล่าวจบ ดร.เทอดพงษ์ แดงสี ได้ชี้แจงเสริมเรื่องการตรวจสอบการยืนยันตัวตนนอกจากจะตรวจสอบผู้ขายแล้ว เว็บไซต์ฉลาดโอนยังสามารถรองรับตรวจสอบผู้ซื้อได้ด้วย เว็บไซต์ฉลาดโอนจึงรองรับการยืนยันตัวตนทั้งผู้ซื้อและผู้ขาย

7) พ.ต.ท. บดินทร วิยาภรณ์ จากสำนักงานป้องกันและปรามการฟอกเงิน ปปง. ได้ให้ข้อมูลค่าใช้จ่ายในการยึด อายัด เอาทรัพย์สินมาคืนผู้เสียหาย ซึ่งนำไปเทียบเคียงกับคดีอาญาของ TDRI ซึ่งเป็นงานวิจัยที่ทำไว้เมื่อปี 2554 คือ 1 คดีต้องใช้ต้นทุนจำนวน 76,400 บาท ถ้ามาดูคดีฟอกเงินการดำเนินคดี 1 คดี คาดว่าไม่ต่ำกว่า 200,000 บาท ในการเป็นต้นทุนเรื่องของการไปขอเอกสารจากธนาคาร การดำเนินการต่าง ๆ อย่างอื่นด้วย จึงได้กล่าวชมโครงการนี้ว่าเป็นประโยชน์ในเชิงป้องกันอย่างแท้จริง และแสดงความเห็นว่า ปัญหาในตอนนี้คิดว่าจะนำเสนอโครงการนี้อย่างไรให้ประชาชนรับรู้ อาจจะเป็นการจัดในสถานศึกษาให้เด็กรุ่นใหม่รับรู้ตั้งแต่แรก ก็จะมีผลกับการไปบอกคนในครอบครัวว่าจะต้องดำเนินการและจัดการอย่างไร และเรื่องการจัดการกับบัญชีม้า ซึ่งมีการปรึกษาว่าจะจัดการกับบัญชีนี้อย่างไร อาจจะเป็นการเพิ่มความผิด ซึ่งอำนาจของพนักงานสอบสวนสามารถยึดทรัพย์สินได้ ตำรวจก็จะมีหนังสือไปขอความร่วมมือจากธนาคาร หากจะให้เป็นผลดีที่สุด ผู้โอนต้องระวังและเพิ่มความรู้ที่จะตรวจสอบว่าบุคคลที่จะโอนเงินไปมีความน่าเชื่อถือมากเพียงใด และอยากให้ต่อยอดโดยการมีการโฆษณาหรือการประชาสัมพันธ์โครงการนี้ไปถึงนักเรียน นักศึกษา ซึ่งเป็นกระบอกเสียงที่ดี เพราะคนยุคใหม่สามารถใช้อุปกรณ์เทคโนโลยีได้ดีที่สุด ดังนั้นจะต้องพิจารณาการให้ความรู้กับคนยุคใหม่ เพื่อจะได้ไปถ่ายทอดความรู้กับคนในครอบครัวต่อไป

8) คุณดวงใจ กุศลฉันท์ ผู้อำนวยการฝ่ายการกำกับการปฏิบัติงานของธนาคารออมสิน ได้แสดงความคิดเห็นเรื่อง การประชาสัมพันธ์อย่างไรให้เข้าถึงประชาชน ซึ่งจะทำให้ฉลาดโอนเป็นประโยชน์มากขึ้น

9) คุณจุฑาธัช คูเกษมรัตน์ จากสถาบันเพื่อการยุติธรรมแห่งประเทศไทย ได้ชี้แจงและให้ความคิดเห็นว่าสถาบันเพื่อการยุติธรรมแห่งประเทศไทยไม่ได้มีบทบาทหน้าที่โดยตรง ที่ดูในเรื่องของการฉ้อโกงออนไลน์ หน้าที่ของสถาบันเป็นในเรื่องของการเสริมกระบวนการยุติธรรม โดยงานหลักจะดูในเรื่องของมาตรฐานในเชิงนวัตกรรมโดยการใช้เทคโนโลยีที่จะพัฒนาในเรื่องของตัวกระบวนการยุติธรรม ในส่วนของเรื่องเช็คตัวตนผู้ขายเป็นฟังก์ชันที่มีความสำคัญเช่นกัน หากเมื่อดูจากสถิติการใช้งานจะมีเพียงแค่ร้อยละ 2.77 หากทางฉลาดโอนสามารถที่จะสร้างแรงจูงใจให้ผู้ขายมายืนยันตัวตนและถ้าผู้ขายมีใบอนุญาตอาจจะทำให้ได้รับผลประโยชน์บางอย่างหรือสามารถทำให้ผู้ขายและผู้ซื้อมีความเชื่อมั่นมาใช้งานมากขึ้น

กว่าเดิม หากสามารถสร้างเครือข่ายทำให้ผู้ขายสินค้าออนไลน์มาใช้หรืออยู่ในวงจรมากขึ้นกว่าเดิม ก็จะทำให้ผู้ซื้อมีความมั่นใจมากขึ้น

10) คุณรังสรรค์ วิริยะวารี Project Director ผู้แทน Best Enterprise Co., Ltd. ผู้พัฒนาระบบของธนาคาร (และเคยเป็นผู้บริหารในธนาคารแห่งหนึ่ง) ได้แสดงความคิดเห็นและให้ข้อมูลว่า ธนาคารจะมีระบบที่เซ็ตขึ้นมาเรียกว่า ระบบ Ford monitoring real time ซึ่งก็จะเซ็ตเงื่อนไขเข้าไป บัญชีเหล่านี้ก็จะมีข้อสังเกตคือ จะเปิดบัญชีแค่ 100 500 หรือไม่เกิน 1000 บาท แต่หลังจะนั้น 1 เดือน จะมีเงินโอนเข้ามาหลักแสน หลักล้าน ถ้าจากการ KYC ในการเปิดบัญชี จะไม่มีความเป็นไปได้ที่จะมีเงินโอนเข้ามาหลักแสน หลักล้าน ภายในระยะเวลาไม่เกิน 3 เดือน ซึ่งจะเซ็ตระบบขึ้นมาว่าบัญชีไหนที่เปิดมาใหม่และมีเงินโอนมาจำนวนมาก ๆ ก็จะให้เตือนเข้ามาในระบบของ Ford monitoring real time เพื่อที่จะโทรไปหาบุคคลที่จะโอนเข้าบัญชีนั้นก่อนว่า ได้โอนเข้าบัญชีนี้จริงหรือไม่ และเว็บไซต์ฉลาดโอนเป็นสิ่งที่ดี ถ้าได้ฐานข้อมูลที่มากขึ้น เพราะฐานข้อมูลฉลาดโอนส่วนมากได้จากประชาชนแจ้งมา แต่ถ้าสามารถที่จะนำเข้าข้อมูลจากแบล็กลิสต์และวอทช์ลิสต์ของธนาคารแต่ละธนาคารหรือของ ปปง. มาเชื่อมกับฐานข้อมูลของฉลาดโอนได้ จะทำให้ได้ฐานข้อมูลที่มากขึ้น เป็นประโยชน์มากขึ้น และสามารถป้องกันได้มากขึ้น ถ้าอนาคตระบบนี้สามารถพัฒนาเป็นระบบ เรียลไทม์ โดยเอาฐานข้อมูลของแบล็กลิสต์และวอทช์ลิสต์ของธนาคารหรือ ปปง. ทำให้ระบบมา machine learning AI ก็จะง่ายขึ้น เราจะศึกษาพฤติกรรมของการฉ้อโกงได้แบบทันที และในช่วงท้ายท่านได้เสริมเรื่อง การออกกฎระเบียบให้เหมือนกับ visa mastercard ซึ่งธนาคารจะต้องบังคับให้ร้านค้า Verify by visa มีข้อดีคือ ถ้ามีลูกค้าไปใช้แล้วถูกทุจริต สามารถที่จะเคลมร้านค้านี้กับธนาคารที่เป็นเจ้าของร้านค้านี้ได้เต็มจำนวน จะช่วยลดปัญหาความเดือดร้อนของประชาชนในภาพกว้างได้

11) พ.ต.ท.ณัทกฤช พรหมจันทร์ จากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ได้ชี้แจงเสริม คุณรังสรรค์ วิริยะวารี ว่า ส่วนที่เกี่ยวข้องกับ สกมช. ในการแจ้งเตือนภัยไซเบอร์ในปัจจุบัน มีเซิร์ตชาติ จะมีกระบวนการในการแจ้งเตือนไปยังหน่วยงาน โครงสร้างพื้นฐานสำคัญสารสนเทศ ในส่วนของเว็บฉลาดโอนที่จะใช้ประโยชน์จากช่องทางนี้ คือ ให้เว็บฉลาดโอนสรุปข้อมูลที่เป็นข้อมูลดิบ หรือข้อมูลที่เป็นประโยชน์ที่อยู่ในเว็บตอนนี้ทำเป็นข้อมูลที่มีการกรอง ทำให้ข้อมูลต่าง ๆ เข้าใจได้ง่ายขึ้น เช่นการจัดลำดับ เรียบเรียงว่าเรื่องใดเป็นเรื่องสำคัญหรือข้อมูลใดที่เปิดเผยแล้วไม่เสียหายต่อหน่วยงานนั้น ตรงนี้สามารถนำเข้าช่องทางเซิร์ตได้ ถ้ารวมกับข้อมูลที่เป็นประโยชน์กับเว็บฉลาดโอนเข้าไปก็จะทำให้สื่อสารไปถึงองค์กรต่าง ๆ ที่เป็นองค์กรขนาดใหญ่ที่ดูแลเรื่องโครงสร้างพื้นฐานสำคัญสารสนเทศได้และจะนำไปสู่พนักงานได้ ก็จะเป็นการเสริมช่องทางการประชาสัมพันธ์เว็บฉลาดโอนได้อีกช่องทางหนึ่ง

12) ดร.เทอดพงษ์ แดงสี หัวหน้าโครงการฯ มีประเด็นสอบถามสองประเด็น ได้แก่

- ประเด็นที่หนึ่ง ให้ สกมช. ช่วยประชาสัมพันธ์หรือผลักดันเว็บไซต์ฉลาดโอน เพื่อให้ประชาชนรับรู้มากขึ้นได้หรือไม่ พ.ต.ท.ณัทกฤช พรหมจันทร์ ได้ชี้แจงประเด็นเรื่องนี้ว่า สกมช. มีความยินดีประชาสัมพันธ์เพื่อเป็นประโยชน์ส่วนรวม

- ประเด็นที่สอง ตัวหนังสือควรใหญ่ขึ้นกว่านี้หรือไม่ เพื่อให้ศาลมองเห็นชัดขึ้น พ.ต.ต. ไกรทอง โพธิ์ตาด ได้ชี้แจงประเด็นเรื่องนี้ว่า ตัวหนังสือสามารถอ่านได้ ไม่มีปัญหาเรื่องของการอ่านข้อความ

13) ดร.ธริศร์ ทิมทอง ที่ปรึกษาโครงการ ได้ให้ข้อมูลเรื่องการป้องกันการเปิดบัญชีม้ากับธนาคารเอกชน 2 แห่ง คือธนาคารแลนด์ แอนด์ เฮ้าส์ จำกัด (มหาชน) และธนาคารกสิกรไทย จำกัด (มหาชน) หลักการคือ ชื่อคนที่เป็นบัญชีม้าที่แจ้งมา จะต้องมีการยืนยันตัวตนโดยบัตรประชาชน มีเลขเลเซอร์โค้ด

และนำเลเซอร์โค้ดไปเช็ดกับ กรมการปกครอง (DOPA) ก็สามารถส่งข้อมูลบัญชีที่ถูกแจ้งไปให้ทางธนาคาร และธนาคารจะใช้เกณฑ์ป้องกันไม่ให้เปิดบัญชีออนไลน์ แต่จะให้ไปที่เคาน์เตอร์ธนาคารเพื่อไปแสดงตนต่อเจ้าหน้าที่ธนาคาร จึงจะเปิดบัญชีได้ และมีประเด็นสอบถามหลายประเด็น

- ประเด็นที่หนึ่ง ธนาคารอื่นหรือธนาคารแห่งประเทศไทยมีความคิดเห็นอย่างไรในเรื่องนี้และมีความเป็นไปได้หรือไม่ พ.ต.ต. เมธา พจน์สันเทียะ ได้ชี้แจงประเด็นเรื่องนี้ว่า ประเด็นเรื่องของบัญชีม้าไม่มีความผิดในการรับจ้างเปิดบัญชีเฉพาะ จนกว่าบัญชีม้านั้นจะถูกนำไปใช้ในการทุจริตหรือว่าไปเกี่ยวพันกับคดีอาญาอื่น ซึ่ง ปปง. อยู่ในระหว่างการผลักดันในส่วนของการที่จะไปเขียนกฎหมายเฉพาะ เรื่องรายการเปิดบัญชีแทนหรือการรวบรวมบัญชีเพื่อนำไปขายเป็นความผิดเฉพาะ ทาง ธปท. ได้มีการปรึกษากับสมาคมธนาคาร ปปง. และหลาย ๆ หน่วยงาน ว่าจะหาช่องทางอย่างไรในการกำจัดไม่ให้มีการเปิดบัญชีม้าเรื่อย ๆ ซึ่งมีแนวคิดในเรื่องของการจำกัดการเปิดบัญชี การทำ KYC ซึ่งอยู่ระหว่างการปรึกษา แต่ก็มีแนวทางเบื้องต้นเพื่อที่จะไม่ให้ม้าที่รับจ้างเปิดบัญชีไปเปิดบัญชีกับหลาย ๆ ธนาคาร ซึ่งข้อมูลของม้าที่รับจ้างเปิดบัญชีที่อยู่ในแต่ละธนาคาร ธนาคารพาณิชย์อาจจะไม่ได้มีการแชร์ข้อมูลกัน เพราะติดในเรื่องของ พรบ. ธุรกิจสถาบันการเงินเรื่องข้อมูลส่วนบุคคล ซึ่งข้อมูลในแต่ละกลุ่มธนาคารจะเป็นของธนาคารนั้นโดยเฉพาะ จึงพยายามหาวิธีที่จะแชร์ข้อมูลให้ได้โดยที่ ไม่ขัดต่อหลักกฎหมาย

- ประเด็นที่สอง อยากให้ฉลาดโอนทดลอง ทดสอบอะไรที่ทำให้ข้อจำกัดขั้นตอนนั้น ๆ ของที่รับผิดชอบอยู่ให้ลดลง เช่นบอกให้ผู้เสียหายไปที่ ปปง. เพื่อไปยื่นคำร้องได้เลยแต่ก็ต้องเป็นไปตามกระบวนการ ถ้าจะทำระดับแค่ยืนยันตัวตน ถ่ายรูปบัตรประชาชน สแกนใบหน้าและเปรียบเทียบ KYC เพียงเท่านี้แล้วส่งไปที่ ปปง. ได้หรือไม่ พ.ต.ท. บดินทร วิยาภรณ์ ได้ชี้แจงประเด็นเรื่องนี้ว่า ทาง ปปง. ไม่เคยเก็บข้อมูลเรื่องสแกนใบหน้า ถ้าจะต้องให้ทุกคนเข้ามาติดต่อจะต้องมีช่องทางอื่น เพราะเครื่องมือไม่เพียงพอ ซึ่งใช้การแสดงตัวตนผ่านออนไลน์ก็ได้ แต่ก็ยังมีข้อปัญหาเรื่องการจะคุ้มครองสิทธิของผู้เสียหายที่เกิดขึ้นแล้วและชัดเจนว่าเสียหายจริง ปปง. อำนวยความสะดวกด้วยการให้ส่งเอกสารและลงทะเบียนผ่านอินเทอร์เน็ตมาสุดท้ายก็ยังมีปัญหา เพราะประชาชนไม่ทราบข้อมูลว่าจะต้องใช้อะไรบ้าง ส่วนนี้คาดว่าจะต้องมีการประชาสัมพันธ์ ในช่วงท้ายท่านได้เสริมว่า โครงการนี้ดีที่สุดคือการป้องกันและให้ความรู้ การแสดงตนจึงเป็นเรื่องที่ดี แต่ควรแสดงตัวทั้งสองฝ่าย ถ้าคนโอนทราบว่าบัญชีที่จะโอนไป เจ้าของบัญชีประกอบอาชีพอะไร มีรายได้เท่าไหร่ต่อปี ปีที่แล้วเสียภาษีเท่าไหร่ ในการแสดงฐานข้อมูลนี้เป็นข้อมูลเบื้องต้นที่คนจะร่วมลงทุนหรือผู้โอนควรทราบก่อน ก็จะทำให้มีความระมัดระวังมากขึ้น

- ประเด็นที่สาม คนติดแบล็กลิสต์ของ ปปง. ปปง.ก็จะส่งรายชื่อให้กับธนาคารเอกชนที่เกี่ยวข้องบุคคนนี้ก็จะเปิดบัญชีไม่ได้เลยถูกต้องหรือไม่ และวาระที่จะปลดออกจากแบล็กลิสต์มีเกณฑ์หรือไม่ ถ้าไม่สามารถเปิดบัญชีที่ไหนได้เลยตลอดชีวิต พ.ต.ท. บดินทร วิยาภรณ์ ได้ชี้แจงประเด็นเรื่องนี้ว่า ปปง. ไม่สามารถกำหนดแบล็กลิสต์ได้ อย่างน้อยต้องผ่านองค์กรนานาชาติและการยื่นคำร้องขอต่อศาลก่อน ซึ่งต้องป้องกันคนเพื่อไม่ให้ตกเป็นเหยื่อด้วยการให้ความรู้ก่อนโอนเงินเข้าบัญชีของมิจฉาชีพ จะต้องมีประวัติเช็คคนที่เป็นมิจฉาชีพว่าทำอะไรมาก่อนบ้าง หรือมีการเฝ้าระวังก่อน จะช่วยตัดวงจรของมิจฉาชีพได้มากขึ้น และเรื่องการปลดแบล็กลิสต์ ต้องมีหนังสือสอบถามธนาคารว่าที่ไม่ให้ดำเนินการมีจากหน่วยงานใดแจ้งมาและจึงไปสอบถามหน่วยงานนั้น เพราะจะเป็นการตัดช่องทางในการประกอบอาชีพในอนาคต

- ประเด็นที่สี่ เรื่องการอายัดบัญชี จะมีระเบียบให้ทราบว่าผู้นำเข้าข้อมูลมีความสัมพันธ์กับเจ้าของบัญชีหรือไม่ และถ้าคนที่มาแจ้งทั้งหมดไม่ใช่บุคคลที่จะอยากดำเนินคดี แต่การแจ้งอายัดบัญชีนั้นทางธนาคารมีเกณฑ์ที่จะให้ไปแจ้งเจ้าหน้าที่ตำรวจเพื่อดำเนินคดี จะเป็นไปได้หรือไม่ถ้าฉลาดโอนส่ง

ธนาคารเจ้าของบัญชีให้และให้ ปปง. ใช้หลักเกณฑ์ใดก็ได้ในการพิจารณาและจะดำเนินการอย่างไร ในเรื่องของการอายัดบัญชีโดยข้ามขั้นตอนเดิม พ.ต.ต. เมธา พจน์สันเทียะ ได้ชี้แจงเสริมประเด็นเรื่องนี้ว่า ปัจจุบัน ธปท. ได้ออกเกณฑ์เรื่องการ KYM ว่าในการรับชำระเงินแทนหรือในการบริการรับชำระที่มาเชื่อมต่อกับผู้ประกอบธุรกิจที่ได้รับอนุญาตจาก ธปท. จะต้องทำ KYM เพื่อจะพิสูจน์ตัวตนของร้านค้าว่ามีอยู่จริง คาดว่าในอนาคตจะช่วยได้ในระดับนึง

- ประเด็นที่ห้า IP address ของผู้นำข้อมูลอันเป็นเท็จเข้าสู่ระบบคอมพิวเตอร์ ซึ่ง IP address ของผู้ถูกกล่าวหาสามารถหามาได้ แต่ไม่สามารถพิสูจน์ได้ว่าคือใคร ในมุมมองของอัยการสามารถใช้ข้อมูลนี้ได้หรือไม่ พ.ต.ต. ไกรทอง โพธิ์ตาด ได้ชี้แจงประเด็นเรื่องนี้ว่า ถ้าได้เฉพาะ IP address จะยังไม่เพียงพอที่จะยืนยันตัวบุคคลที่กระทำความผิด จึงอยากให้หน่วยงานที่เกี่ยวข้องลองพิจารณาว่าจะทำอย่างไร ในการหาพยานหลักฐานเพื่อยืนยันตัวบุคคล

- ประเด็นที่หก เรื่องนิติของปราบปราม ยังติดเรื่องการขอหลักฐาน ติดเรื่องการขอข้อมูลจากธนาคาร ซึ่งสิ่งที่ฉลาดโอนทำได้คือ เรื่องของการป้องกันที่พยายามให้ผู้แจ้งยืนยันตัวตนเพื่อประชาชนคนอื่นได้ไม่ถูกหลอก แต่ในเรื่องของปราบปราม ตำรวจจะต้องขอหลักฐานจาก Operator เพื่อที่จะขอตำแหน่ง IP address ซึ่งใช้ระยะเวลานาน ทำให้บัญชีถูกปิดไปหรือเปลี่ยนไป แต่มิจฉาชีพยังอยู่ พ.ต.ต. เมธา พจน์สันเทียะ ได้ชี้แจงเสริมประเด็นว่า ทาง ธปท. พยายามช่วยแจ้งปิดเว็บไซต์ที่เกี่ยวกับการซื้อ ขายบัญชีและกลุ่มเฟสบุ๊กที่เป็นกลุ่มในการแลกเปลี่ยน ซื้อ ขาย บัญชี ซึ่งทาง ธปท. เคยไปปรึกษากับกระทรวงดิจิตอลเพื่อเศรษฐกิจและสังคมว่าจะทำอย่างไรในการปิดกลุ่มต่าง ๆ นี้ แต่ก็ติดปัญหาในเรื่องข้อกฎหมายและเงื่อนไขตามเกณฑ์ของ Social Media ซึ่งทำได้แค่การ report นอกจากนี้ในช่วงท้าย ดร.ธริศร์ ทิมทอง ได้เสริมว่า เครือข่ายผู้เสียหายได้แจ้งมาให้ตั้งกลุ่มเพื่อช่วยกัน report และจะลองนำไปทดลองว่าเมื่อ report กลุ่มปิดจริงหรือไม่

จากการประชุมเสวนาดังกล่าว ที่ประชุมมีมติร่วมกันคือ รับทราบและพร้อมที่จะให้ความร่วมมือและสนับสนุนโครงการนี้

5.4 การประชุมแถลงผล

ทางผู้วิจัย ได้จัดงานประชุมแถลงผลการดำเนินโครงการ“การออกแบบและพัฒนาระบบต้นแบบเพื่อสนับสนุนงานป้องกันและปราบปรามมิจฉาชีพออนไลน์ : เว็บไซต์ฉลาดโอน” ในวันพฤหัสบดีที่ 17 มีนาคม 2565 ผ่านระบบออนไลน์ โดยมีรายละเอียดของงาน ดังนี้

5.4.1 รายชื่อผู้เข้าร่วมงานประชุมแถลงผล

5.4.1.1 รายชื่อวิทยากรบรรยาย

1) พ.ต.อ.ดร.ปราโมทย์ จันทร์บุญแก้ว ผู้กำกับการฝ่ายอำนวยการ ๕ กองบังคับการอำนวยการ กองบัญชาการตำรวจนครบาล
2) พ.ต.ท.ธวัชชัย เกริกสกุลทรัพย์ สารวัตรสอบสวน สถานีตำรวจนครบาลบางโพ
3) ร.ต.ท.หญิง ปุญชรัสมี ขำฟัก รองสารวัตรสอบสวน สถานีตำรวจนครบาลบางโพ

5.4.1.2 รายชื่อผู้เข้าร่วมรับฟังการบรรยาย

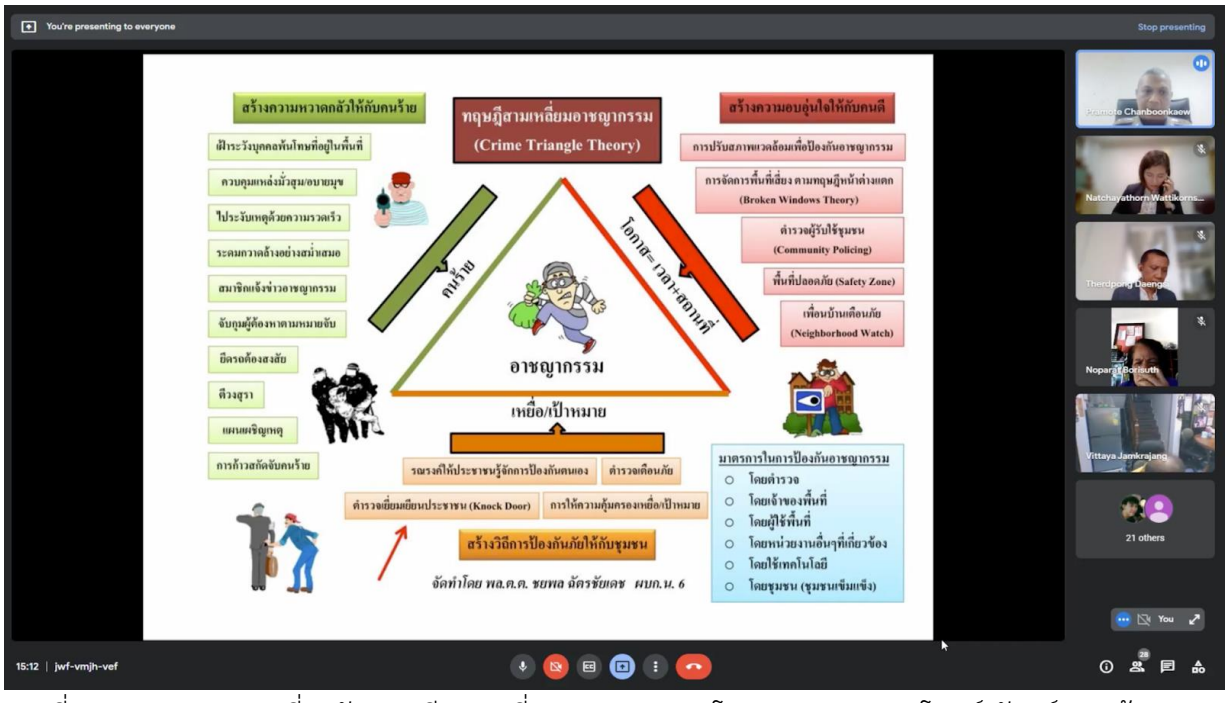
1) คุณวิทยา แจ่มกระจ่าง ประธานสมาพันธ์ชมรมคุ้มครองผู้บริโภค
2) คุณกนกภรณ์ จงเจริญรุ่งเรือง นักประชาสัมพันธ์ชุมชน เขตวังทองหลาง กทม.
3) คุณกนกภรณ์ จงเจริญรุ่งเรือง สมาพันธ์ชมรมคุ้มครองผู้บริโภค เขตวังทองหลาง กทม.
4) คุณปรางค์ทิพย์ วรวัฒนานุกูล สมาพันธ์ชมรมคุ้มครองผู้บริโภค เขตบึงกุ่ม กทม.
5) คุณนพรัตน์บริสุทธิ์ สมาพันธ์ชมรมคุ้มครองผู้บริโภค เขตมีนบุรี กทม.
6) คุณกานต์ วรวัฒนานุกูล สมาพันธ์ชมรมคุ้มครองผู้บริโภค กทม.
7) คุณสุดศิริ บุนนาค ทากาโน สมาพันธ์ชมรมคุ้มครองผู้บริโภค กทม.
8) คุณศิริวัฒนา จารุบรรยงค์ สมาพันธ์ชมรมคุ้มครองผู้บริโภค กทม.
9) คุณภคพัชร ปานแก้ว สมาพันธ์ชมรมคุ้มครองผู้บริโภค
10) คุณไพวรรณ งามไมตรี สมาพันธ์ชมรมคุ้มครองผู้บริโภค
11) คุณศิริวัฒนา จารุบัญยง สมาพันธ์ชมรมคุ้มครองผู้บริโภค
12) คุณจงรักษ์ พูลเกิด สมาพันธ์ชมรมคุ้มครองผู้บริโภค
13) คุณดลฤดี วงศ์สุขวิวัฒนา สมาพันธ์ชมรมคุ้มครองผู้บริโภค
14) คุณยุทธิยงค์ แสวงทอง สมาพันธ์ชมรมคุ้มครองผู้บริโภค
15) คุณวรพล กาญจนกันติ สมาพันธ์ชมรมคุ้มครองผู้บริโภค
16) คุณสุรสิทธิ์ สุขจิตร สมาพันธ์ชมรมคุ้มครองผู้บริโภค
17) คุณยอดธง รุนรุจิ สมาพันธ์ชมรมคุ้มครองผู้บริโภค
18) คุณมงคล ศิริวงศ์ สมาพันธ์ชมรมคุ้มครองผู้บริโภค
19) คุณปลื้มจิตต์ นราภิมย์ขวัญ สมาพันธ์ชมรมคุ้มครองผู้บริโภค
20) คุณนิธิกุล เตชะ สมาพันธ์ชมรมคุ้มครองผู้บริโภค
21) คุณทิมพ์มณี รมย์พันธ์ สมาพันธ์ชมรมคุ้มครองผู้บริโภค
22) คุณยศยง แก้วทิพย์ สมาพันธ์ชมรมคุ้มครองผู้บริโภค
23) คุณราชวิทย์ ยุติวงษ์ สมาพันธ์ชมรมคุ้มครองผู้บริโภค
24) คุณอำนาจ หัสถีธรรม สมาพันธ์ชมรมคุ้มครองผู้บริโภค
25) คุณพรศิริ โพธิ์สุวรรณ สมาพันธ์ชมรมคุ้มครองผู้บริโภค
26) คุณปรกธน แสงนิล สมาพันธ์ชมรมคุ้มครองผู้บริโภค

27) คุณจงกลณี ปานแก้ว สมาพันธ์ชมรมคุ้มครองผู้บริโภค
28) คุณกฤชวรรณ ปานแก้ว สมาพันธ์ชมรมคุ้มครองผู้บริโภค
29) คุณธนพร บุญชู สมาพันธ์ชมรมคุ้มครองผู้บริโภค
30) คุณวงศ์วัฒน์ คำสร้อย สมาพันธ์ชมรมคุ้มครองผู้บริโภค
31) คุณธันยาทิพย์ อัยสานนท์ สมาพันธ์ชมรมคุ้มครองผู้บริโภค
32) คุณอดิเรก สังข์นุช สมาพันธ์ชมรมคุ้มครองผู้บริโภค

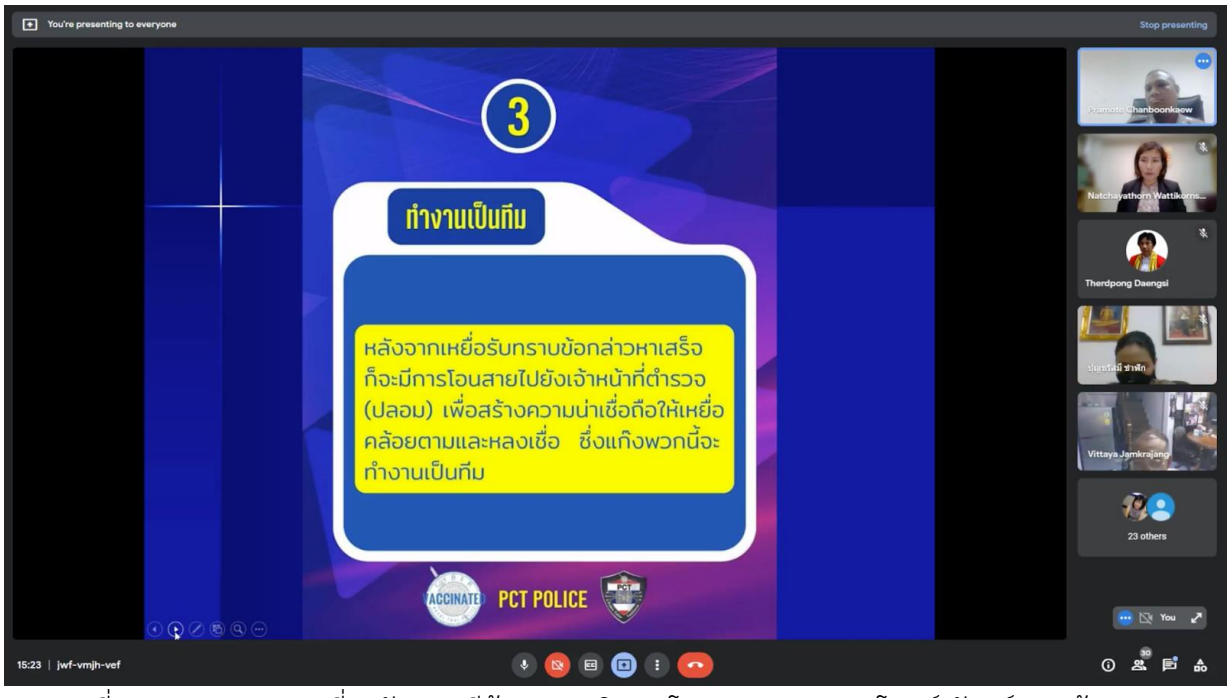
5.4.1.3 รายชื่อตัวแทนคณะผู้วิจัย

1) ดร.เทอดพงษ์ แดงสี หัวหน้าโครงการ มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร

5.4.2 ภาพบรรยากาศการประชุมแถลงผล

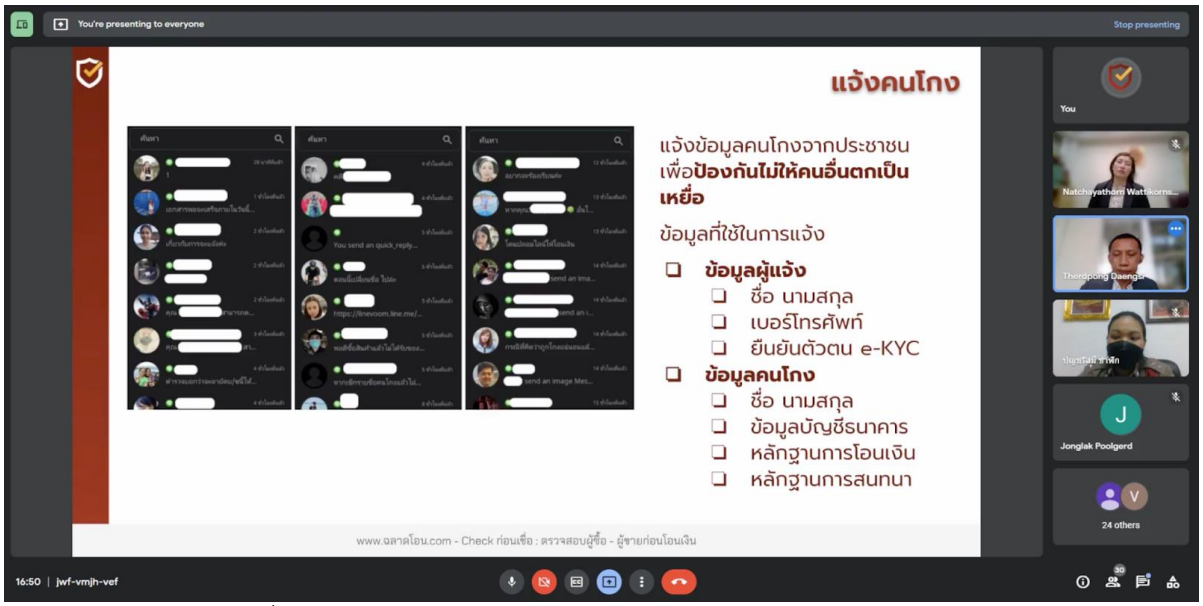


รูปที่ 5-12 การบรรยายเกี่ยวกับทฤษฎีสามเหลี่ยมอาชญากรรม โดย พ.ต.อ.ดร.ปราโมทย์ จันทร์บุญแก้ว



รูปที่ 5-13 การบรรยายเกี่ยวกับทฤษฎีด้านอาชญวิทยา โดย พ.ต.อ.ดร.ปราโมทย์ จันทร์บุญแก้ว

รูปที่ 5-14 การบรรยายกรณีตัวอย่างคดีเกี่ยวกับมิจฉาชีพออนไลน์ที่มีการติดตามจับกุม



รูปที่ 5-15 การนำเสนอระบบฉลาดโอน โดย ดร.เทอดพงษ์ แดงสี

5.4.3 บันทึกการประชุมแถลงผล

เวลา 15:00 น. ดร.ณัฐวรพล รัชสิริวัชรบุล อธิการบดี มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร ประธานในพิธี ได้กล่าวเปิดงาน โดยได้กล่าวถึงที่มาของโครงการและสภาพปัญหาภัยคุกคามจากผู้ไม่ประสงค์ดีที่อาศัยช่องโหว่ ทั้งจากคน ระบบ และกระบวนการ ตลอดจนข้อกฎหมายที่ยังมีจุดอ่อน และข้อจำกัดต่างๆ ที่กลายเป็นช่องทางให้มิจฉาชีพแอบแฝงเข้ามาหาผลประโยชน์ด้วยกลโกงรูปแบบต่าง ๆ จึงได้มีโครงการนี้ขึ้นมา เพื่อเป็นแนวทางในการป้องกันและปราบปรามมิจฉาชีพออนไลน์ รวมทั้งสนับสนุนการดำเนินงานของเจ้าหน้าที่ตำรวจในการทำสำนวนเพื่อดำเนินคดี และหวังว่าในอนาคตจะได้มีส่วนในการพัฒนาและได้รับการสนับสนุนจากกองทุน กทปส. เพื่อสร้างความยั่งยืนในการป้องกันและปราบปรามต่อไปในอนาคต

จากนั้นผู้ดำเนินรายการได้เชิญให้พ.ต.อ.ดร.ปราโมทย์ จันทร์บุญแก้ว ผู้กำกับการฝ่ายอำนวยการ ๕ กองบังคับการอำนวยการกองบัญชาการตำรวจนครบาล โดยได้บรรยายเกี่ยวกับด้านทฤษฎีอาชญวิทยาที่เกี่ยวข้องกับมิจฉาชีพออนไลน์ ซึ่งสรุปสาระสำคัญได้ดังนี้

การเกิดเหตุอาชญากรรม ประกอบไปด้วยองค์ประกอบ 3 องค์ประกอบ ได้แก่ ผู้เสียหาย ผู้กระทำความผิด และโอกาส ซึ่งโอกาสในการเกิดเหตุอาชญากรรมนี้มีโอกาสในการเกิดเหตุสูง แม้ว่าจะมีทฤษฎีป้องกันการเกิดเหตุอาชญากรรมก็ตาม ทั้งนี้จึงได้มีการดำเนินโครงการที่อาศัยความร่วมมือจากประชาชนในการป้องกันและปราบปราม และทฤษฎีการป้องกันและปราบอาชญากรรมจากสภาพแวดล้อม ซึ่งไม่ครอบคลุมถึงปัญหาอาชญากรรมออนไลน์ จึงได้มีการพัฒนาฉลาดโอนขึ้น เพื่อเป็นแนวทางในการป้องกันและปราบปรามมิจฉาชีพออนไลน์ อันเป็นปัญหาสำคัญในปัจจุบัน และได้มีการกล่าวถึงรูปแบบการฉ้อโกงออนไลน์ที่เกิดขึ้น ตลอดจนแนวทางการป้องกันไม่ให้ตนเองตกเป็นเหยื่อ และระงับโอกาสในการเกิดเหตุอาชญากรรม

เมื่อเสร็จสิ้นการบรรยายจาก พ.ต.อ.ดร.ปราโมทย์ จันทร์บุญแก้ว ผู้กำกับการฝ่ายอำนวยการ ๕ กองบังคับการอำนวยการกองบัญชาการตำรวจนครบาล ผู้ดำเนินรายการได้เชิญให้พ.ต.ท.ธวัชชัย เกริกสกุลทรัพย์ สารวัตรสอบสวน สถานีตำรวจนครบาลบางโพ และร.ต.ท.หญิง ปุญชรัสมี ขำฟัก รองสารวัตร

สอบสวน สถานีตำรวจนครบาลบางโพ บรรยายเกี่ยวกับตัวอย่างคดีที่เกี่ยวข้องกับมิจฉาชีพออนไลน์ที่มีการติดตามจับกุมได้ ซึ่งสรุปสาระสำคัญได้ดังนี้

ยกตัวอย่างคดีเกี่ยวกับมิจฉาชีพออนไลน์ที่มีการจับกุมได้ สรุปพฤติการณ์ของคนร้ายในการก่อเหตุอาชญากรรมฉ้อโกงออนไลน์ที่นิยมในปัจจุบันได้ ดังนี้

1. คอลเซ็นเตอร์ล่อลวงให้โอนเงินไปยังบริษัทขนส่ง โดยอ้างชื่อบุคคลที่ไม่มีตัวตน ซึ่งคนร้ายจะแอบอ้างว่าตนเป็นบริษัทขนส่ง หรือแอบอ้างตนเองเป็นเจ้าหน้าที่ตำรวจ
2. หลอกขายสินค้าออนไลน์ อาศัยช่องโอกาสที่บัญชีเฟสบุ๊กเพื่อขายสินค้านี้มีผู้ติดตามจำนวนมาก และหากมีผู้เสียหายหลงเชื่อโอนเงินเพื่อชำระค่าสินค้า คนร้ายรายนี้จะส่งสินค้าปลอมหรือสินค้าอื่น ๆ ไปให้ หรือเรียกว่า สินค้าไม่ตรงปก
3. รับฝากซื้อสินค้าแสตนอะคริลิค แจ้งว่าการซื้อสินค้านี้จะใช้เวลาในการรอสินค้าเป็นเวลานานตั้งแต่ 1 เดือนขึ้นไป ต่อมาได้มีการสารภาพว่าที่ผ่านมาได้นำเงินค่าสินค้าไปใช้จ่ายส่วนตัว และใช้ข้อความประวิงเวลาไม่ให้ผู้เสียหายไปแจ้งความ เพื่อประวิงเวลาให้คดีหมดอายุความเสียก่อน

จากตัวอย่างคดี สามารถสรุปพฤติการณ์คนร้ายได้ว่า ในกรณีที่เกี่ยวกับการซื้อขายสินค้าออนไลน์ คนร้ายจะเลือกใช้แพลตฟอร์มออนไลน์ที่มีเซิร์ฟเวอร์อยู่ต่างประเทศ เพื่อป้องกันการติดตามตำแหน่งหรือติดตามตัวคนร้ายเอง ทั้งนี้ยังรวมไปถึงการระแวดระวังร้านค้าหรือผู้ขายที่มีจำนวนผู้ติดตามจำนวนมาก เพราะถึงแม้จะมีผู้ติดตามจำนวนมาก แต่ไม่ได้หมายความว่าจะปลอดภัยเสมอไป การทำธุรกรรมซื้อขายสินค้าออนไลน์ควรตรวจสอบแบลคลิสต์ก่อน เพื่อเป็นการป้องกันการเกิดเหตุอาชญากรรม

เมื่อเสร็จสิ้นการบรรยายจากพ.ต.ท.ธวัชชัย เกริกสกุลทรัพย์ สารวัตรสอบสวน สถานีตำรวจนครบาลบางโพ และร.ต.ท.หญิง ปุญชรัสมี ขำฟัก รองสารวัตรสอบสวน สถานีตำรวจนครบาลบางโพ ผู้ดำเนินรายการได้เชิญดร.เทอดพงษ์ แดงสี หัวหน้าโครงการ มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร บรรยายสรุปผลการดำเนินงานโครงการ การใช้งานเว็บไซต์ฉลาดโอน รวมทั้งสถิติผู้เข้าใช้งานระบบฉลาดโอน โดยได้กล่าวถึงที่มาของโครงการและสภาพปัญหาการฉ้อโกงในการธุรกรรมออนไลน์ ฟังก์ชันหลักของฉลาดโอน ทั้ง 4 ฟังก์ชัน ได้แก่

เช็กก่อนโอน หรือการตรวจสอบข้อมูลผู้กระทำความผิดที่ได้รับข้อมูลจากแหล่งข้อมูลทั้งภาครัฐและภาคเอกชน รวมถึงการแจ้งข้อมูลคนโกงจากประชาชนที่ได้ยืนยันตัวตนกับฉลาดโอน

แจ้งคนโกง หรือการให้ข้อมูลคนโกง เพื่อป้องกันไม่ให้ผู้อื่นตกเป็นเหยื่อได้อีก โดยที่ผู้เสียหายต้องยืนยันตัวตนก่อน จากนั้นจึงจะสามารถแจ้งข้อมูลการการโกง และข้อมูลคนโกงได้

ช่วยรวมหลักฐาน เป็นการทำเอกสารเพื่อให้ผู้เสียหายนำไปประกอบการแจ้งความดำเนินคดี โดยจมีเจ้าหน้าที่ลำดับเหตุการณ์ สรุปพฤติการณ์ และจัดทำเอกสารรูปแบบPDF ให้กับผู้เสียหาย

เช็กตัวตนผู้ขาย หรือการตรวจสอบข้อมูลผู้ขายที่ไม่มีการยืนยันตัวตนกับฉลาดโอน

นอกจากนี้ยังมีการกล่าวถึงสถิติการใช้งานบริการฉลาดโอน อาทิ จำนวนการตรวจสอบผู้กระทำความผิดบนเว็บไซต์ฉลาดโอน, จำนวนผู้ลงทะเบียนในระบบ, จำนวนการแจ้งข้อมูลคนโกงและรวบรวมหลักฐาน ตลอดจนจำนวนการใช้บริการฉลาดโอนผ่านช่องทางไลน์

จากนั้นผู้ดำเนินรายการได้เชิญให้ผู้รับฟังบรรยายจากหน่วยงานต่าง ๆ ร่วมกันซักถามข้อสงสัยในการใช้งานเว็บไซต์ฉลาดโอน และข้อมูลเกี่ยวกับการทำธุรกรรมออนไลน์

บทที่ 6
ภาพรวมระบบป้องกันและปราบปรามมิจฉาชีพออนไลน์ที่ไม่ระบุตัวตน

บทที่ 6 นี้ จัดทำขึ้นเพื่อแสดงรายละเอียดของภาพรวมและแผนการดำเนินงานของโครงการพัฒนาระบบป้องกันและปราบปรามมิจฉาชีพออนไลน์ที่ไม่สามารถระบุตัว ตลอดจนแนวทางการแลกเปลี่ยนข้อมูลและภาพรวมการพัฒนาระบบต้นแบบฯ นี้

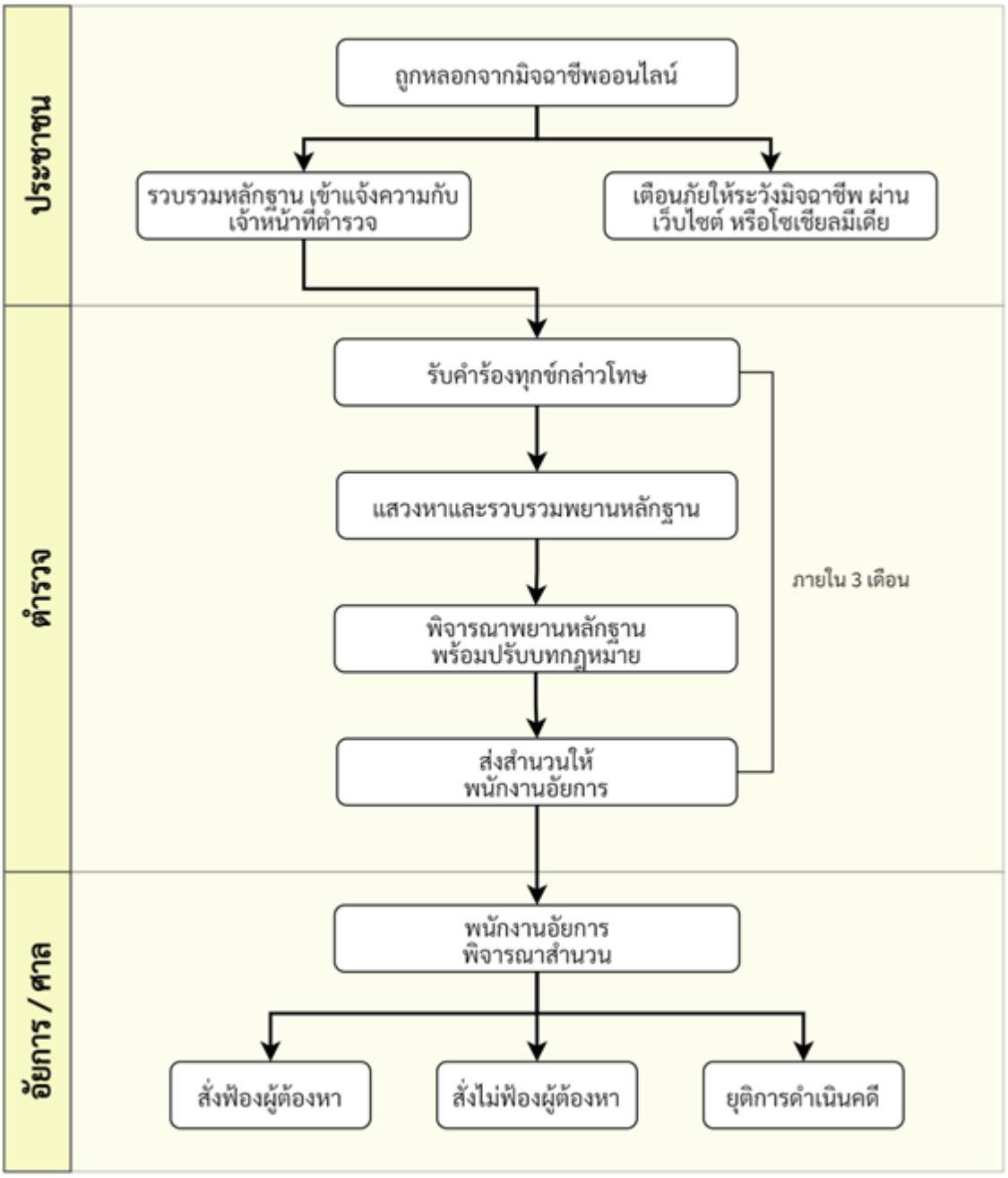
6.1 แนวทางหลักเกณฑ์และระเบียบปฏิบัติในการรวบรวมพยานหลักฐาน

1) การทำงานของสำนักงานตำรวจ

โดยทั่วไป เมื่อมีเหตุกรณีฉ้อโกงออนไลน์เกิดขึ้น สำหรับผู้เสียหายจะต้องเข้าแจ้งความกับเจ้าหน้าที่ตำรวจ ณ สถานีตำรวจท้องที่ที่เกิดเหตุฉ้อโกงออนไลน์ขึ้น ภายในระยะเวลา 3 เดือน นับจากวันที่ทราบเรื่อง โดยผู้เสียหายต้องจัดเตรียมหลักฐานต่าง ๆ อย่างน้อย ดังนี้

(1) รูปภาพของสินค้า
(2) หน้าเว็บไซต์ที่ขายของ โพสต์ประกาศซื้อหรือขายสินค้า
(3) ข้อความการสนทนาระหว่างผู้ซื้อและผู้ขาย
(4) ชื่อบัญชีและเลขบัญชีธนาคารของผู้ขาย
(5) สลิปหรือภาพหลักฐานการโอนเงินชำระค่าสินค้า

จากนั้น พนักงานสอบสวนประจำสถานีตำรวจจะดำเนินตามขั้นตอนตั้งแต่ การรับเรื่องร้องเรียนจากผู้เสียหาย การสืบสวนสอบสวน การพิจารณาหลักฐาน และส่งสำนวนต่อไปยังอัยการเพื่อพิจารณาการสั่งฟ้องหรือสั่งไม่ฟ้องต่อไป



รูปที่ 6-1 ขั้นตอนการแจ้งความเมื่อถูกฉ้อโกงออนไลน์

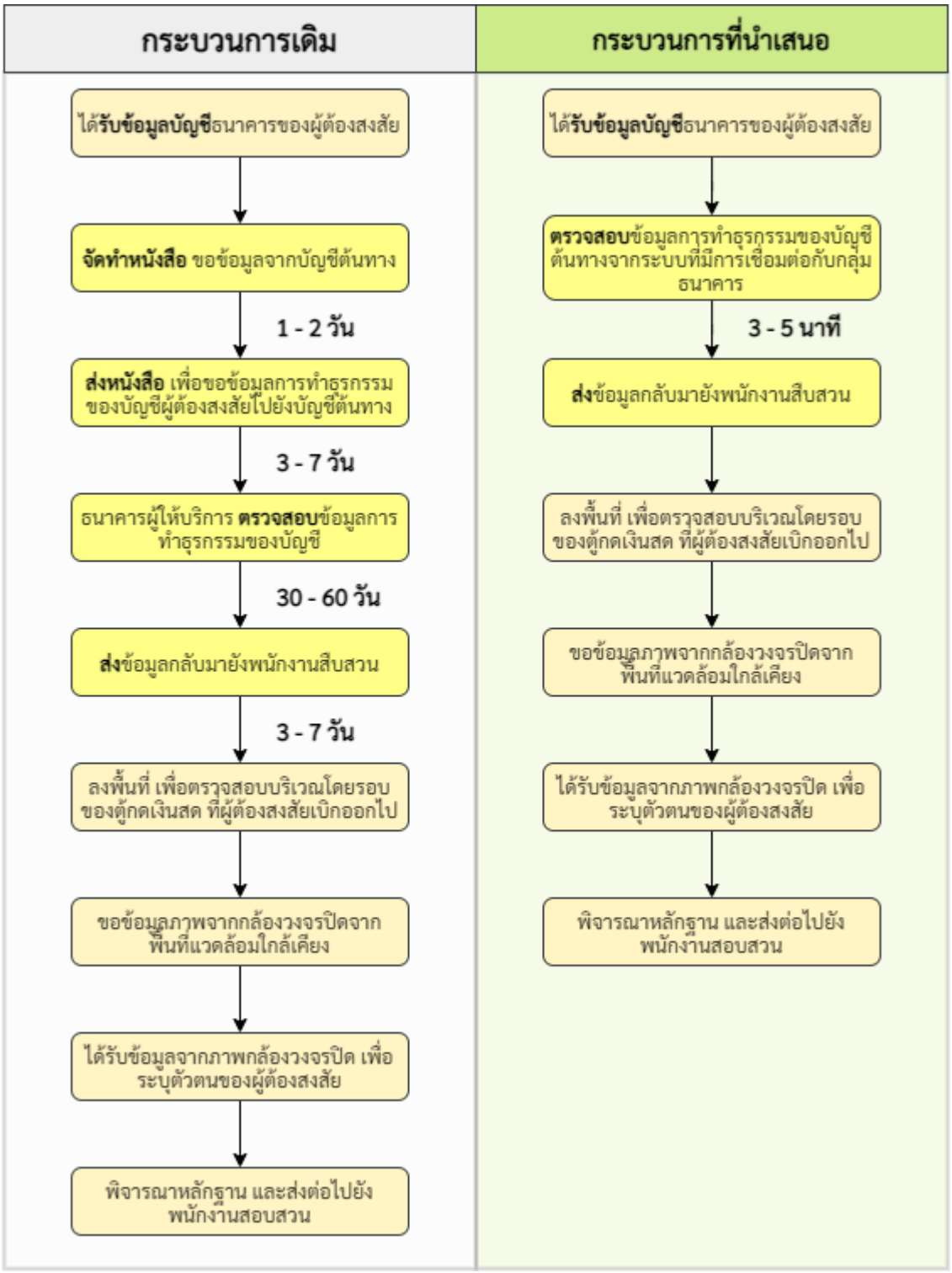
การดำเนินการ ในส่วนของเจ้าหน้าที่ตำรวจเกี่ยวกับคดีฉ้อโกงออนไลน์ มีขั้นตอน ดังนี้

1) รับคำร้องทุกข์กล่าวโทษ

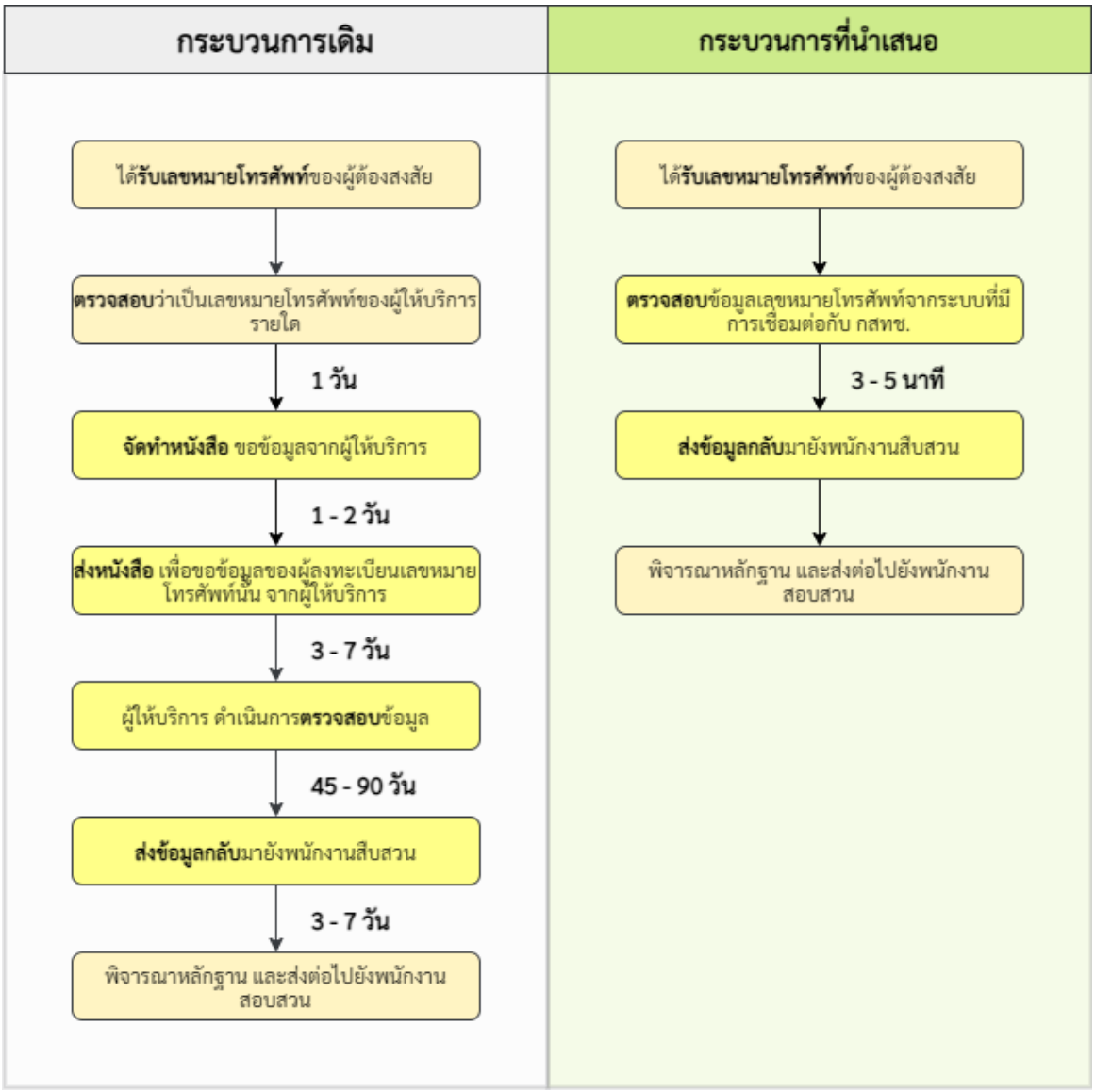
พนักงานสอบสวนเวร จะปฏิบัติหน้าที่เพื่อรับคำร้องทุกข์หรือคำกล่าวโทษ เมื่อดำเนินการจะลงบันทึกประจำวันรับแจ้งความดำเนินคดี เพื่อเป็นหลักฐานเอาไว้ โดยในขั้นตอนนี้ จะมีข้อพิจารณาเบื้องต้น เช่น (1) กรณีที่ได้รับแจ้งเป็นคดีอาญาหรือไม่, (2) ผู้แจ้งเป็นผู้เสียหายหรือผู้กล่าวโทษหรือไม่, (3) อยู่ในเขตอำนาจสอบสวนหรือไม่ เป็นต้น โดยเมื่อพนักงานสอบสวนเวรได้ข้อสรุปเบื้องต้นแล้ว ก็จะดำเนินการในขั้นตอนถัดไป

2) การแสวงหาและรวบรวมพยานหลักฐาน

ขั้นตอนนี้เป็นขั้นตอนสำคัญของการสืบสวนเพื่อพิสูจน์ตัวตนของผู้กระทำความผิด ของคดีฉ้อโกงออนไลน์ โดยมิจฉาชีพจะใช้เครื่องมือหลัก ๆ ในการดำเนินการฉ้อโกงออนไลน์ ได้แก่ ช่องทางการชำระสินค้า ซึ่งจะอยู่ในรูปแบบของบัญชีเงินฝากธนาคาร หรือกระเป๋าสตางค์อิเล็กทรอนิกส์ (E-Wallet) เพราะเป็นช่องทางให้ผู้เสียหายชำระสินค้ามายังมิจฉาชีพได้ กรณีที่เป็นบัญชีเงินฝากของธนาคาร จะถือว่าเป็นช่องทางมีที่มาตรฐานความปลอดภัยระดับหนึ่ง มีธนาคารพาณิชย์อันเป็นสถาบันการเงินตามกฎหมายเป็นผู้รับผิดชอบ โดยมีธนาคารแห่งประเทศไทยเป็นผู้ควบคุมดูแล และผู้ที่จะเปิดบัญชีเงินฝากกับธนาคารพาณิชย์ต้องยืนยันตัวตนอย่างชัดเจน ธนาคารพาณิชย์ซึ่งเป็นผู้รับผิดชอบบัญชีเงินฝากเหล่านั้น จึงต้องปฏิบัติตามที่พนักงานสอบสวนสั่งการในอำนาจตามกฎหมายเสมอ และการดำเนินการต่าง ๆ ของธนาคารนั้นสามารถทำการตรวจสอบได้ ส่วนกระเป๋าสตางค์อิเล็กทรอนิกส์นั้น ผู้ให้บริการกระเป๋าสตางค์อิเล็กทรอนิกส์บางรายไม่ได้มีการตรวจสอบหรือให้ผู้เข้ารับบริการเปิดบัญชีต้องยืนยันตัวตนอย่างละเอียด และผู้ให้บริการบางรายยังไม่ได้ผ่านการรับรองหรือตรวจสอบการดำเนินงานจากธนาคารแห่งประเทศไทย จึงทำให้ยากต่อการตรวจสอบหลักฐานการดำเนินการต่างๆจากพนักงานสอบสวนอย่างยิ่ง โดยกระบวนการตรวจสอบข้อมูลจากบัญชีเงินฝากธนาคาร แสดงดังรูปที่ 2-2 และกระบวนการตรวจสอบข้อมูลจากกระเป๋าสตางค์อิเล็กทรอนิกส์ แสดงดังรูปที่ 2-3



รูปที่ 6-2 กระบวนการตรวจสอบข้อมูล กรณีเป็นบัญชีเงินฝากธนาคาร



รูปที่ 6-3 กระบวนการตรวจสอบข้อมูล กรณีเป็นกระเป๋าสตางค์อิเล็กทรอนิกส์

3) พิจารณาพยานหลักฐานพร้อมปรับบทกฎหมาย
การพิจารณาพยานหลักฐานของเจ้าหน้าที่สอบสวน มีขั้นตอนดังนี้
(1) ข้อเท็จจริงที่เกี่ยวกับการกระทำ
การพิจารณาจากพยานหลักฐานที่รวบรวมมา
(2) กฎหมายที่เกี่ยวข้องกับการกระทำ
การนำข้อเท็จจริงที่เกิดขึ้นในคดีมาปรับกับตัวบทกฎหมายและวินิจฉัยชี้ขาดว่าข้อเท็จจริงนั้นมีผลทางกฎหมายอย่างไร การกระทำเหล่านั้นเป็นความผิดอย่างไร ฐานใด ชอบด้วยกฎหมาย มีสิทธิตามกฎหมายที่จะกระทำได้หรือไม่ เป็นต้น
(3) ความเห็นทางคดีของพนักงานสอบสวน
พนักงานสอบสวนผู้รับผิดชอบ สรุปสำนวนการสอบสวนโดยต้องประกอบด้วยข้อเท็จจริงและความเห็นในข้อเท็จจริงที่ได้จากพนักงานเจ้าหน้าที่
(4) เสนอผู้บังคับบัญชาพิจารณา
พนักงานสอบสวนผู้รับผิดชอบ เสนอสำนวนสอบสวนต่อผู้บังคับบัญชา เพื่อพิจารณาเสนอพนักงานอัยการต่อไป

4) ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 140-144 พนักงานสอบสวนจะต้องทำความเห็นหลังจากรวบรวมหลักฐานแล้ว ว่าเห็นควร อย่างไร "เห็นควรสั่งฟ้อง" "เห็นควรสั่งไม่ฟ้อง" ในคดีที่ไม่ทราบตัวผู้กระทำความผิด ให้มีความเห็น "เห็นควรงดการสอบสวน" จากนั้นดำเนินการส่งเรื่องต่อไปยังพนักงานอัยการเพื่อให้ลงความเห็นต่อไป

สรุปการวิเคราะห์ปัญหาและแนวทางแก้ไข

ช่วงเวลา	ผลจากการวิเคราะห์ปัญหา	แนวทางในปัจจุบัน			แนวทางที่ควรปรับปรุง
		ผู้ที่เกี่ยวข้อง	สาเหตุที่พบ	ผลที่ตามมา	
ก่อนเกิดเหตุ	ซื้อหรือโอน **ทั้งๆ ที่รู้ว่าอาจถูกหลอกได้** คิดว่าตัวเองแน่นอนละเอียดพอ	-	การตรวจสอบความน่าเชื่อถือในการซื้อ-ขาย **รู้ไม่เท่าทันโจร**	เกิดการซื้อขายด้วย **วิธีที่โจรกำหนด**	**ให้เครื่องมือ** แบบนำไปใช้และแนะนำต่อได้จริงและทันสมัย (ถ้า**ให้ความรู้**แบบเอาไปใช้จริงไม่ได้ คนไม่อยากอ่าน)
ระหว่างเกิดเหตุ	ซื้อด้วย**อารมณ์ที่ถูกกระตุ้น** ไม่ทันฉุกคิด/หาข้อมูล/ถาม	-	มองโลกในแง่ดี คิดว่าเป็นเงินเล็กน้อย เสียได้	**โดนหลอก** และ **สร้างโจรเพิ่ม**ขึ้น	**หยุดโจรหน้าใหม่**ที่จะเพิ่มขึ้นและทำให้**หน้าเก่าทำงานยาก**

ช่วงเวลา	ผลจากการวิเคราะห์ปัญหา	แนวทางในปัจจุบัน			แนวทางที่ควรปรับปรุง
		ผู้ที่เกี่ยวข้อง	สาเหตุที่พบ	ผลที่ตามมา	
					ขึ้น
หลังเกิดเหตุ	ไปแจ้งความแค่เพื่อ**ต้องการเอกสารไปขออายัดบัญชีที่ธนาคาร** เท่านั้น แต่เอกสารดังกล่าวต้อง**แจ้งความดำเนินคดี** และตำรวจบอกว่าการแจ้งความดำเนินคดีต้องมีการดำเนินการจนถึงที่สุดด้วย (ได้เงินคืนเป็นของแถม)	ตำรวจ ใกล้บ้าน	ไปแจ้งความดำเนินคดี แต่กลับถูก**ตำรวจปฏิเสธ**	ตำรวจไม่รับแจ้งแบบดำเนินคดี แต่จะรับลงบันทึกประจำวันไว้ เพราะพิจารณาแล้วว่าไม่น่าจะนำตัวผู้ถูกกล่าวหามาดำเนินคดีได้จริง เพราะรู้ว่าจะเป็นบัญชีม้า จับไม่ได้แน่นอน	ปรับปรุงระเบียบให้**แจ้งความดำเนินคดีเพื่ออายัดบัญชี<u>เป็นกรณีพิเศษ</u>** เพื่อหยุดการสร้างโจร และทำให้**การแจ้งความดำเนินคดีเป็นไปได้**อย่างรวดเร็ว (โดยตำรวจไม่ต้องดำเนินคดีต่อ)
หลังเกิดเหตุ	ตำรวจ ร้องขอข้อมูลกับหน่วยงานที่เกี่ยวข้อง **มีความล่าช้า** หรือ **พิจารณาว่ามูลค่าความเสียหายน้อย** ไม่คุ้มกับทรัพยากรของรัฐที่เสียไป (งบประมาณและเวลา) โจรอาจคืนเงิน	ธนาคาร (บัญชีม้า / การโอนต่อไปไหน) หรือ ผู้ให้บริการอินเตอร์เน็ต (Log / IP / User Address) หรือ ผู้ให้บริการโทรศัพท์เคลื่อนที่ (Call Detail Log / Cell Site / User Address)	ผู้ที่เกี่ยวข้องมองว่าตนเอง**เป็นแค่คนกลาง** จึงไม่ได้ให้ความสำคัญ เพราะ**เหตุเกิดที่แพลตฟอร์ม** ตัวการหลักควรจะเป็น**เจ้าของแพลตฟอร์ม**ที่ต้องให้ข้อมูล ซึ่งกฎหมายไทยยังไม่สามารถบังคับหรือขอ	เกิดความ**ล่าช้า** หรือไม่สามารถสืบหาข้อมูลประกอบการดำเนินคดีได้ ทำให้เกิดคดีต่อเนื่องจำนวนมาก สร้างโจรเพิ่มขึ้น ไปจนถึงไม่ได้หลักฐานที่จะเอาผิดได้	**สร้างเครื่องมือร่วมกัน**เพื่อให้ลดระยะเวลาการแลกเปลี่ยนข้อมูล และสร้างเครื่องมือที่ทำให้ตำรวจ**ลดการขอข้อมูล**จากหน่วยงานอื่น

ช่วงเวลา	ผลจากการวิเคราะห์ปัญหา	แนวทางในปัจจุบัน			แนวทางที่ควรปรับปรุง
		ผู้ที่เกี่ยวข้อง	สาเหตุที่พบ	ผลที่ตามมา	
	กับผู้ฟ้องเพราะผู้ไม่ฟ้องยังมีอีกมากและยอมความในที่สุด ตำรวจจึงต้องพิจารณารับดำเนินคดีเฉพาะเป็นคดีฉ้อโกงประชาชน		ความร่วมมือได้		
หลังเกิดเหตุ	**ไม่สามารถระบุตัวตนจริง**ของโจรได้ จากข้อมูลที่ผู้เสียให้ในปัจจุบัน เพราะส่วนใหญ่เป็นข้อมูลหลอก	ผู้ซื้อ/ผู้โอน/ผู้เสียหาย	คิดว่าหลักฐานที่แชทกันจะใช้เป็นหลักฐานสำคัญได้ เพราะมีเบอร์บัญชีผู้รับโอนจริง ถึงแม้จะติดต่อผ่าน ทางเฟซบุ๊ค	ระบุตัวตนของโจรไม่ได้ และไปแจ้งความตำรวจไม่รับดำเนินคดี	**สร้างเครื่องมือให้ผู้ซื้อ**นำไปใช้ในการตรวจสอบและเก็บหลักฐานช่วยตำรวจให้มากที่สุด

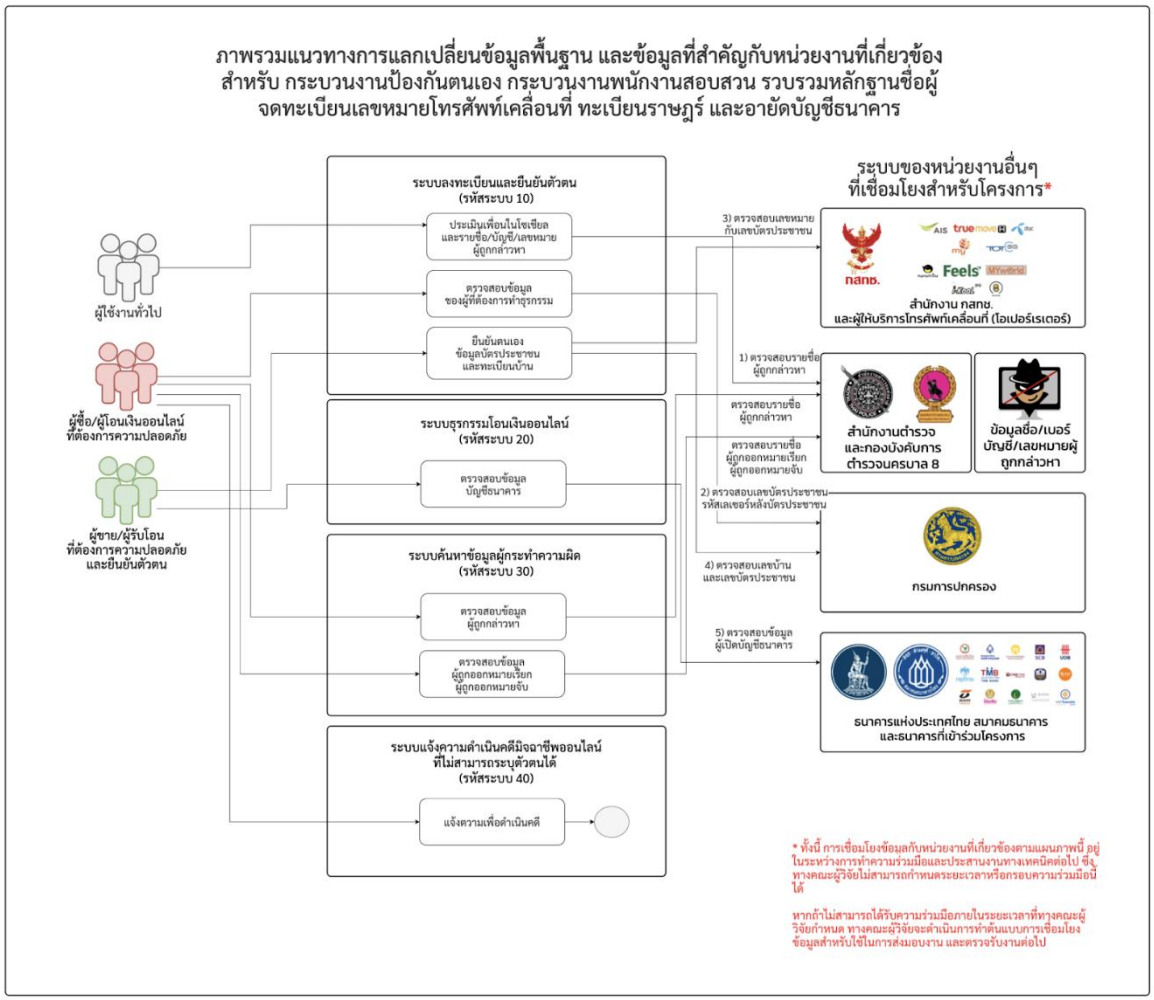
จากผลการศึกษาความเป็นไปได้ในการป้องกัน และปราบปรามมิจฉาชีพออนไลน์แบบระบุตัวตนไม่ได้นั้น ผู้ทรงคุณวุฒิได้อภิปรายเป็นในทางเดียวกันว่าทางภาครัฐจำเป็นต้องบังคับใช้กฎหมายอย่างเด็ดขาด กับเจ้าของระบบแพลตฟอร์มที่เข้ามาให้บริการแก้ประชาชนคนไทย อาทิเช่น Facebook, Instagram, Twitter, LINE ตามแนวทางที่ประเทศเจ้าของแพลตฟอร์ม หรือประเทศอื่นๆ ที่กำลังดำเนินการแก้ไขกฎหมายให้สอดคล้องกับปัญหาของสังคมที่อาจจะเกิดขึ้นได้ในอนาคต ตลอดทั้งการทำความร่วมมือกับทางเจ้าของแพลตฟอร์มก่อนที่จะอนุญาตในการให้บริการดังกล่าว

แต่ทั้งนี้ขอบเขตของการศึกษาความเป็นไปได้ในระยะนี้ จึงมีความจำเป็นต้องแนวทางการเชื่อมโยงข้อมูลกับหน่วยงานที่เกี่ยวข้อง และ/หรือเป็นช่องทางให้กับมิจฉาชีพนั้นมีความสำคัญเป็นอย่างมากต่อการป้องกันและปราบปรามดังกล่าว ได้แก่

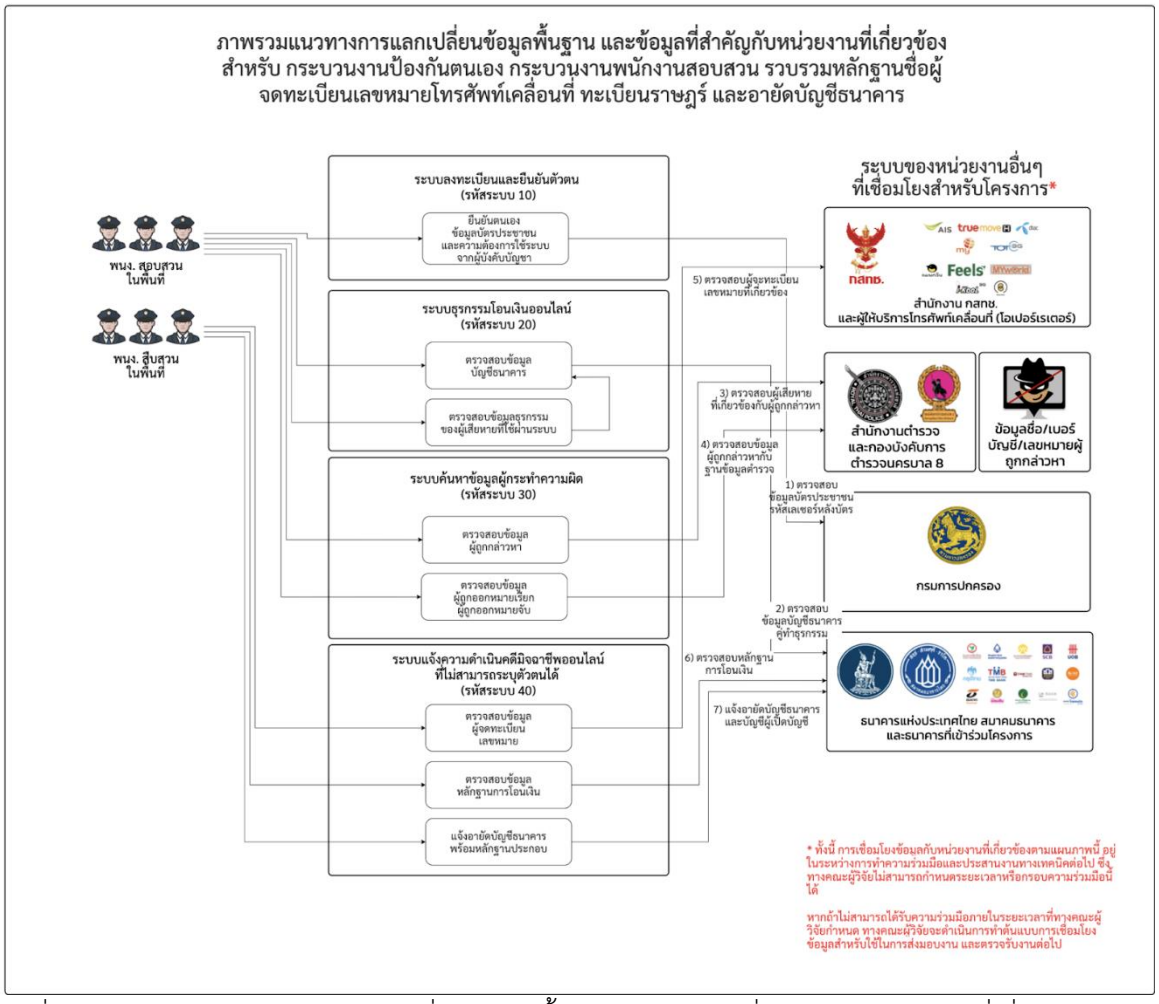
1. ผู้ให้บริการโทรศัพท์เคลื่อนที่ ที่เป็นช่องทางสำคัญเพื่อจะขอใช้บริการอินเตอร์เน็ต
2. ผู้ให้บริการอินเตอร์เน็ต ที่เป็นช่องทางหลักในการเข้าใช้งานของมิจฉาชีพ และผู้เสียหาย

3. สมาคมธนาคารแห่งประเทศไทย ที่เป็นช่องทางที่มิจฉาชีพจะให้ผู้เสียหายโอนเงินเข้าบัญชีที่เปิดกับธนาคารในประเทศไทย ก่อนที่จะโอนเงินต่อไปยังบัญชีเป้าหมาย หรือฟอกเงินไปยังทรัพย์สินอื่นๆ หรือไปจนเกิดการเบิกเงินที่ตู้เอทีเอ็มต่อไป
4. ทรูมันนี่ วอลเล็ท ที่เป็นช่องทางที่มิจฉาชีพใช้เป็นกระเป๋าเงินอิเล็กทรอนิกส์ ก่อนที่จะโอนเงินต่อไปยังบัญชีเป้าหมาย หรือฟอกเงินไปยังทรัพย์สินอื่น ๆ ต่อไป

คณะผู้วิจัยออกแบบแนวทางการแลกเปลี่ยนข้อมูลเพื่อให้เจ้าหน้าที่ตำรวจในพื้นที่ของงานวิจัยนี้เป็นผู้ขอข้อมูลดังกล่าวอย่างเป็นทางการต่อไป ซึ่งทางคณะผู้วิจัยไม่สามารถกำหนดระยะเวลาหรือกรอบความร่วมมือนี้ได้ แต่ระบบต้นแบบฯ ที่พัฒนาขึ้นนี้จะรองรับการบันทึกข้อมูลจากแหล่งข้อมูลที่ได้รับ เพื่อเป็นแนวทางในการนำเสนอให้ผู้บริหารของหน่วยงานที่เกี่ยวข้องเข้าใจถึงแนวทางการป้องกัน และปราบปราม และจะเห็นชอบในการร่วมมือได้ในอนาคต



รูปที่ 6-4 แผนภาพแนวทางการแลกเปลี่ยนข้อมูลพื้นฐาน และข้อมูลที่สำคัญกับหน่วยงานที่เกี่ยวข้องส่วนของผู้ใช้งานทั่วไป ผู้ซื้อผู้โอน ผู้ขายผู้รับโอน



รูปที่ 6-5 แผนภาพแนวทางการแลกเปลี่ยนข้อมูลพื้นฐาน และข้อมูลที่สำคัญกับหน่วยงานที่เกี่ยวข้อง ส่วนของพนักงานสอบสวน และพนักงานสืบสวน

6.2 ผลการแลกเปลี่ยนข้อมูลกับหน่วยงานภายนอก

ทางคณะผู้วิจัย ได้ประสานไปยังหน่วยงานต่าง ๆ เพื่อขอเชื่อมหรือขอใช้ข้อมูล ที่คาดว่าจะเป็นประโยชน์ต่อโครงการ โดยมีรายละเอียด ดังนี้

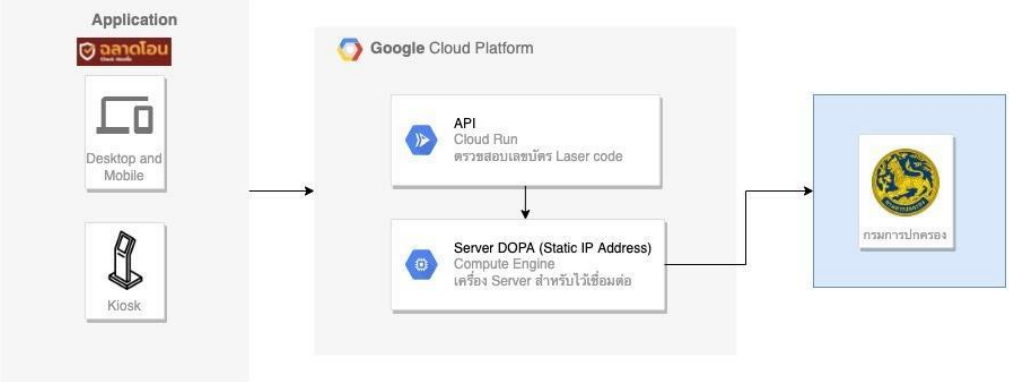
1) การเชื่อมต่อกับสำนักงาน กสทช.
   เป็นการเชื่อมโยงกับระบบการพิสูจน์และยืนยันตัวตนในรูปแบบบัตรประจำตัวอิเล็กทรอนิกส์บนโทรศัพท์เคลื่อนที่ โดยมีชื่อว่า “แทนบัตร” หรือ “Mobile ID” ที่ถูกพัฒนาขึ้น โดยสำนักงาน กสทช. ที่จะอำนวยความสะดวกแก่ประชาชนในการพิสูจน์และยืนยันตัวตนโดยไม่ต้องใช้บัตรประจำตัวประชาชน แต่เนื่องจากมีข้อจำกัดทางข้อกฎหมาย การเชื่อมต่อในปัจจุบันจึงอยู่ในขั้นตอนการร่างเอกสารบันทึกข้อตกลงความร่วมมือ (Memorandum of Understanding) และทำข้อตกลงกันให้แล้วเสร็จก่อนที่จะเริ่มมีเชื่อมต่อ
2) การเชื่อมต่อกับกรมการปกครอง
   เป็นการเชื่อมโยงเพื่อตรวจสอบความถูกต้องของบัตรประจำตัวประชาชน หน้าข้อมูลจาก DOPA โดยมีการได้ขอเชื่อมผ่าน API ที่ทาง DOPA จัดทำให้ โดยระบบฉลาดโอนจะขอให้ผู้ใช้พิมพ์เลขหลังบัตร (Laser code) เข้าระบบ แล้วระบบจะนำชื่อ นามสกุล หมายเลขบัตรประชาชน หมายเลขหลังบัตรประชาชน ส่งไปตรวจสอบความถูกต้องกับ DOPA

Request Header	
Service Name	ระบบตรวจสอบรหัสเลเซอร์หลังบัตรกับเลขบัตรประชาชน
API Name	api/v1/check_lasercode_dopa
API Desc	ใช้ตรวจสอบเลขบัตรประชาชนกับกรมการปกครอง
API URL	{endpoint}/api/v1/check_lasercode_dopa
Authenticate	Basic Authen
Format	JSON
Version	Version 1.0.0
Update Date	2021/07/27

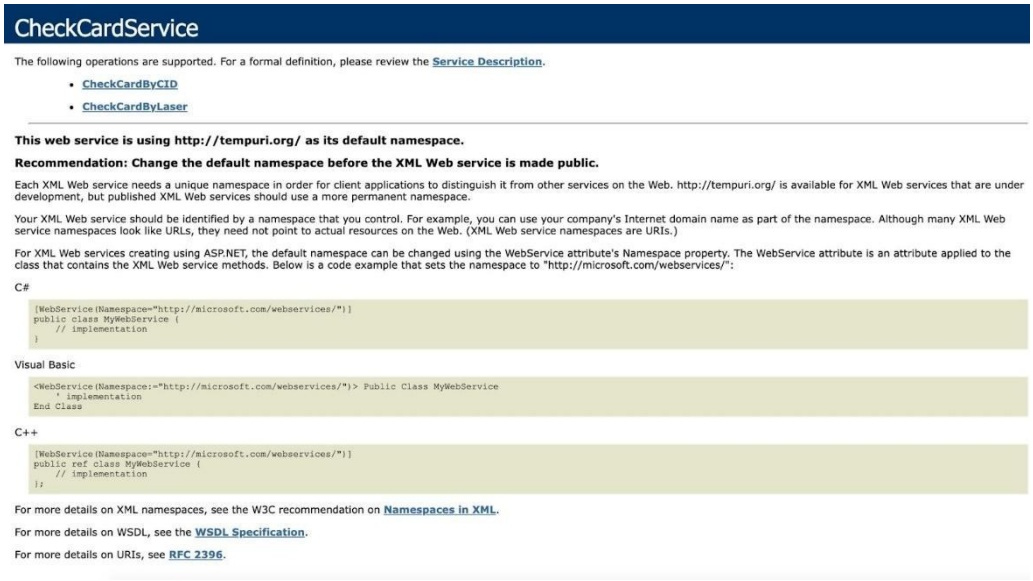
Method	URL
POST	{endpoint}/api/v1/check_dopa

Response Parameter				
Parameter	Name	Type	Require	Description
	CitizenID	int(13)	Y	เลขบัตรประชาชน
	operator	int(2)	Y	ผู้ให้บริการ
Example	{ "CitizenID" : "1228833221122" , “LaserCode” : “IME837201” }			
Return Response	{ “matchedRecord”: “01” (ไม่ตรงกัน), “transactionId”:”29301939” }			

Response Parameter	
	{ “matchedRecord”: “00” (ตรงกัน), “transactionId”:”29301939” "CitizenID": "12233332xxxxx", "title": "น.ส.", "fname": "วริศรา", "lname": "รอดคงรวย", "sex": "หญิง", "dob": "19970920", "nat": "ไทย", "hStat": "", "pStat": "ปกติ", "dmovein": "", "age": "13", "fpid": "3102002xxxxx", "mpid": "0", "fFname": "ไชโย", "mFname": "ลำเทียน", "fnat": "ไทย", "mnat": "ไทย", "hid": "102005xxxxx", "houseNo": "126/39", "villageNo": "", "alleyDesc": "", "alleyWayDesc": "", "roadDesc": "ถ.จรัญสนิทวงศ์", "subdistrictCode": "", "subdistrictDesc": "บางขุนศรี", "districtCode": "", "districtDesc": "บางกอกน้อย", "provinceCode": "10", "provinceDesc": "กรุงเทพมหานคร" }

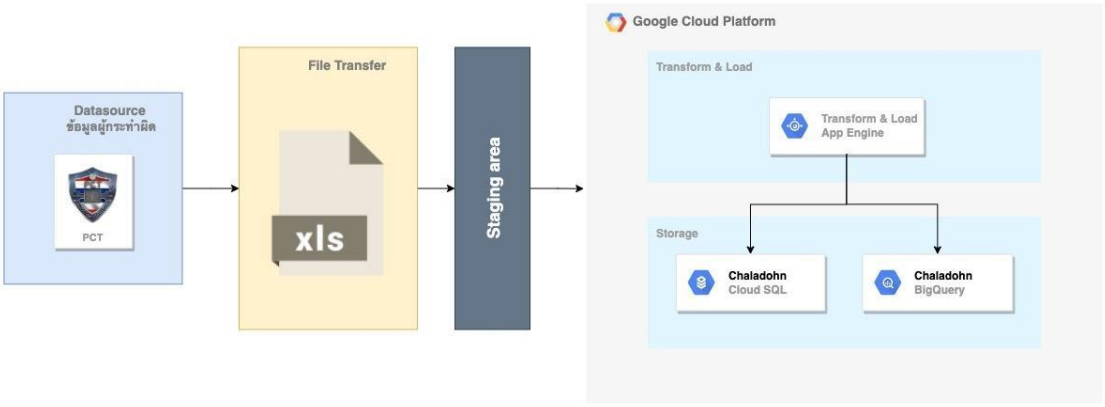


รูปที่ 6-6 ภาพรวมการเรียกขอข้อมูลกับทางกรมการปกครอง



รูปที่ 6-7 ภาพเอกสารอ้างอิงสำหรับการเชื่อมต่อ

3) การขอข้อมูลจากศูนย์ปราบปรามอาชญากรรมทาง
การข้อมูลเรื่องร้องเรียน จากศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ (ศปอส.ตร.) โดยทางศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ (ศปอส.ตร.) ได้ทำการ Export ข้อมูลระบบฐานข้อมูลของศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ (ศปอส.ตร.) ในรูปแบบไฟล์ Excel และได้จัดส่งไฟล์ข้อมูลร้องเรียนย้อนหลังให้กับทีมผู้วิจัย เพื่อให้ทางทีมผู้วิจัยได้นำข้อมูลดังกล่าวมานำเข้าสู่ระบบฐานข้อมูล โดยระบบจะทำการคัดกรอง และจัดกลุ่มประเภทของข้อมูล แล้วส่งไปประมวลผล เพื่อทำ Data model และ Data virtualization ต่อไป โดยหลังจากนี้ จะนำเข้าไฟล์ข้อมูลเป็นประจำทุกเดือนต่อไป แสดงดังรูปที่ 6-8 และแสดงตัวอย่างข้อมูลดังรูปที่ 6-9

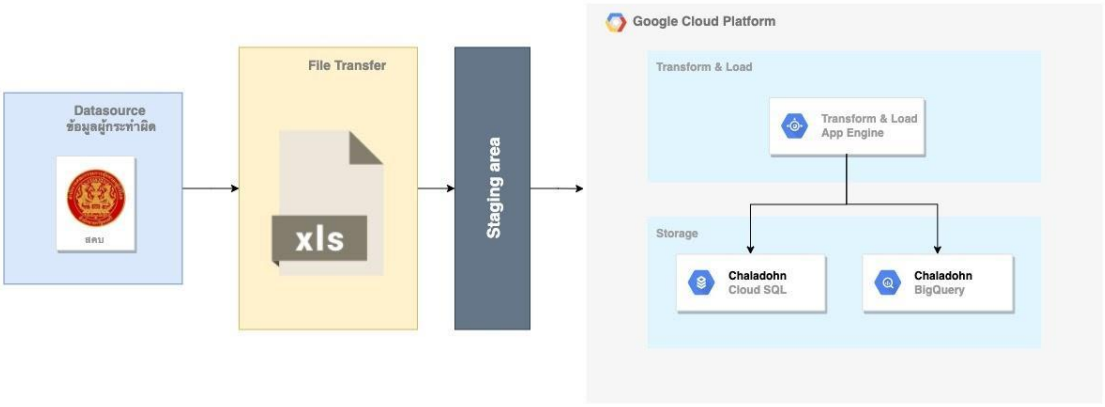


รูปที่ 6-8 ภาพรวมการขอข้อมูลจากศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ (ศปอส.ตร.)

ลำดับ	วัน/เดือน/ปี	เรื่องราวพฤติการณ์	มูลค่าความเสียหาย	วัน/เดือน/ปี	ผู้ร้องเรียน/ผู้เสียหาย	อายุ	ที่อยู่	โทรศัพท์	ผู้ถูกกล่าวหา	ช่องทางรับแจ้ง	พื้นที่	ประเภท	ผู้รับผิดชอบ	ผลการดำเนินการ
1	1/11/62	ธนาคาร ไทยพาณิชย์ฯ ได้ส่งข้อความแจ้งเตือนการชำระค่าสินค้า แต่ผู้แจ้งไม่ได้สั่งซื้อสินค้า	24,350	28 ต.ค. 62	[redacted]	27	ช.หน้าวชิรพยาบาล แขวงเขตดุสิต กทม.	[redacted]	ไม่มี	ศปอส.ตร.	น.	5	ว.ต.อ.วสินต์ แซ่เล่นคง พงส.สน.ชนวมตาลา 088-7283991	โทรแจ้งพงส.แล้ว
2	1/11/62	ผู้เสียหายสั่งยาใจข้อจากเวป แต่หลอกของมา	4,250	30 ต.ค. 62	[redacted]	55	47/129 ม.1 ต.บึงยี่โถ อ.	[redacted]	เวปไซต์ greenofdestiny	1599	ภ.1	1.3	พงส.สภ.ธัญบุรี (ปทุมธานี)	แนะนำให้ผู้เสียหายแจ้งความก่อน
3	2/11/62	เฟสบุ๊ค "Sakura Ac" มาหลอกยืมเงินเพื่อนของ	ไม่มี	2 พ.ย. 62	ไม่ประสงค์ออกนาม	ไม่มี	ไม่มี	ไม่มี	ไม่มี	1599	น.	1.3	พงส.สน.บางซื่อ	โทรกลับไป พบว่าไม่สามารถ
4	3/11/62	มีคนร้าย แอบแฝงข้อมูลมือถือ และแจ้งของผู้แจ้ง แต่ผู้แจ้งยังไม่ได้รับความเสียหายแต่อย่างใด	ไม่มี	3 พ.ย. 62	[redacted]	37	7/36 ม.1 ต.มะขาม อ. มะขาม จ.จันทบุรี	[redacted]	ไม่มี	1155	ภ.2	5	พงส.สภ.มะขาม (จันทบุรี)	โทรประสานหัวหน้างาน สอบสวน สภ.มะขามแล้ว
5	3/11/62	คนร้ายใช้เฟสบุ๊คชื่อ "Jerapon Sommuk" โพสต์	ไม่มี	30 ก.ย. 62	[redacted]	41	333/313 ม.1 ต.บางเพรียง	[redacted]	ไม่มี	1155	ภ.1	5	พงส.สภ.บางพลี	ได้โทรประสาน สว.(สอบสวน)
6	4/11/62	ผู้ต้องหานำบัญชีม้ามาหลอกขายผู้เสียหายไป	ไม่มี	22 ต.ค.62	[redacted]	18	เลขที่ 74 หมู่ 9 ต.บางปรือ	[redacted]	ไม่มี	1155	ไม่มี	5	อยู่ระหว่างเสนอผู้บังคับบัญชา	อยู่ระหว่างเสนอผู้บังคับบัญชา
7	4/11/62	หลอกขายไอเทม ไปร ๑๑ โพสใน	24,350	2 พ.ย.62	[redacted]	ไม่มี	5/11 ซ.พัฒนสิน ถ.บางลี่นใน	[redacted]	น.ส.พัชรกันย์ บุญรู้ยิ่ง	1155	น.	2.3	พ.ต.ท.ศุภชัย หาญคำหล้า	โทรประสานแล้ว
8	5/11/62	เฟสบุ๊ค "Piyanut PK Natsu" โพสขายไอดีเกมส์	ไม่มี	4 พ.ย.62	[redacted]	ไม่มี	95/381 ถ.ลำลูกกาคลอง 8	ไม่มี	ไม่มี	1155	ภ.1	1.3	ร.ต.อ.ธีรศักดิ์ แสนโท	โทรแจ้งพงส.แล้ว
9	5/11/62	ผู้เสียหายถูกหลอกขายโทรศัพท์ที่ห้อ แอปปิ้ล	3,100	26 ต.ค.62	[redacted]	ไม่มี	๑๐๒ ม.๖ ต.คลองตะ	[redacted]	064-1014349	1155	ภ.6	2.3	พ.ต.ท.บุญชัย บุญเอี่ยม	โทรประสานแล้ว
10	6/11/62	ผู้เสียหายนำรถไปจำนำ ที่ลงประกาศในเพจ	๑.๖๐๐,๐๐๐	2 พ.ย.62	[redacted]	39	ไม่มี	[redacted]	BKK autocash	ศปอส.ตร.	น.	2.3	พงส.สน.ห้วยขวาง	นัดหมายให้ผู้เสียหายเข้าพบ
11	7/11/62	คนร้ายเปิดเพจขายของผ่านเฟสบุ๊คหลายเพจ	70,000	มิ.ย.62	[redacted]	32	286/7	[redacted]	ไม่มี	ศปอส.ตร.	น.	2.3	ร.ต.ท.วิชวินท์ สิทธิโชค	นัดหมายให้ผู้เสียหายเข้าพบ
12	7/11/62	แชร์ออนไลน์ ผ่านเฟสบุ๊คชื่อ "เกศกา	1,403,360	16 ส.ค.62	[redacted]	34	10/1 ม.1 ต.เมืองเพีย อ.กุด	[redacted]	เกศกา ปราบปรามและ	ศปอส.ตร.	น.	2.2	บก.ปอศ.	รวบรวมเอกสารร้องทุกข์
13	7/11/62	เพจเฟสบุ๊ค "บ้านหนังสือจอมทอง" ผู้เสียหาย	3,433	27 ต.ค.62	[redacted]	31	99/64 ซ.บางแวก 17 แขวง	[redacted]	บ้านหนังสือจอมทอง	1155	น.	2.3	ร.ต.ท.ธังกูร ธรัสมธรินย์	นัดหมายให้ผู้เสียหายเข้าพบ
14	8/11/62	คนร้ายใช้สืบสควบแกมหักมาพูดคุยกับ	35,000	7 พ.ย.62	[redacted]	37	93 ถ.สมัครรวรมการ อ.	[redacted]	ไม่มี	1155	ภ.6	2.3	พ.ต.ท.ปริมทร อุ่ระย้า โทร.	นัดหมายให้ผู้เสียหายเข้าพบ
15	11/11/62	ผู้เสียหายได้รู้จักพูดคุยกับผู้ต้องหาผ่านทาง	300,000	ไม่มี	[redacted]	63	ไม่มี	ไม่มี	ไม่มี	1155	น.	1.2	พงส.สน.คลองตัน	โทรประสานงานไท์ สน.โชคชัย
16	11/11/62	คนร้ายใช้เฟสบุ๊คชื่อ Chompor Fuuin-ong	ไม่มี	17 ต.ค. 62	[redacted]	28	ไม่มี	ไม่มี	ไม่มี	1155	ภ.7	1.3	พงส.สภ.ดู่ทอง (สุพรรณ)	โทรประสานงานไท์ สภ.ดู่ทอง
17	11/11/62	คนร้ายใช้เฟสบุ๊คชื่อ "Malwan Trayougkam"	39,500	ไม่มี	[redacted]	43	ไม่มี	ไม่มี	ไม่มี	1155	ภ.7	1.2	พงส.สภ.สภ.หัวหิน	แนะนำให้ผู้เสียหายร้องทุกข์ที่
18	12/11/62	หลอกให้ซื้อโทรศัพท์มือถือยี่ห้อไอโฟน X	5,650	11 พ.ย. 62	[redacted]	27	บ้านหนองน้ำใส ต.หนอง	[redacted]	063-8094487	1155	ภ.2	2.3	พงส.สภ.วังน้ำเขียว	โทรประสาน ร.ต.อ.นิรันฯ พงส.
19	12/11/62	หลอกให้ซื้อวองแก้ ในไลน์ชื่อ "อังกฤษ"	2,000	9 พ.ย. 62	[redacted]	19	ต.สุเทพ อ.เมือง จ.	[redacted]	นายอังกฤษ วิเศษสังข์	1155	ภ.5	2.3	พงส.สภ.เมืองเชียงใหม่	แนะนำให้ผู้เสียหายไปร้องทุกข์
20	12/11/62	หลอกซื้อขายเดือมะม่วงพันพนต์ไลอบัญชี	8,400	9 ต.ค.62	[redacted]	22	28/10 ม.4 ต.โคกกระบือ อ.	[redacted]	083-5209976	1155	ภ.7	2.3	พงส.สภ.เมืองสมุทรสาคร	แนะนำให้ผู้เสียหายไปร้องทุกข์
21	12/11/62	คนร้ายได้ปลอมเฟสบุ๊คเป็นกรวยฟูใหญ่บ้าน	20,800	11 พ.ย.62	[redacted]	45	617 หมู่ 3 ต.ไทยสามัคคี อ.	[redacted]	ไม่มี	1155	ภ.3	1.3	พงส.สภ.วังน้ำเขียว	ประสานพนักงานสอบสวนแล้ว
22	12/11/62	ผู้เสียหายถูกผู้ต้องหาหลอกลวงให้ซื้อขายแชร์	88,000	4 เม.ย.62	[redacted]	34	51/33 หมู่ 10 แขวงหนอง	[redacted]	ทั่ว ออย ทั่ว นับ	1155	น.	2.2	พงส.สน.หนองจอก	แนะนำผู้เสียหายร้องทุกข์ที่ สน.
23	12/11/62	ถูกหลอกลวงขาย ไอดีเกมส์ ชื่อ PUBG	20,000	11 พ.ย.62	[redacted]	16	128 หมู่ 1 ต.โคกสะอาด	[redacted]	ไม่มี	1155	ภ.3	2.3	พงส.สภ.ลำปลายมาศ	ประสานงานไท์ พงส. ดำเนินคดี
24	13/11/62	อีเมลของผู้เสียหายถูกhion in เข้าจากที่อื่น และ	800	12 พ.ย. 62	[redacted]	41	1492/103 ถ.จุฬินช์ ต.เมือง	[redacted]	นวพร อภิรานานนิยา	ศปอส.ตร.	น.	1.3	พงส.สน.คลองตัน	ประสานให้ผู้แจ้งไปร้องทุกข์ที่

รูปที่ 6-9 แสดงตัวอย่างข้อมูลที่ได้รับจาก ศปอส.ตร.

4) การขอข้อมูลจากสำนักงานคณะกรรมการคุ้มครองผู้บริโภค (สคบ.)
การข้อมูลเรื่องร้องเรียน จากสำนักงานคณะกรรมการคุ้มครองผู้บริโภค (สคบ.) โดยทางสำนักงานคณะกรรมการคุ้มครองผู้บริโภค (สคบ.) ได้จัดส่งไฟล์ข้อมูลร้องเรียนย้อนหลัง เพื่อให้ทางทีมผู้วิจัยได้นำข้อมูลดังกล่าวมานำเข้าสู่ระบบฐานข้อมูล โดยระบบจะทำการคัดกรอง และจัดกลุ่มประเภทของข้อมูล แล้วส่งไปประมวลผล เพื่อทำ Data model และ Data virtualization ต่อไป โดยหลังจากนี้ จะนำเข้าไฟล์ข้อมูลเป็นประจำทุกเดือนต่อไป แสดงดังรูปที่ 6-10 และตัวอย่างข้อมูลที่ได้รับ แสดงดังรูปที่ 6-11



รูปที่ 6-10 ภาพรวมการขอข้อมูลจากสำนักงานคณะกรรมการคุ้มครองผู้บริโภค (สคบ.)

ข้อมูลผู้ถูกร้องทุกข์ เกี่ยวกับปัญหาการสั่งซื้อสินค้าออนไลน์
สำนักงานคณะกรรมการคุ้มครองผู้บริโภค

ลำดับที่	วันที่ถูกร้องทุกข์	ชื่อร้านค้า หรือเจ้าของร้าน	ชื่อบุคคลผู้รับเงิน	บัญชีธนาคาร	หมายเลขโทรศัพท์	หมายเหตุ
๑.	๑๗/๗/๖๓	[illegible]	[illegible]	ธนาคารไทยเครดิต เพื่อรายย่อย จำกัด (มหาชน) เลขที่ [illegible]	ไม่ปรากฏข้อมูล	หมายจับศาลจังหวัดนนทบุรี ที่ ๘๕/๒๕๖๔ และหมายจับที่ ๘๖/๒๕๖๔
๒.	๑๐/๘/๖๓	[illegible]	[illegible] (เลขประจำตัวประชาชน [illegible])	ธนาคารกรุงศรีอยุธยา จำกัด (มหาชน) เลขที่ [illegible]	ไม่ปรากฏข้อมูล	พฤติการณ์แอบอ้างเปิดร้านในแพลตฟอร์มที่น่าเชื่อถือหลอกขายตู้เย็น
๓.	๒๗/๕/๖๓	[illegible]	[illegible]	ธนาคารกสิกรไทย จำกัด (มหาชน) เลขที่ [illegible]	ไม่ปรากฏข้อมูล	พฤติการณ์แอบอ้างเปิดร้านในแพลตฟอร์มที่น่าเชื่อถือหลอกขายสินค้า
๔.	๒๒/๖/๖๔	[illegible]	[illegible]	ธนาคารทหารไทย เลขที่ [illegible]	[illegible]	พฤติการณ์แอบอ้างเปิดร้านในแพลตฟอร์มที่น่าเชื่อถือหลอกขายเกมส์
๕.	๑๘/๓/๖๓	[illegible]	ไม่พบข้อมูล	ธนาคารกสิกรไทย จำกัด (มหาชน) เลขที่ [illegible]		พฤติกรรมไม่ส่งสินค้า
๖.	๕/๑๑/๖๓	[illegible]	[illegible]	ธนาคารกสิกรไทย จำกัด (มหาชน) เลขที่ [illegible]	[illegible]	พฤติกรรมไม่ส่งสินค้า

รูปที่ 6-11 ตัวอย่างข้อมูลที่ได้รับจาก สคบ.

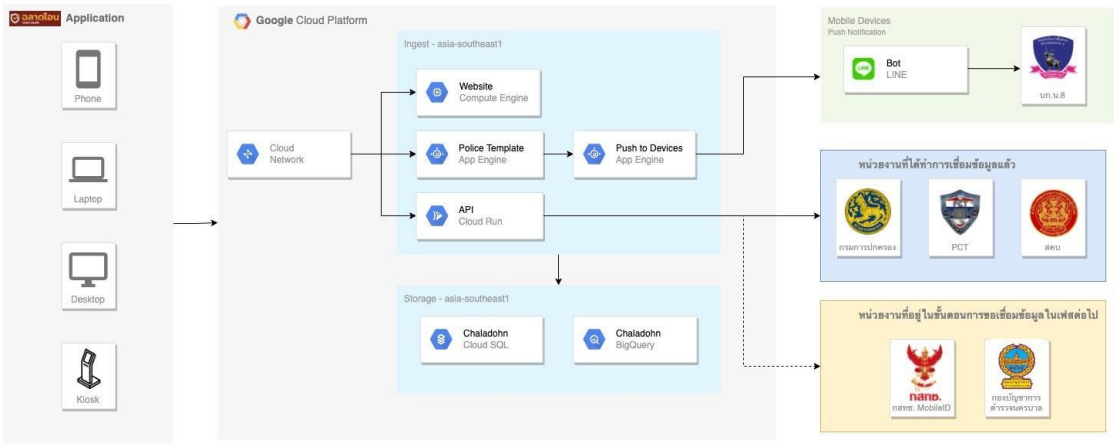
6.3 ภาพรวมของระบบต้นแบบ

ระบบต้นแบบฯ “ระบบป้องกันและปราบปรามมิจฉาชีพออนไลน์ที่ไม่ระบุตัวตน” หรือภาษาอังกฤษเรียกว่า “Unidentified Scammer Prevention and Suppression” หรือใช้อีกชื่อว่า “ฉลาดโอน” เป็นตัวกลางในการแจ้งข้อมูลการทำธุรกรรมโอนเงินที่มีความปลอดภัยโดยผู้ซื้อ (ผู้โอนเงิน) และผู้ขายที่ผ่านการยืนยันตัวตนแล้ว ตลอดจนเป็นฐานข้อมูลมิจฉาชีพที่มีประวัติหรืออยู่ระหว่างการดำเนินคดีฉ้อโกงในโลกออนไลน์ ซึ่งออกแบบให้ระบบนี้เป็น Ecosystem ในการร่วมมือของภาคส่วนที่เกี่ยวข้องเพื่อลดปัญหามิจฉาชีพออนไลน์

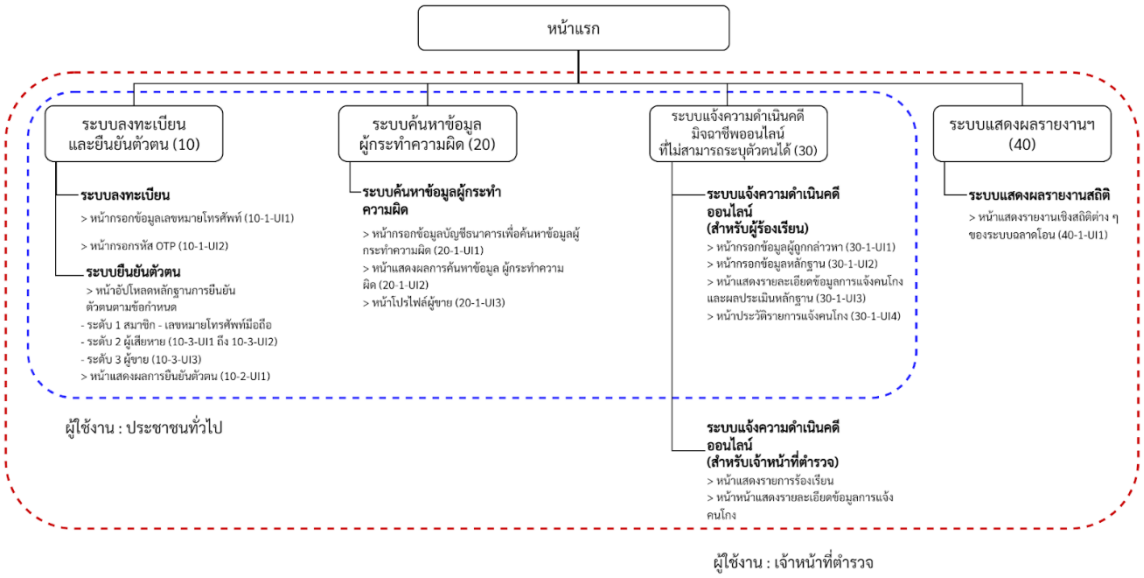
ทางคณะผู้วิจัย ได้สรุปแนวทางการออกแบบระบบต้นแบบฯ โดยแบ่งเป็นภาพรวมระบบต้นแบบฯ เดิมที่เคยออกแบบไว้ และภาพรวมระบบต้นแบบฯ ในปัจจุบัน

สามารถแสดงภาพรวมของระบบต้นแบบ แผนภาพกระแสข้อมูลและแผนผังโครงสร้างข้อมูลในปัจจุบันได้ ดังรูปที่ 6-12 ถึง 6-14 โดยคณะผู้วิจัย จะขอสรุปผลการพัฒนาระบบแต่ละส่วนในบทต่อ ๆ ไป

รูปที่ 6-12 ภาพรวมปัจจุบันของระบบต้นแบบเพื่อสนับสนุนงานป้องกัน
และปราบปรามมิจฉาชีพออนไลน์ที่ไม่สามารถระบุตัวตน
(System Overview)



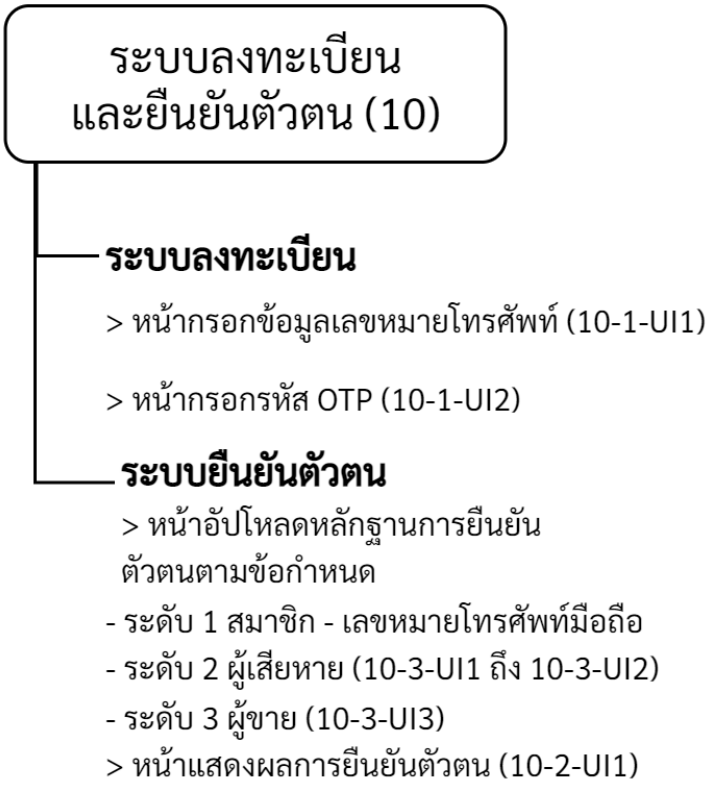
รูปที่ 6-13 แผนภาพกระแสข้อมูล (Dataflow Diagram) และระบบงานหลักของโครงการ



รูปที่ 6-14 ภาพแผนผังโครงสร้างข้อมูล (System Sitemap)
ของระบบต้นแบบฯ

โดยแบ่งได้เป็น 4 ระบบงานหลัก ดังนี้

1) ระบบลงทะเบียนและยืนยันตัวตน เป็นระบบสำหรับตรวจสอบผู้ที่ต้องการใช้งานระบบฉลาดโอน โดยแบ่งระดับผู้ใช้งานออกเป็น 3 ระดับ ได้แก่ สมาชิก ผู้เสียหาย และผู้ขาย



รูปที่ 6-15 ระบบลงทะเบียนและยืนยันตัวตน (10)

โครงสร้างข้อมูลของระบบลงทะเบียนและยืนยันตัวตน มีรายละเอียดดังนี้

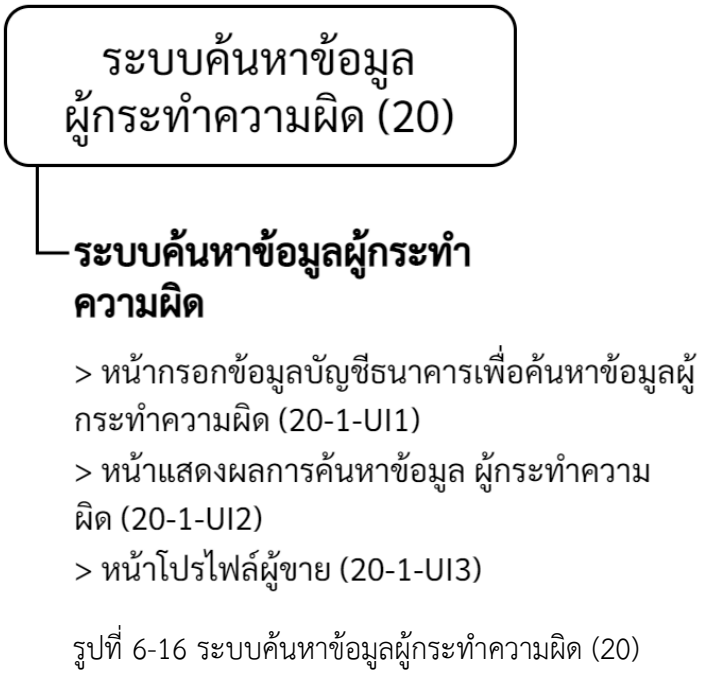
ระบบลงทะเบียน ประกอบด้วย

- หน้ากรอกข้อมูลเลขหมายโทรศัพท์ มีไว้สำหรับให้ผู้เข้าใช้งานกรอกเบอร์โทรศัพท์เพื่อรับ OTP สำหรับเข้าสู่ระบบ
- หน้ากรอกรหัส OTP มีไว้สำหรับให้ผู้ใช้งานกรอกรหัส OTP ที่ได้รับ เพื่อเข้าใช้งานระบบ

ระบบยืนยันตัวตน ประกอบด้วย

- หน้าอัปโหลดหลักฐานการยืนยันตัวตน ซึ่งจะมีทั้งสิ้น 3 ระดับ ได้แก่
  ระดับ 1 สมาชิก สามารถยืนยันตัวตนในระดับนี้โดยใช้เลขหมายโทรศัพท์มือถือเท่านั้น
  ระดับ 2 ผู้เสียหาย สามารถยืนยันตัวตนในระดับนี้ ด้วยเลขหมายโทรศัพท์มือถือ บัตรประจำตัวประชาชนและภาพถ่ายใบหน้า
  ระดับ 3 ผู้ขาย สามารถยืนยันตัวตนในระดับนี้ ด้วยเลขหมายโทรศัพท์มือถือ บัตรประจำตัวประชาชน ภาพถ่ายใบหน้า และสมุดบัญชีธนาคาร
- หน้าแสดงผลการยืนยันตัวตน มีไว้สำหรับ แสดงสถานะของผู้ใช้งานในระบบ สามารถกดยืนยันตัวตนเพิ่มเติมได้จากหน้าแสดงผลนี้

2) ระบบค้นหาข้อมูลผู้กระทำความผิด เป็นระบบสำหรับผู้ที่ต้องการโอนเงินเพื่อทำธุรกรรมทางออนไลน์ สามารถตรวจสอบความน่าเชื่อถือของบุคคลที่ต้องการทำธุรกรรมด้วยได้

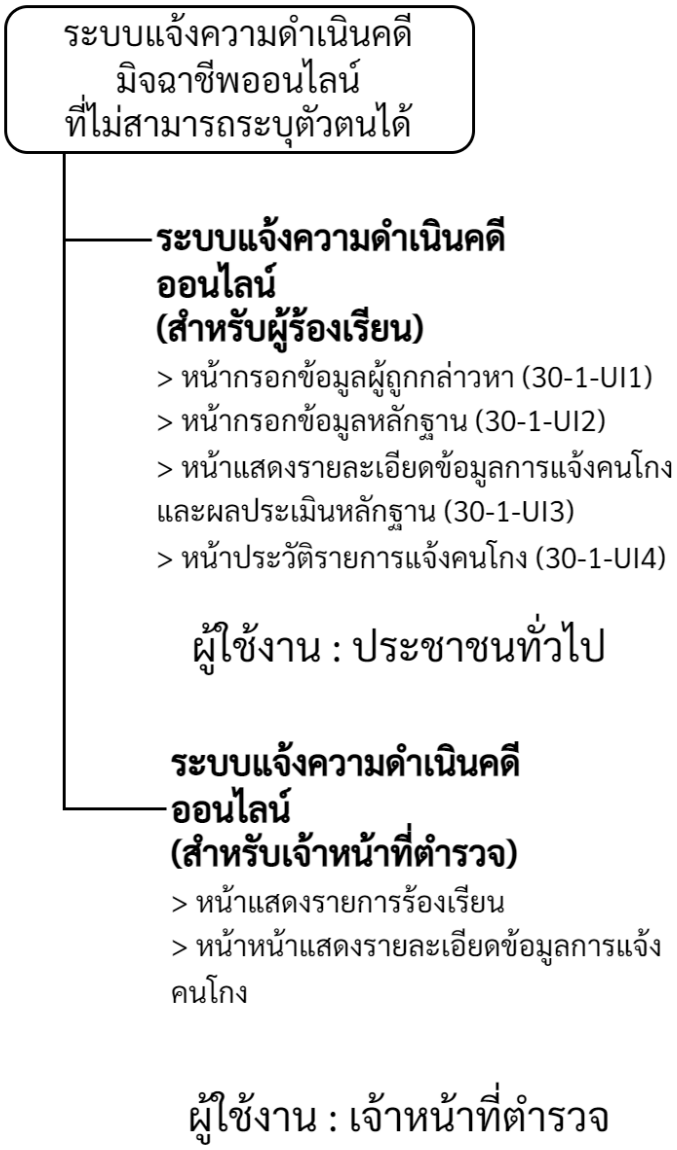


รูปที่ 6-16 ระบบค้นหาข้อมูลผู้กระทำความผิด (20)

โครงสร้างข้อมูลของระบบค้นหาข้อมูลผู้กระทำความผิด มีรายละเอียดดังนี้

- หน้ากรอกข้อมูลบัญชีธนาคาร เพื่อค้นหาข้อมูลผู้กระทำความผิด มีไว้เพื่อให้ผู้ใช้งานทั่วไปเข้ามาสืบค้นข้อมูลของผู้ที่ต้องการทำธุรกรรมด้วย ว่าเคยมีประวัติการถูกร้องเรียนหรือไม่ โดยสามารถสืบค้นได้หลากหลายช่องทาง ได้แก่ เลขบัญชีธนาคาร ชื่อบัญชีธนาคาร นอกจากนี้ยังรวมถึงเลขบัญชีพร้อมเพย์หรือบัญชีทรูมันนี่ อีกด้วย
- หน้าแสดงผลการค้นหาข้อมูล ผู้กระทำความผิด จะแสดงผลข้อมูลของบัญชีที่ได้ทำการค้นหา โดยจะแสดงใน 2 รูปแบบ คือ “บัญชีนี้ไม่พบเรื่องร้องเรียน” “บัญชีนี้พบเรื่องร้องเรียน” ซึ่งจะเป็นการเตือนให้ผู้ซื้อมีความระมัดระวังในการซื้อขายเพิ่มมากขึ้น

3) ระบบแจ้งความดำเนินคดีมิจฉาชีพออนไลน์ที่ไม่สามารถระบุตัวตนได้ เป็นระบบสำหรับให้ผู้เสียหายแจ้งเรื่องร้องเรียนที่เกิดจากมิจฉาชีพออนไลน์ โดยสามารถบันทึกข้อมูลหลักฐานทางอิเล็กทรอนิกส์ต่าง ๆ เพื่อประกอบสำนวนการดำเนินคดี เพื่อให้เจ้าหน้าที่ที่เกี่ยวข้องสามารถเข้ามาตรวจสอบพยานหลักฐานของผู้แจ้งความในเบื้องต้นก่อนตัดสินใจรับแจ้งความและสามารถตรวจสอบประวัติผู้ถูกกล่าวหาเพื่อพิจารณาแนวทางในการดำเนินคดีต่อไป



รูปที่ 6-17 ระบบแจ้งความดำเนินคดีมิจฉาชีพออนไลน์ที่ไม่สามารถระบุตัวตนได้ (30)

โครงสร้างข้อมูลของระบบแจ้งความดำเนินคดีมิจฉาชีพออนไลน์ ที่ไม่สามารถระบุได้ แบ่งออกเป็น 2 ส่วน ส่วนสำหรับประชาชนทั่วไป และส่วนสำหรับเจ้าหน้าที่ตำรวจ มีรายละเอียดดังนี้

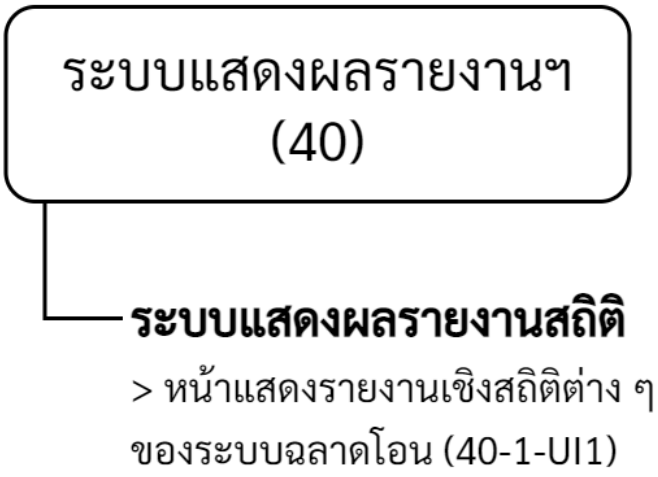
ส่วนสำหรับประชาชนทั่วไป

- หน้ากรอกข้อมูลผู้ถูกกล่าวหา มีไว้สำหรับกรอกข้อมูลของเรื่องที่ต้องการร้องเรียน แบ่งข้อมูลออกเป็น 3 ส่วน ได้แก่

(1) ข้อมูลผู้ถูกกล่าวหา ประกอบด้วย ชื่อ นามสกุล เลขบัตรประชาชน และเลขหมายโทรศัพท์ของผู้ถูกกล่าวหา
(2) เหตุการณ์ ประกอบด้วย ช่องทางที่พบ รายละเอียดช่องทางที่พบเห็น ประเภทของเรื่องร้องเรียน และรายละเอียดเรื่องราวที่ประสบเหตุ
(3) ข้อมูลการชำระเงิน ประกอบด้วย ประเภทการชำระเงิน ชื่อธนาคาร เลขบัญชีธนาคาร ชื่อบัญชีธนาคาร วันที่โอนเงิน เวลาที่โอนเงิน จำนวนยอดเงินที่โอน

- หน้ากรอกข้อมูลหลักฐาน มีไว้สำหรับอัปโหลดหลักฐานที่เป็นรูปภาพเข้าระบบ ประกอบด้วยหลักฐานการชำระเงิน หลักฐานการสนทนา รูปภาพสินค้า และบัตรประชาชนผู้ถูกกล่าวหา โดยจะให้ลงชื่อยอมรับเงื่อนไขและข้อตกลง ก่อนส่งข้อมูลเข้าระบบ
- หน้าแสดงรายละเอียดข้อมูลการแจ้งคนโกงและผลประเมินหลักฐาน จะแสดงข้อมูลสรุปจากรายการร้องเรียนที่ส่งเข้าระบบ พร้อมกับผลการประเมินหลักฐาน
- หน้าประวัติรายการแจ้งคนโกง จะแสดงรายการร้องเรียนทั้งหมดที่ผู้ใช้งานได้เคยแจ้งร้องเรียนผ่านระบบเอาไว้

4) ระบบแสดงผลรายงานฯ เป็นระบบแสดงผลรายงานเกี่ยวกับจำนวนผู้ใช้งาน ผู้ลงทะเบียนและยืนยันตัวตน รวมถึงสถิติของการแจ้งความที่ถูกแจ้งเข้ามาผ่านระบบ



รูปที่ 6-18 ระบบแสดงผลรายงานฯ (40)

โครงสร้างข้อมูลของระบบแสดงผลรายงานฯ ประกอบ 4 ส่วน ดังนี้

- ส่วนที่ 1 ส่วนแสดงจำนวนสถิติของจำนวนรายการตรวจสอบ จำนวนสมาชิกทั้งหมด จำนวนสมาชิกที่ยืนยันตัวตนสำเร็จ และจำนวนรายการแจ้งคนโกงทั้งหมด
- ส่วนที่ 2 ส่วนแสดงรายการตรวจสอบบัญชีของผู้รับโอนของผู้ใช้งาน และสัดส่วนจำนวนการตรวจสอบบัญชีแยกตามชื่อและเลขที่บัญชี
- ส่วนที่ 3 ส่วนแสดงจำนวนของผู้ใช้งานที่ลงทะเบียนและยืนยันตัวตนสำเร็จ และสัดส่วนสมาชิกแยะตามระดับผู้ใช้งาน
- ส่วนที่ 4 จำนวนรายการแจ้งคนโกงของผู้ใช้งาน สัดส่วนจำนวนรายการแจ้งคนโกงแยกตามประเภทการถูกโกง และสัดส่วนจำนวนรายการชำระเงินแยกตามช่องทางการชำระเงิน

ตารางที่ 6-1 ตารางแสดงรายละเอียดข้อมูลระบบต้นแบบฯ

ข้อมูลระบบงานหลัก	ข้อมูลระบบงานย่อย	หน้าจอและรายละเอียด	คำอธิบาย
ระบบลงทะเบียนและยืนยันตัวตน (รหัสระบบ 10)	(1) บันทึกข้อมูลสำหรับลงทะเบียน (2) ยืนยันตัวตนระดับผู้ใช้งาน (3) สร้างQR Code สำหรับตรวจสอบสมาชิก	10-1-UI1 หน้าจอสำหรับกรอกข้อมูลเลขหมายโทรศัพท์ 10-1-UI2 หน้าจอสำหรับกรอกรหัส OTP 10-2-UI1 หน้าจอแสดงสถานะการยืนยันตัวตน 10-3-UI1 หน้าจอสำหรับอัปโหลดบัตรประชาชนเพื่อยืนยันตัวตน 10-3-UI2 หน้าจอสำหรับอัปโหลดภาพใบหน้าบุคคลเพื่อยืนยันตัวตน 10-3-UI3 หน้าจอสำหรับอัปโหลดบัญชีธนาคารเพื่อยืนยันตัวตน	ส่วนบันทึกข้อมูลสำหรับการเข้าใช้งานระบบ
ระบบสืบค้นข้อมูลผู้กระทำความผิด (รหัสระบบ 20)	(1) ค้นหาข้อมูลประวัติผู้กระทำความผิด (2) ตรวจสอบข้อมูลสมาชิก (3) การออกเอกสารขอความร่วมมือจากหน่วยงานภายนอก	30-1-UI1 หน้าจอแสดงการค้นหาข้อมูลผู้ลงทะเบียนจากการกรอกข้อมูล 30-1-UI2 หน้าจอแสดงผลการค้นหาข้อมูลจากชื่อบัญชีหรือเลขที่บัญชีธนาคาร 30-1-UI3 หน้าจอแสดงผลการค้นหาข้อมูลจากคิวอาร์โค้ด	ส่วนค้นหาข้อมูลผู้ลงทะเบียนจากชื่อบัญชีธนาคาร, เลขที่บัญชีธนาคาร, พร้อมเพย์ และคิวอาร์โค้ด
ระบบแจ้งความดำเนินคดีมิจฉาชีพออนไลน์ที่ไม่สามารถระบุตัวตนได้	(1) บันทึกข้อมูลแจ้งความดำเนินคดีเบื้องต้น (2) พิจารณาความ	30-1-UI1 หน้าจอสำหรับกรอกข้อมูลผู้ถูกกล่าวหา 30-1-UI2 หน้าจอ	ส่วนบันทึกข้อมูลแจ้งความดำเนินคดีเบื้องต้น, ตรวจสอบเพื่อพิจารณารับแจ้งความ, พิจารณาคดี และการติดตาม

ข้อมูลระบบงานหลัก	ข้อมูลระบบงานย่อย	หน้าจอและรายละเอียด	คำอธิบาย
(รหัสระบบ 30)	เป็นไปได้	สำหรับกรอกข้อมูลหลักฐาน 30-1-UI3 หน้าจอสำหรับแสดงรายละเอียดการรายงานผู้ถูกกล่าวหา 30-1-UI4 หน้าประวัติรายการแจ้งคนโกง	สถานะคดี
ระบบแสดงผลรายงานฯ (รหัสระบบ 40)	รายงานผลสำหรับตนเอง	40-1-UI1 หน้าจอแสดงรายงานเชิงสถิติต่าง ๆ ของระบบฉลาดโอน	ส่วนแสดงรายงานเชิงสถิติของระบบฉลาดโอน

6.4 การออกแบบองค์ประกอบอื่น ๆ ที่เกี่ยวข้อง

6.4.1 ชื่อของระบบฯ

ระบบต้นแบบฯ “ระบบป้องกันและปราบปรามมิจฉาชีพออนไลน์ที่ไม่ระบุตัวตน” หรือภาษาอังกฤษเรียกว่า “Unidentified Scammer Prevention and Suppression” เป็นระบบที่ทางคณะผู้วิจัยได้ร่วมมือกับหน่วยงานภาคส่วนอื่นๆ ที่ต้องการออกแบบระบบนี้ให้เป็นเสมือน Ecosystem ที่จะป้องกันและปราบปรามมิจฉาชีพออนไลน์ ดังนั้น การออกแบบชื่อของระบบต้นแบบฯ นี้ ทางคณะผู้วิจัยและเจ้าหน้าที่ตำรวจ ได้คัดเลือกชื่อและข้อความสั้นๆ หรือ Tagline เพื่อสื่อสารถึงระบบต้นแบบฯ และวัตถุประสงค์ของระบบต้นแบบฯ เป็น “ฉลาดโอน: Checkก่อนเชื่อ” เนื่องจากสามารถถ่ายทอดถึงวัตถุประสงค์สำคัญของระบบต้นแบบฯ นั่นคือ การให้ผู้บริโภคตระหนักถึงความสำคัญของข้อมูลที่ระบุตัวตนผู้ขาย รวมทั้งประวัติการกระทำความผิดของผู้ขาย ผ่านการตรวจสอบชื่อบัญชีธนาคาร และเลขบัญชีธนาคารก่อนการโอนเงินเพื่อสร้างความมั่นใจก่อนการทำธุรกรรมทุกครั้ง เพื่อป้องกันเหตุหลอกลวงจากมิจฉาชีพออนไลน์ รวมถึงร่วมสร้างสังคมปลอดภัยต่อการทำธุรกรรมออนไลน์ต่อไป

6.4.2 โลโก้ของระบบ

ทางคณะผู้วิจัย ได้สรุปแนวทางการออกแบบสัญลักษณ์ให้สอดคล้องกับชื่อระบบฉลาดโอน และข้อความสั้นๆ หรือ Tagline พร้อมทั้งยังสื่อสารถึงการตรวจสอบข้อมูลการระบุตัวตนและประวัติการกระทำความผิดของผู้รับโอนเงินเสียก่อนที่จะตัดสินใจทำธุรกรรมโอนเงิน

คณะผู้วิจัยและเจ้าหน้าที่ตำรวจ ได้คัดเลือกแบบร่างสัญลักษณ์ของระบบฉลาดโอน เป็นรูปโล่และ เครื่องหมายถูก เนื่องจากสามารถสื่อสารและถ่ายทอดถึงวัตถุประสงค์ของระบบฉลาดโอนในการป้องกันและปราบปรามมิจฉาชีพออนไลน์ที่สื่อถึงความปลอดภัยในการทำธุรกรรมซื้อ-ขายสินค้าออนไลน์ รวมทั้งร่วมสร้างสภาพแวดล้อมสังคมปลอดภัยในการทำธุรกรรมออนไลน์ ผ่านการตรวจสอบความถูกต้องของการระบุตัวตนและประวัติการกระทำความผิดของผู้ขาย ตลอดจนการตรวจสอบชื่อบัญชีธนาคารและเลขที่บัญชีธนาคารที่ต้องการโอนเงิน เพื่อให้มั่นใจก่อนทำธุรกรรมโอนเงินออนไลน์ และปลอดภัยต่อการทำธุรกรรมทุกครั้ง ดังรูปที่ 6-19

รูปที่ 6-19 สัญลักษณ์ระบบฉลาดโอนปัจจุบัน

6.4.3 แนวทางการนำเสนอบทความ

การนำเสนอระบบฉลาดโอน หรือระบบต้นแบบฯ เพื่อสนับสนุนแนวทางการป้องกันและปราบปรามมิจฉาชีพออนไลน์ อันมีวัตถุประสงค์เพื่อมุ่งเน้นให้ผู้ใช้งานระบบต้นแบบฯ หรือผู้บริโภคสินค้าออนไลน์ตระหนักถึงความสำคัญของการศึกษาและตรวจสอบข้อมูลที่ระบุถึงตัวตน รวมทั้งประวัติการกระทำความผิดของบุคคลที่ตนต้องการทำธุรกรรมโอนเงินเสียก่อน คณะผู้วิจัยจึงได้ออกแบบแนวทางการนำเสนอเนื้อหาให้เป็นไปตามแนวทางการป้องกันและปราบปรามมิจฉาชีพออนไลน์ โดยผ่านการถ่ายทอดที่มุ่งเน้นให้ผู้ใช้งานระบบต้นแบบฯ เล็งเห็นถึงความสำคัญของการตระหนักรู้ถึงความสำคัญของการตรวจสอบข้อมูลบุคคลที่ตนต้องการจะทำธุรกรรมโอนเงิน หรือทราบถึงประวัติการกระทำความผิดของบุคคลนั้น ตลอดจนชื่อบัญชีธนาคาร หรือเลขที่บัญชีธนาคารก่อนการทำธุรกรรมโอนเงินออนไลน์ รวมทั้งออกแบบส่วนการเสริมสร้างองค์ความรู้เกี่ยวกับการทำธุรกรรมออนไลน์ เพื่อให้ผู้ใช้งานระบบต้นแบบฯ ทราบถึงแนวทางการป้องกันและปราบปรามมิจฉาชีพออนไลน์ผ่านบทความที่จะให้เสริมสร้างความรู้และความเข้าใจเกี่ยวกับกฎหมายและกรณีตัวอย่างที่มีความเกี่ยวข้องกับการทำธุรกรรมออนไลน์อีกด้วย ทั้งนี้การนำเสนอระบบฉลาดโอนจะเป็นไปในแนวทางที่เป็นกันเอง หรือการนำเสนอที่สื่อถึงให้ผู้ใช้งานระบบสามารถเข้าถึงเนื้อหาบนระบบต้นแบบฯ ได้อย่างกระชับ และเข้าใจง่าย

การเสริมสร้างองค์ความรู้ที่เกี่ยวข้องกับการทำธุรกรรมออนไลน์ให้แก่ผู้ใช้งานระบบต้นแบบฯ ทางคณะผู้วิจัยจึงได้ออกแบบหมวดหมู่แนวทางการนำเสนอบทความ ออกเป็น 4 หมวดหมู่ ได้แก่

1) เตือนภัยไซเบอร์
2) กฎหมายน่ารู้
3) ข่าวประชาสัมพันธ์
4) ข่าวปราบปรามมิจฉาชีพ

เตือนภัยไซเบอร์

เตือนภัยไซเบอร์ในหัวข้อหมวดหมู่เตือนภัยไซเบอร์จะนำเสนอในแง่มุมของการนำเสนอผ่านเหตุการณ์ข่าวสารในปัจจุบันที่มีความเกี่ยวข้องกับการทำธุรกรรมออนไลน์ โดยมีเนื้อหาถึงเหตุการณ์ที่เกิดขึ้น ข้อสรุปของเหตุการณ์ และข้อกฎหมายที่มีความเกี่ยวข้องกับเหตุการณ์ ให้มีความเข้าใจง่ายประชาชนทั่วไปสามารถเข้าถึงสาระสำคัญของข้อกฎหมายนั้น และสามารถนำความรู้ที่เกี่ยวข้องกับข้อกฎหมายนั้นไปประยุกต์ใช้ได้ในการดำเนินชีวิต เพื่อเป็นแนวทางการป้องกันและปราบปรามมิจฉาชีพออนไลน์

กฎหมายน่ารู้

ในหัวข้อหมวดหมู่กฎหมายน่ารู้ ทางผู้วิจัยได้นำเสนอบทความในมุมมองของการนำข้อกฎหมายที่มีความเกี่ยวข้องกับการทำธุรกรรมออนไลน์มานำเสนอในแง่มุมที่เข้าใจง่าย เป็นประโยชน์ต่อประชาชนทั่วไปที่มีพฤติกรรมในการซื้อ-ขายสินค้าออนไลน์ หรือให้ความสนใจต่อขั้นตอนการค้นหาบัญชีผู้กระทำความผิด เพื่อเสริมสร้างองค์ความรู้ และเสริมสร้างความมั่นใจก่อนการทำธุรกรรมโอนเงินออนไลน์

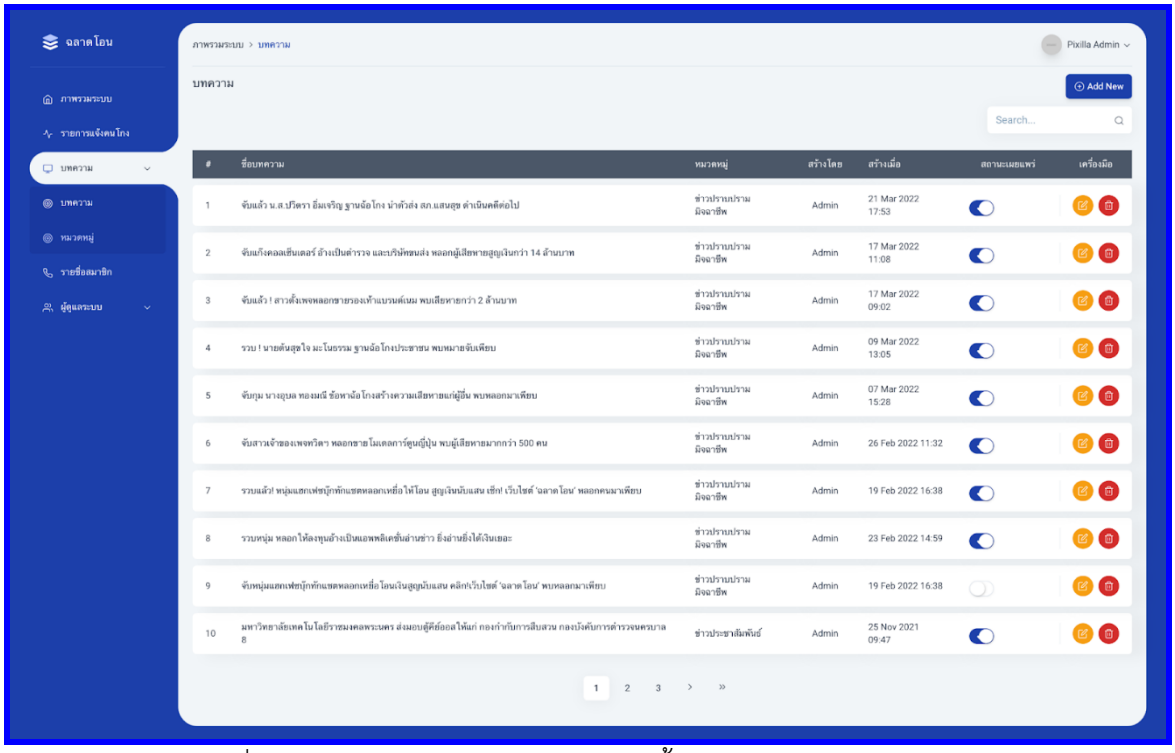
ข่าวประชาสัมพันธ์

ในหัวข้อหมวดหมู่ข่าวประชาสัมพันธ์ มีการนำเสนอข่าวต่างๆ ที่เกี่ยวข้องของโครงการ ซึ่งเป็นข้อมูลเพื่อประชาสัมพันธ์ให้ประชาชนทั่วไปได้เข้าใจถึงที่มา และวัตถุประสงค์ของโครงการ ไม่ว่าจะเป็นเรื่องที่เกี่ยวกับการจัดสัมมนา การประชุมปรึกษาหารือเกี่ยวกับแนวทางการพัฒนาของโครงการ เป็นต้น

ข่าวปราบปรามมิจฉาชีพ

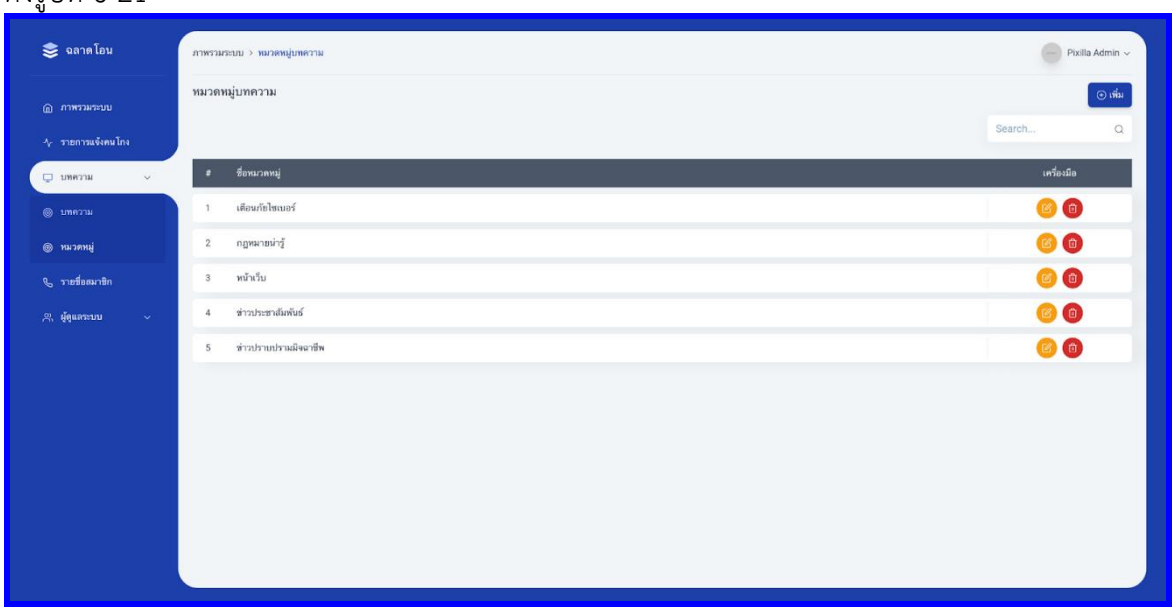
ในหัวข้อหมวดหมู่ข่าวปราบปรามมิจฉาชีพ เป็นหัวข้อที่นำเสนอเกี่ยวกับการจับกุมผู้กระทำความผิดของเจ้าหน้าที่ตำรวจ ที่ได้รับข้อมูลการกระทำความผิดจากระบบต้นแบบฯ ในการขยายผลเพื่อติดตามจับกุมผู้กระทำความผิด

โดยหน้าบทความจะแบ่งเป็น 2 ส่วนคือ บทความและหมวดหมู่ ส่วนแรกเป็นบทความต่าง ๆ ที่ได้มีการเขียนไว้ทั้งหมด แสดงรายละเอียดเป็นตารางประกอบด้วย ชื่อบทความ หมวดหมู่ สร้างโดย สร้างเมื่อ สถานะการเผยแพร่ และเครื่องมือ ดังรูปที่ 6-20



รูปที่ 6-20 หน้าจอแสดงรายการบทความทั้งหมดบนเว็บไซต์ฉลาดโอน

ในส่วนของหมวดหมู่บทความจะแสดงหมวดหมู่ของบทความที่มีอยู่และสามารถเพิ่ม หรือแก้ไขได้ ดังรูปที่ 6-21



รูปที่ 6-21 หน้าจอแสดงหมวดหมู่ของบทความบนเว็บไซต์ฉลาดโอน

ข้อมูล Term of Agreement

เว็บไซต์ฉลาดโอน ได้มีการจัดเก็บข้อมูลส่วนตัวที่สามารถระบุตัวตนของบุคคล รวมทั้งยังมีการร้องเรียน และอ้างถึงบุคคลอื่น ทางคณะผู้วิจัยจึงได้มีการกำหนดข้อตกลงการใช้งานเว็บไซต์ฉลาดโอนไว้ โดยแบ่งออกเป็น 3 ส่วน ได้แก่

1) นโยบายคุกกี้
   เว็บไซต์ฉลาดโอนใช้คุกกี้ เพื่อบันทึกการเข้าเยี่ยมชมและสมัครเข้าใช้งานเว็บไซต์ของผู้ใช้งาน โดยทำให้สามารถจดจำการใช้งานเว็บไซต์ได้ง่ายขึ้น และข้อมูลเหล่านี้จะถูกนำไปเพื่อปรับปรุงเว็บไซต์ให้ตรงกับความต้องการของผู้ใช้งานเพื่ออำนวยความสะดวกในการใช้งานเว็บไซต์เงื่อนไขข้อตกลงและนโยบายการคุ้มครองข้อมูลส่วนบุคคล
2) เงื่อนไขข้อตกลงการใช้งานเว็บไซต์ฉลาดโอน
   ทางคณะผู้วิจัยได้กำหนดเนื้อหาในส่วนของเงื่อนไขข้อตกลงการใช้งานเว็บไซต์ฉลาดโอน และนโยบายความเป็นส่วนตัว โดยเงื่อนไขข้อตกลงจะกล่าวถึงที่มาของโครงการพัฒนาระบบต้นแบบฯ ตลอดจนขอบเขตการดำเนินงานของระบบฉลาดโอน และเนื้อหาในส่วนของนโยบายการคุ้มครองข้อมูลส่วนบุคคล ได้กล่าวถึงการใช้งาน การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล การเชื่อมโยงข้อมูล ตลอดจนการตรวจสอบและการแก้ไขข้อมูลเงื่อนไขข้อตกลงแจ้งความดำเนินคดีมิจฉาชีพออนไลน์ที่ไม่สามารถระบุตัวตน
3) เงื่อนไขและข้อตกลงของการแจ้งความดำเนินคดีมิจฉาชีพออนไลน์ที่ไม่สามารถระบุตัวตน
   ทางคณะผู้วิจัยได้มีการกำหนดเงื่อนไขและข้อตกลงของการแจ้งความดำเนินคดีมิจฉาชีพออนไลน์ที่ไม่สามารถระบุตัวตน ผ่านการแจ้งเรื่องร้องเรียนที่เกิดจากมิจฉาชีพออนไลน์ โดยการบันทึกข้อมูลหลักฐานทางอิเล็กทรอนิกส์ต่าง ๆ เพื่อประกอบสำนวนการดำเนินคดี ซึ่งในเนื้อหาในส่วนนี้ ทางคณะผู้วิจัยได้ศึกษาข้อมูลข้อกำหนดจากหน่วยงานอื่นๆ ที่มีลักษณะ

ใกล้เคียงกับเว็บไซต์ฉลาดโอน จากการศึกษาคณะผู้วิจัยจึงได้อ้างอิงข้อมูลเงื่อนไขข้อตกลงในการแจ้งความดำเนินคดีมิจฉาชีพออนไลน์ที่ไม่สามารถระบุตัวตน จากสำนักงานคณะกรรมการคุ้มครองผู้บริโภค (สคบ.)

6.4.5 การทำความร่วมมือกับหน่วยงานอื่น ๆ

ระบบต้นแบบฯ หรือ ระบบฉลาดโอน ได้รับการพัฒนาโดยมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร ร่วมกับ กองกำกับการสืบสวน กองบังคับการนครบาล 8 โดยได้รับสนับสนุนจากสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ และกองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะ

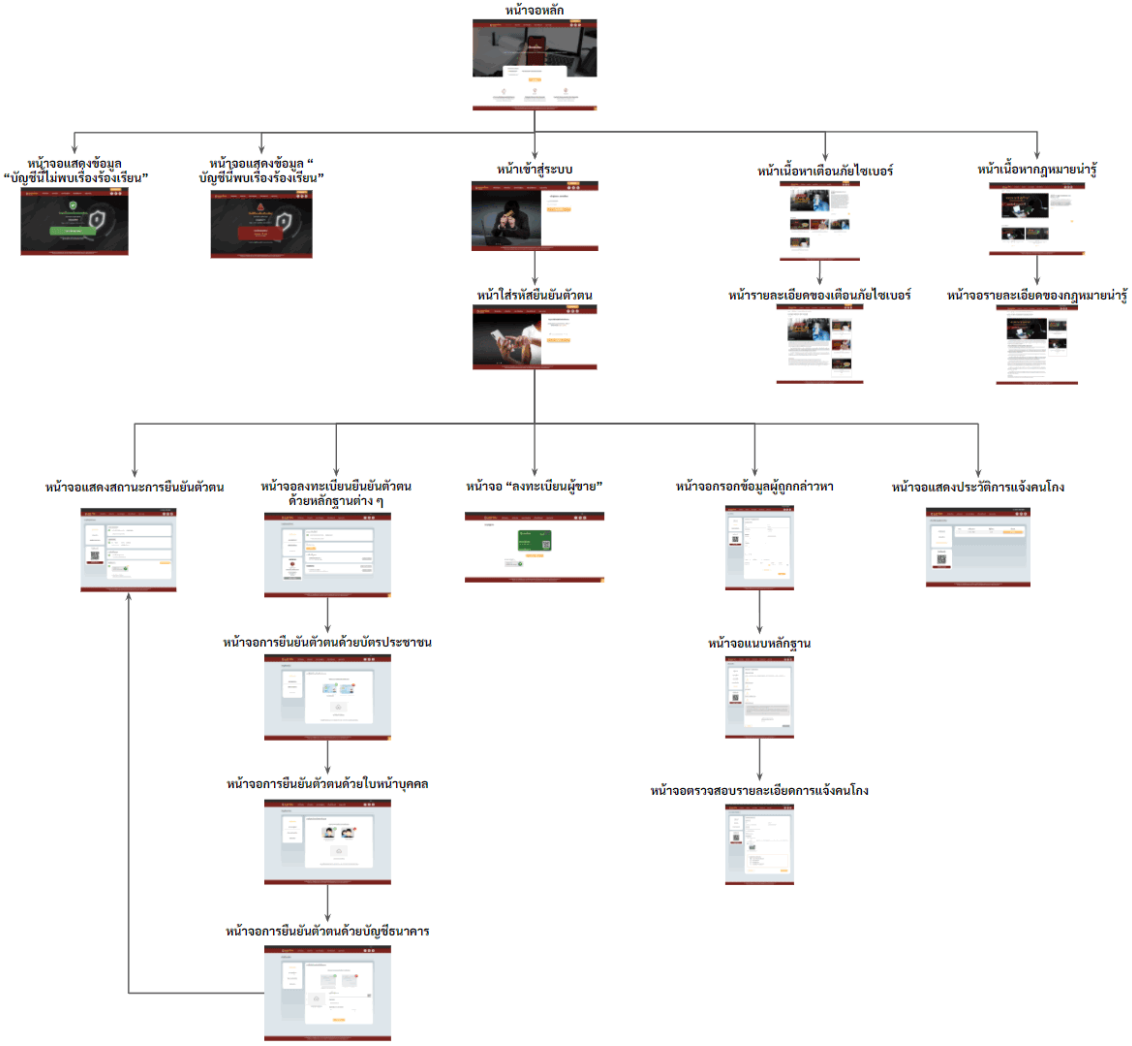
สัญลักษณ์	ชื่อหน่วยงาน
กสทช.	สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ
กทปส.	กองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะ
กองกำกับการสืบสวน ตำรวจนครบาล ๘ พิทักษ์สันติราษฎร์	กองกำกับการสืบสวน กองบังคับการนครบาล 8

สัญลักษณ์	ชื่อหน่วยงาน
	มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร
	คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร

ทางคณะผู้วิจัย ได้พัฒนาเว็บไซต์ระบบฉลาดโอน เพื่อให้ประชาชน หรือผู้ใช้งานระบบต้นแบบฯ ขึ้น เพื่อให้การใช้งานเป็นไปได้อย่างสะดวก และรวดเร็ว โดยเว็บไซต์ฉลาดโอนนี้ จะแบ่งออกเป็น 4 เมนูหลัก ได้แก่

1) เช็กก่อนโอน หรือ ระบบค้นหาข้อมูลผู้กระทำความผิด สำหรับให้ประชาชนตรวจสอบข้อมูลผู้กระทำความผิด ผ่านชื่อบัญชีธนาคาร หรือเลขที่บัญชีธนาคาร
2) เช็กตัวตนผู้ขาย หรือ ระบบค้นหาผู้กระทำความผิด ในส่วนของการตรวจสอบผู้ขายที่มีการลงทะเบียนยืนยันตัวตนกับระบบต้นแบบ
3) แจ้งคนโกง หรือ ระบบแจ้งความดำเนินคดีมิจฉาชีพออนไลน์ที่ไม่สามารถระบุตัวตน สำหรับให้ประชาชนสามารถแจ้งเรื่องร้องเรียนที่เกิดจากมิจฉาชีพออนไลน์ โดยการบันทึกข้อมูลหลักฐานทางอิเล็กทรอนิกส์ต่าง ๆ เพื่อเตือนภัยต่อผู้อื่นในส่วนระบบค้นหาข้อมูลผู้กระทำความผิดต่อไป
4) ช่วยรวบรวมหลักฐาน หรือระบบแจ้งความดำเนินคดีออนไลน์ที่ไม่สามารถสามารถระบุตัวตน สำหรับเตรียมเอกสารประกอบการแจ้งความดำเนินคดีเพื่อให้ผู้ใช้บริการนำเอกสารประกอบการแจ้งความนี้ไปแจ้งความดำเนินคดีกับเจ้าหน้าที่ตำรวจ

โดยเว็บไซต์ฉลาดโอนมีแผนผังเว็บไซต์ ดังนี้



รูปที่ 6-22 ภาพแผนผังหน้าจอเว็บไซต์ของเว็บฉลาดโอนดอทคอม

บทที่ 7
ผลการพัฒนาระบบป้องกันและปราบปรามมิจฉาชีพออนไลน์ที่ไม่ระบุตัวตน

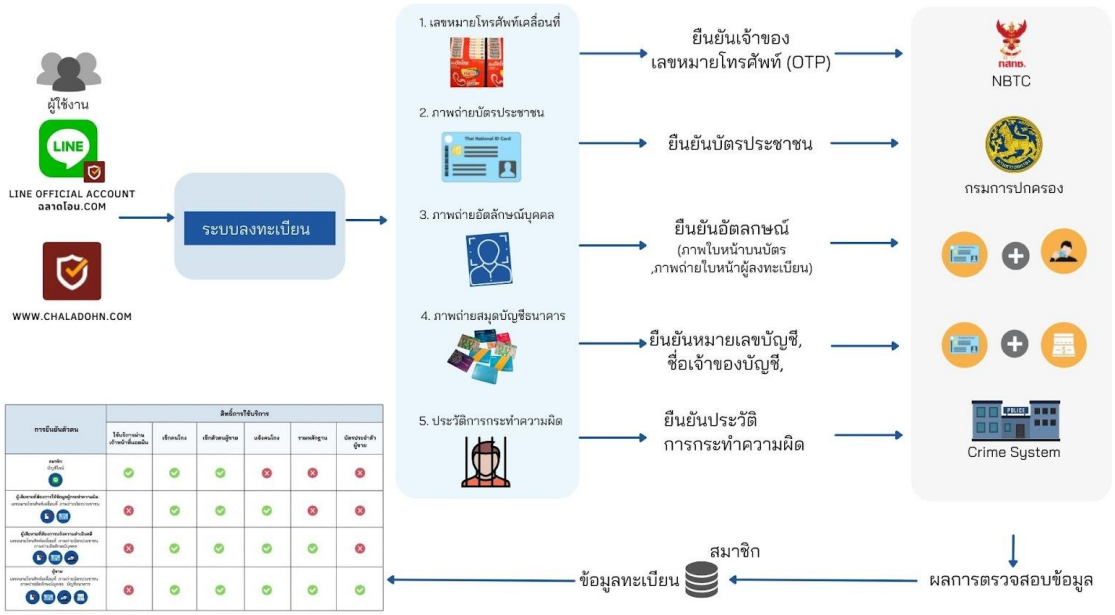
บทที่ 7 นี้ จัดทำขึ้นเพื่อแสดงรายละเอียดของผลการพัฒนาระบบป้องกันและปราบปรามมิจฉาชีพออนไลน์ที่ไม่สามารถระบุตัวตนได้ ตามที่ได้มีการวิเคราะห์ ออกแบบ ระบบต้นแบบฯนี้ไว้ เพื่อให้ทราบถึงกระบวนการทำงานของแต่ละระบบย่อยภายในระบบต้นแบบฯนี้

7.1 การพัฒนาระบบลงทะเบียนและยืนยันตัวตน

ระบบการลงทะเบียนและการยืนยันตัวตน เป็นระบบสำหรับให้ผู้ใช้งานสามารถเข้ามาใช้บริการต่าง ๆ อาทิ การตรวจสอบบัญชีผู้กระทำความผิด การตรวจสอบบัญชีผู้ขายที่ยืนยันตัวตน การแจ้งความดำเนินคดีออนไลน์ ตลอดจนการรวบรวมเอกสารหลักฐานประกอบการแจ้งความ ผ่านระบบต้นแบบฯ โดยการใช้งานผู้ใช้งานจำเป็นต้องยืนยันตัวตน เพื่อเป็นการระบุตัวตนว่าด้วยการพิสูจน์และยืนยันตัวตน เพื่อช่วยลดความเสี่ยงจากเหตุการณ์ฉ้อโกงออนไลน์ รวมทั้งสร้างความมั่นใจในความปลอดภัยต่อการทำธุรกรรม ให้กับผู้ทำธุรกรรม

7.1.1 แนวทางการลงทะเบียนและยืนยันตัวตน

สำหรับการใช้งานระบบต้นแบบฯ ผู้ใช้งานต้องทำการลงทะเบียนและยืนยันตัวตนก่อนเป็นอันดับแรก จากนั้นจึงจะสามารถเข้าใช้งานระบบต้นแบบฯ ในส่วนอื่น ๆ ต่อได้ และเพื่อให้เป็นไปตามข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยมีขั้นตอนการลงทะเบียนและยืนยันตัวตน แสดงดังรูปที่ 7-1



รูปที่ 7-1 ภาพรวมขั้นตอนการลงทะเบียนและยืนยันตัวตน

สำหรับการใช้งานระบบต้นแบบฯ ผู้ใช้งานต้องลงทะเบียนและยืนยันตัวตนเพื่อเข้าใช้งานระบบต้นแบบฯ ซึ่งการใช้งานระบบต้นแบบฯ สามารถเข้าใช้งานได้จาก 2 ช่องทาง คือ ช่องทางเว็บไซต์ฉลาดโอนดอทคอมที่ผู้ใช้งานสามารถใช้บริการได้ด้วยตนเอง และช่องทาง LINE Official Account ฉลาดโอน.com ที่จะมีเจ้าหน้าที่อำนวยความสะดวกในการใช้งานให้กับผู้ใช้งาน โดยระบบต้นแบบฯ จะแบ่งการยืนยันตัวตน ออกเป็น 5 ระดับ ดังรูปที่ 7-2 ได้แก่

ระดับ 1 สมาชิก

ช่องทาง LINE Official Account ฉลาดโอน.com

หลักฐานที่ใช้ : บัญชีไลน์

บริการที่สามารถใช้ได้ :

- สอบถามข้อมูลกับเจ้าหน้าที่แอดมินฉลาดโอนและแชทบอท

ระดับ 2 ผู้ให้ข้อมูลผู้กระทำความผิด

หลักฐานที่ใช้ : เลขหมายโทรศัพท์เคลื่อนที่ ผ่านรหัสผ่านครั้งเดียว (One Time Password : OTP) และภาพถ่ายบัตรประชาชน

บริการที่สามารถใช้ได้ :

- ตรวจสอบข้อมูลการกระทำผิดของบุคคลที่ต้องการทำธุรกรรม
- ตรวจสอบข้อมูลผู้ขายหรือผู้รับโอนที่มีการยืนยันตัวตนกับฉลาดโอน
- แจ้งรายชื่อผู้กระทำความผิดกับฉลาดโอน

ระดับ 3 ผู้เสียหายที่ต้องการแจ้งความดำเนินคดี

หลักฐานที่ใช้ : เลขหมายโทรศัพท์เคลื่อนที่ผ่านรหัสผ่านครั้งเดียว (One Time Password : OTP), ภาพถ่ายบัตรประชาชน และภาพถ่ายใบหน้าของผู้ลงทะเบียน

บริการที่สามารถใช้ได้ :

- ตรวจสอบข้อมูลการกระทำผิดของบุคคลที่ต้องการทำธุรกรรม
- ตรวจสอบข้อมูลผู้ขายหรือผู้รับโอนที่มีการยืนยันตัวตนกับฉลาดโอน
- สร้างเอกสารประกอบการแจ้งความดำเนินคดีฉ้อโกงออนไลน์ที่ไม่สามารถระบุตัวตนได้

ระดับ 4 ผู้ขาย หรือผู้รับโอนเงิน

หลักฐานที่ใช้ : เลขหมายโทรศัพท์เคลื่อนที่ผ่านรหัสผ่านครั้งเดียว (One Time Password : OTP), ภาพถ่ายบัตรประชาชน, ภาพถ่ายใบหน้าของผู้ลงทะเบียน และภาพถ่ายบัญชีธนาคาร

บริการที่สามารถใช้ได้ :

- ตรวจสอบข้อมูลการกระทำผิดของบุคคลที่ต้องการทำธุรกรรม
- ตรวจสอบข้อมูลผู้ขายหรือผู้รับโอนที่มีการยืนยันตัวตนกับฉลาดโอน
- แจ้งรายชื่อผู้กระทำความผิดกับฉลาดโอน
- สร้างเอกสารประกอบการแจ้งความดำเนินคดีฉ้อโกงออนไลน์ที่ไม่สามารถระบุตัวตนได้
- บัตรประจำตัวผู้ขาย เพื่อใช้การันตีตนเองกับผู้ซื้อ

การยืนยันตัวตน	สิทธิ์การใช้บริการ					
	ใช้บริการผ่านเจ้าหน้าที่แอดมิน	เช็กคนโกง	เช็กตัวตนผู้ขาย	แจ้งคนโกง	รวมหลักฐาน	บัตรประจำตัวผู้ขาย
สมาชิก บัญชีไลน์	✓	✓	✓	✗	✗	✗
ผู้เสียหายที่ต้องการให้ข้อมูลผู้กระทำความผิด เลขหมายโทรศัพท์เคลื่อนที่ ภาพถ่ายบัตรประชาชน	✗	✓	✓	✓	✗	✗
ผู้เสียหายที่ต้องการแจ้งความดำเนินคดี เลขหมายโทรศัพท์เคลื่อนที่ ภาพถ่ายบัตรประชาชน ภาพถ่ายอัตลักษณ์บุคคล	✗	✓	✓	✓	✓	✗
ผู้ขาย เลขหมายโทรศัพท์เคลื่อนที่ ภาพถ่ายบัตรประชาชน ภาพถ่ายอัตลักษณ์บุคคล บัญชีธนาคาร	✗	✓	✓	✓	✓	✓

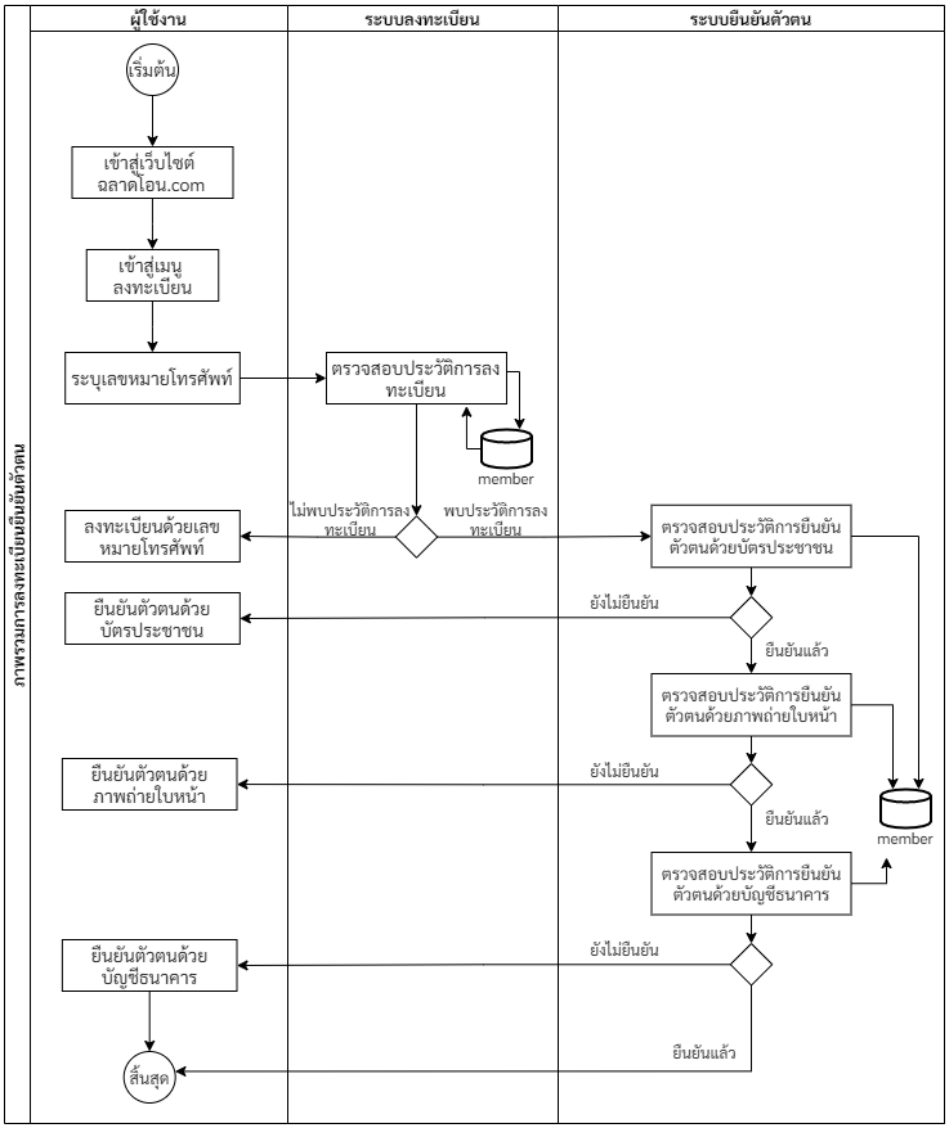
รูปที่ 7-2 ภาพรวมสิทธิ์การใช้บริการ

7.1.2 กระบวนการทำงานของระบบ

การทำงานของระบบลงทะเบียนและยืนยันตัวตน จะมีทั้งหมด 4 ขั้นตอน ได้แก่

1) การยืนยันตัวตนด้วยเลขหมายโทรศัพท์
2) การยืนยันตัวตนด้วยบัตรประจำตัวประชาชน
3) การยืนยันตัวตนด้วยรูปใบหน้า
4) การยืนยันตัวตนด้วยสมุดบัญชีธนาคาร

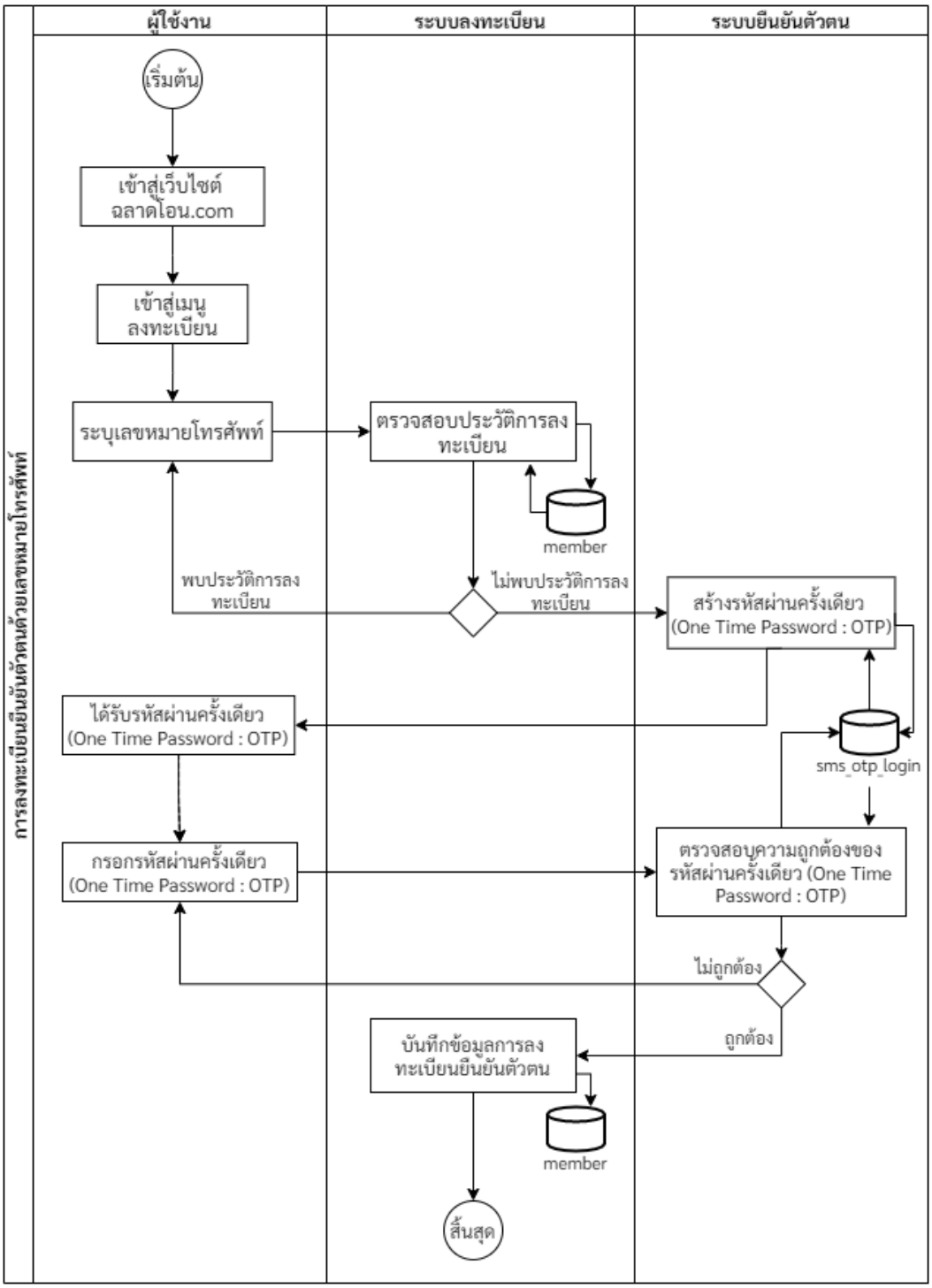
แสดงกระบวนการทำงาน ดังรูปที่ 7-3



รูปที่ 7-3 ภาพรวมขั้นตอนการยืนยันตัวตนของระบบลงทะเบียนยืนยันตัวตน

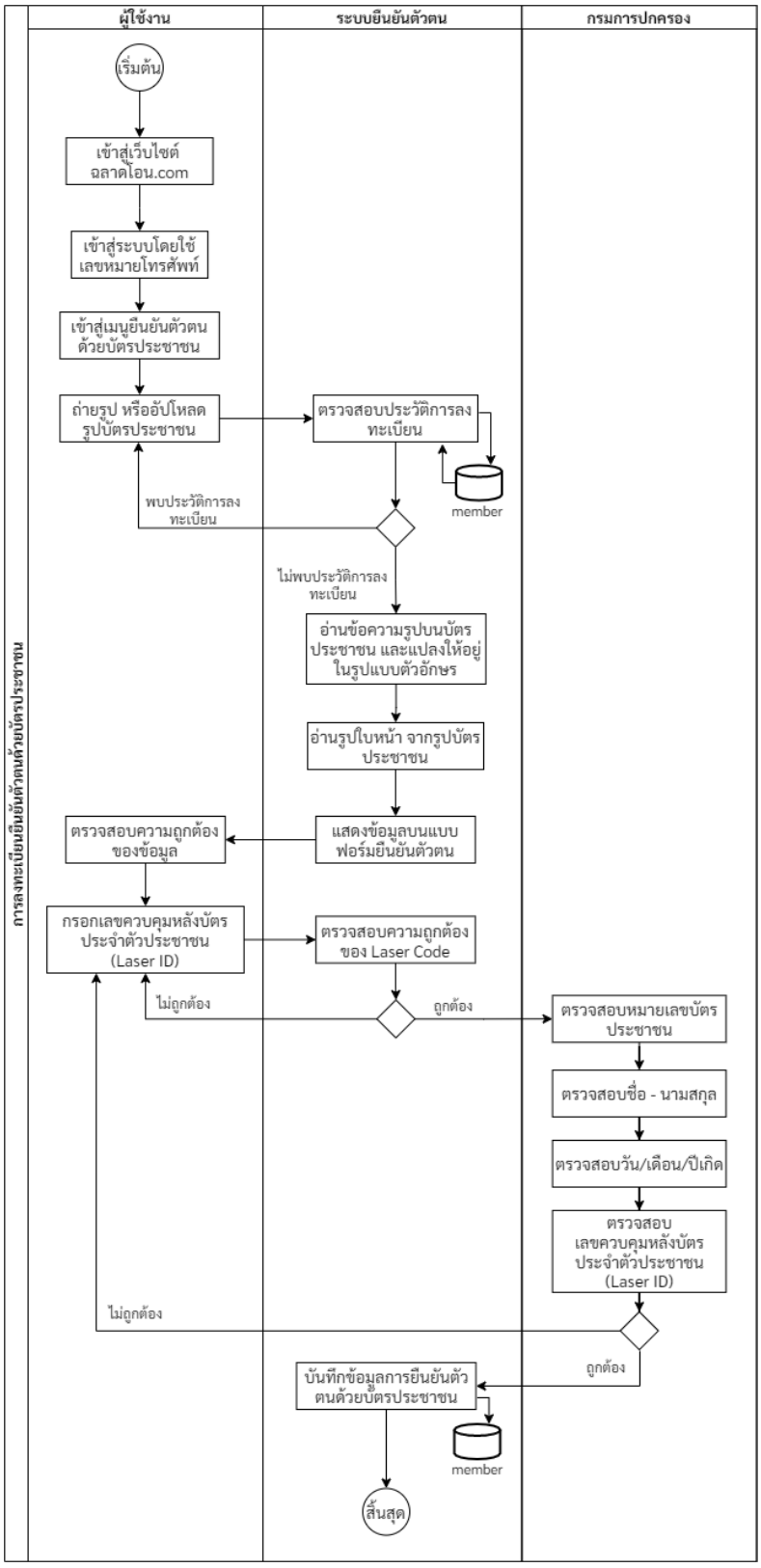
จากรูปที่ 7-3 ผู้ใช้เข้าสู่ระบบโดยใช้เลขหมายโทรศัพท์ที่ตนเองมีอยู่ เมื่อเข้าสู่ระบบสำเร็จ ระบบจะบันทึกบัญชีที่ผู้ใช้ล็อกอินเก็บเข้าฐานข้อมูล จากนั้นจะเข้าสู่ระบบยืนยันตัวตนของเว็บไซต์ โดยระบบยืนยันตัวตนจะมีทั้งหมด 3 ขั้นตอน โดยต้องทำการยืนยันตัวตนไปทีละขั้นตอน หรือเลือกที่จะยืนยันตัวตนในภายหลังก็ได้ แต่จะไม่สามารถใช้งานระบบได้เต็มรูปแบบหรือการใช้งานบางส่วนไม่สามารถใช้งานได้ เพราะต้องผ่านการยืนยันตัวตนก่อน โดยเริ่มแรกจะเป็นการยืนยันตัวตนโดยใช้เลขหมายโทรศัพท์ของผู้ใช้งาน ระบบจะให้ผู้ใช้กรอกหมายเลขโทรศัพท์เพื่อส่งรหัสผ่านครั้งเดียว (One Time Password : OTP) OTP แล้วนำ OTP ที่ได้รับมากรอก ถ้ารหัสตรงกันจะเป็นการเสร็จสิ้นการยืนยันตัวตนขั้นแรก ต่อมาเป็นการยืนยันตัวตนด้วยบัตรประชาชน ระบบจะให้ผู้ใช้อัปโหลดรูปบัตรประชาชน จากนั้นระบบจะทำการตรวจสอบว่าเป็นบัตรประชาชนจริงหรือไม่ ถ้าใช่จะให้ผู้ใช้กรอกเลขหลังบัตรประชาชนเพิ่มเติม เป็นอันเสร็จสิ้นการยืนยันตัวตนขั้นที่สอง ต่อมาเป็นการยืนยันตัวตนโดยใช้ภาพถ่ายอัตลักษณ์ ให้ผู้ใช้งาน

ทำการเซลฟี่ตนเองคู่กับบัตรประชาชนแล้วอัปโหลดรูป ระบบจะทำการตรวจสอบว่าถูกต้องหรือไม่ ถ้าถูกต้องเป็นอันเสร็จสิ้นการยืนยันตัวตนขั้นที่3 สุดท้ายการยืนยันตัวตนโดยใช้หน้าสมุดธนาคาร เมื่ออัปโหลดรูประบบจะทำการตรวจสอบ จากนั้นผู้ใช้งานจะเลือกว่าเป็นธนาคารอะไร เป็นอันเสร็จสิ้นการยืนยันตัวตนขั้นสุดท้าย ถือเป็นการสิ้นสุดกระบวนการการลงทะเบียนและยืนยันตัวตน



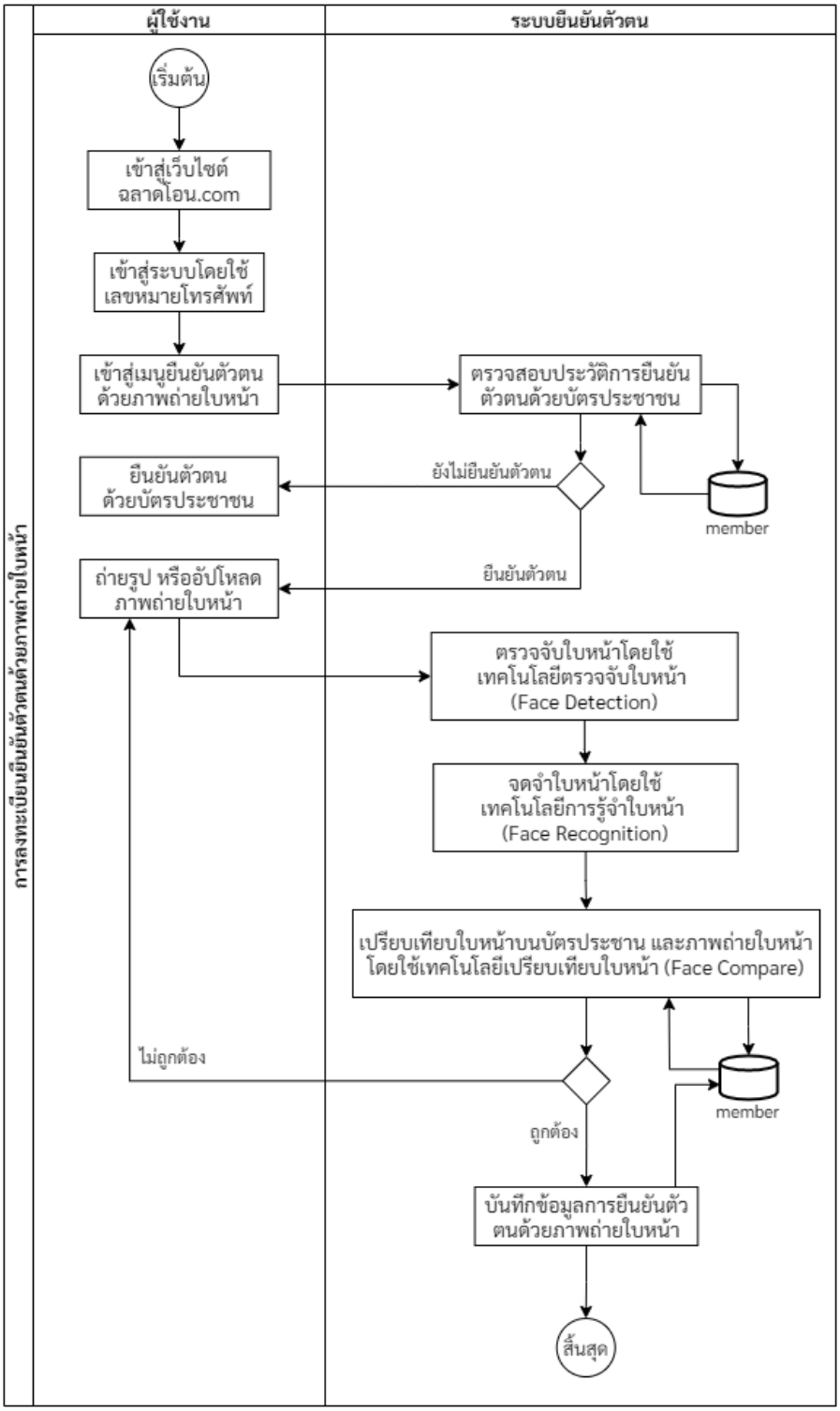
รูปที่ 7-4 ขั้นตอนการยืนยันตัวตนด้วยเลขหมายโทรศัพท์

จากรูปที่ 7-4 ผู้ใช้ลงทะเบียนและยืนยันตัวตนโดยใช้เลขหมายโทรศัพท์ที่ตนเองใช้งาน โดยกรอกเลขหมายโทรศัพท์ จากนั้นระบบจะตรวจสอบว่าเลขหมายโทรศัพท์นี้ได้มีการลงทะเบียนไว้ในระบบต้นแบบฯหรือไม่ หากพบว่ายังไม่มีการลงทะเบียน ระบบต้นแบบฯ จะสร้างรหัส OTP : One Time Password เพื่อส่งให้ผู้ใช้งานผ่าน SMS ไปที่เลขหมายโทรศัพท์นั้น หลังจากที่ผู้ใช้งานได้รับรหัส OTP : One Time Password ผู้ใช้งานต้องนำรหัส OTP : One Time Password ดังกล่าวมาใส่ในระบบต้นแบบฯ จากนั้นระบบยืนยันตัวตนจะตรวจสอบความถูกต้องของรหัส OTP : One Time Password หากรหัสดังกล่าวถูกต้องจะถือว่าลงทะเบียนและยืนยันตัวตนด้วยเลขหมายโทรศัพท์สำเร็จ



รูปที่ 7-5 ขั้นตอนการยืนยันตัวตนด้วยบัตรประชาชน

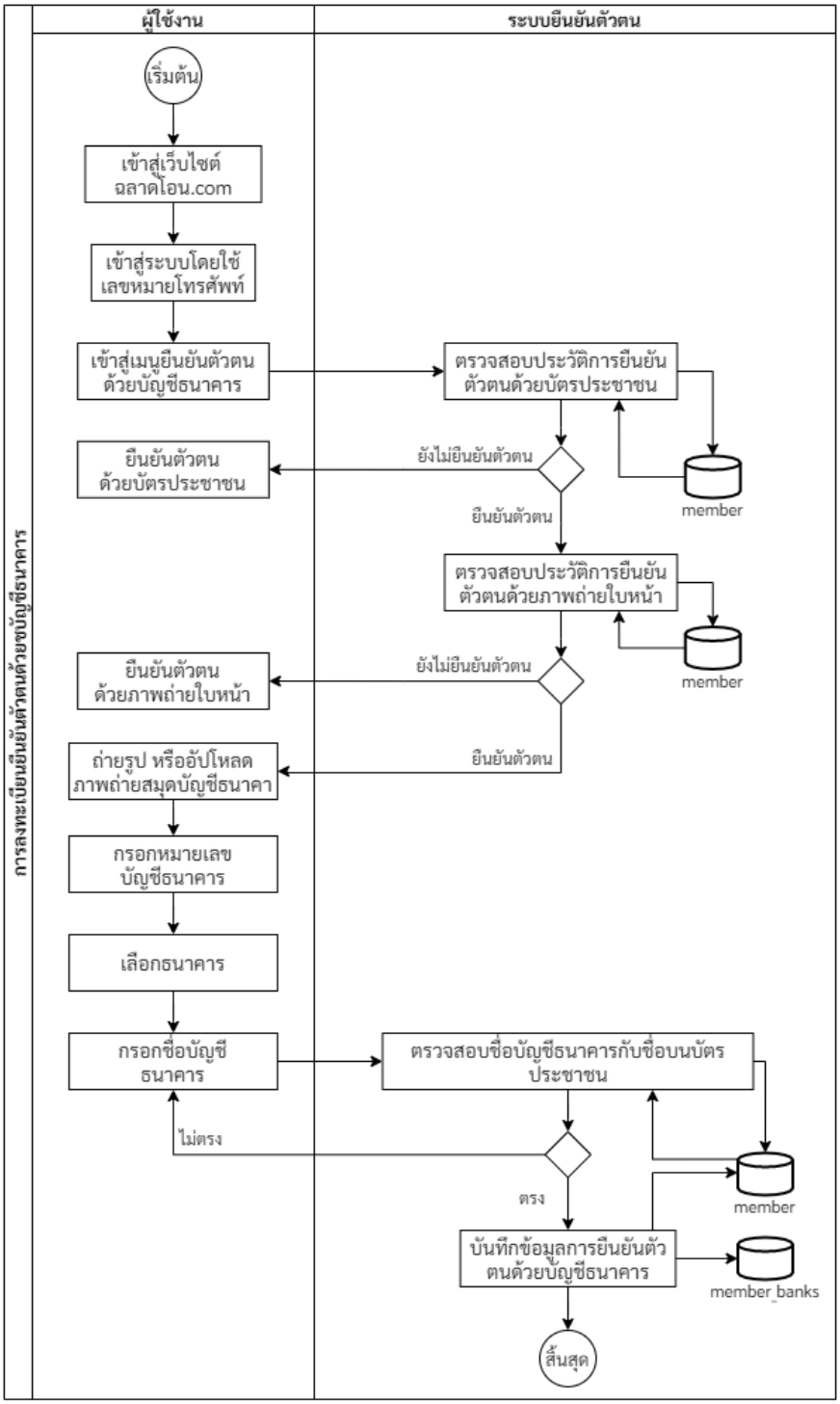
จากรูปที่ 7-5 ผู้ใช้ยืนยันตัวตนโดยใช้บัตรประจำตัวประชาชนของตนเอง โดยเริ่มจากผู้ใช้งานทำการถ่ายรูปหรืออัปโหลดรูปบัตรประจำตัวประชาชนเข้าสู่ระบบ จากนั้นระบบจะทำการ OCR : Optical Character Recognition ข้อความบนบัตรประชาชน และทำการตัดรูปใบหน้าบนบัตรประชาชนเพื่อใช้งานในขั้นตอนยืนยันตัวตนถัดไป หลังจากที่ระบบทำการ OCR:Optical Character Recognition บัตรประจำตัวประชาชนเสร็จเรียบร้อย ระบบจะให้ผู้ใช้งาน ตรวจสอบข้อมูลบนบัตรประจำตัวประชาชน และให้กรอกข้อมูลเลขเลเซอร์โค้ดที่อยู่ด้านหลังของบัตรประจำตัวประชาชน หลังจากที่ผู้ใช้งานตรวจสอบและกรอกเลขเลเซอร์โค้ดเสร็จสิ้นแล้ว จากนั้นระบบจะส่งข้อมูลดังกล่าวไปตรวจสอบความถูกต้องกับกรมการปกครองเพื่อตรวจสอบข้อมูลจากบัตรประชาชน ได้แก่ หมายเลขบัตรประชาชน, ชื่อ นามสกุล, วัน เดือน ปีเกิด และเลขควบคุมหลังบัตรประจำตัวประชาชน(Laser ID) หากตรวจสอบความถูกต้องเรียบร้อย จะถือว่าการยืนยันตัวตนด้วยบัตรประจำประชาชนสำเร็จ



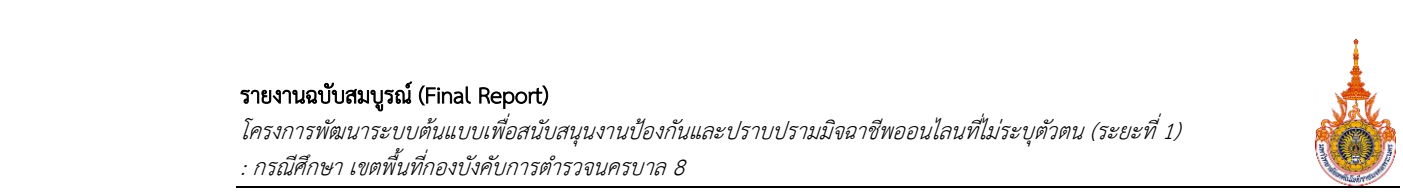
รูปที่ 7–6 ขั้นตอนการยืนยันตัวตนด้วยภาพถ่ายใบหน้า

จากรูปที่ 7-6 ผู้ใช้งานเข้าสู่ระบบ เพื่อยืนยันตัวตนด้วยภาพถ่ายใบหน้า ระบบจะตรวจสอบก่อนว่าผู้ใช้งานได้มีการยืนยันตัวตนด้วยบัตรประจำประชาชนแล้วหรือไม่ หากยังไม่มีการยืนยันตัวตน ระบบจะให้ยืนยันตัวตนด้วยบัตรประชาชนให้เรียบร้อยก่อน แต่หากได้มีการยืนยันตัวตนเรียบร้อยแล้ว ระบบจะให้

ผู้ใช้งานถ่ายรูปหรืออัปโหลดภาพถ่ายใบหน้าตนเองคู่กับบัตรประจำตัวประชาชน จากนั้นจะมีการเปรียบเทียบใบหน้าจริงของผู้ใช้งานและรูปใบหน้าบนบัตรประจำตัวประชาชน หากตรวจสอบความถูกต้องเรียบร้อยแล้ว ระบบจะบันทึกลงฐานข้อมูลผู้ยืนยันตัวตนของระบบต้นแบบฯ ซึ่งถือว่ายืนยันตัวตนด้วยภาพใบหน้าสำเร็จ



รูปที่ 7-7 ขั้นตอนการยืนยันตัวตนด้วยบัญชีธนาคาร



จากรูปที่ 7-7 ผู้ใช้งานเข้าสู่ระบบ เพื่อยืนยันตัวตนด้วยบัญชีธนาคาร ระบบจะตรวจสอบก่อนว่าผู้ใช้งานได้มีการยืนยันตัวตนด้วยภายถ่ายใบหน้าบุคคลหรืออัตลักษณ์บุคคลแล้วหรือไม่ หากยังไม่มีการยืนยันตัวตน ระบบจะให้ยืนยันตัวตนด้วยอัตลักษณ์บุคคลให้เรียบร้อยก่อน แต่หากได้มีการยืนยันตัวตนเรียบร้อยแล้ว ระบบจะให้ผู้ใช้งานถ่ายรูปหรืออัปโหลดภาพถ่ายบัญชีธนาคาร จากนั้นระบบจะให้ผู้ใช้งานกรอกเลขที่บัญชีธนาคาร เลือกชื่อธนาคารของสมุดบัญชีเล่มนั้น และกรอกชื่อบัญชีธนาคาร เมื่อกรอกข้อมูลครบถ้วนแล้ว ระบบจะตรวจสอบชื่อบัญชีธนาคารกับชื่อ นามสกุลบนบัตรประจำตัวปราชนว่าข้อมูลตรงกันหรือไม่ หากชื่อ นามสกุลตรงกันกับชื่อบัญชีธนาคาร ระบบจะบันทึกการยืนยันตัวตนลงฐานข้อมูลผู้ยืนยันตัวตนของระบบต้นแบบฯ ซึ่งถือว่ายืนยันตัวตนด้วยบัญชีธนาคารสำเร็จ

7.1.3 หน้าจอแสดงผลและรายละเอียดการทำงาน

รูปที่ 7-8 หน้าจอเข้าสู่ระบบฉลาดโอน

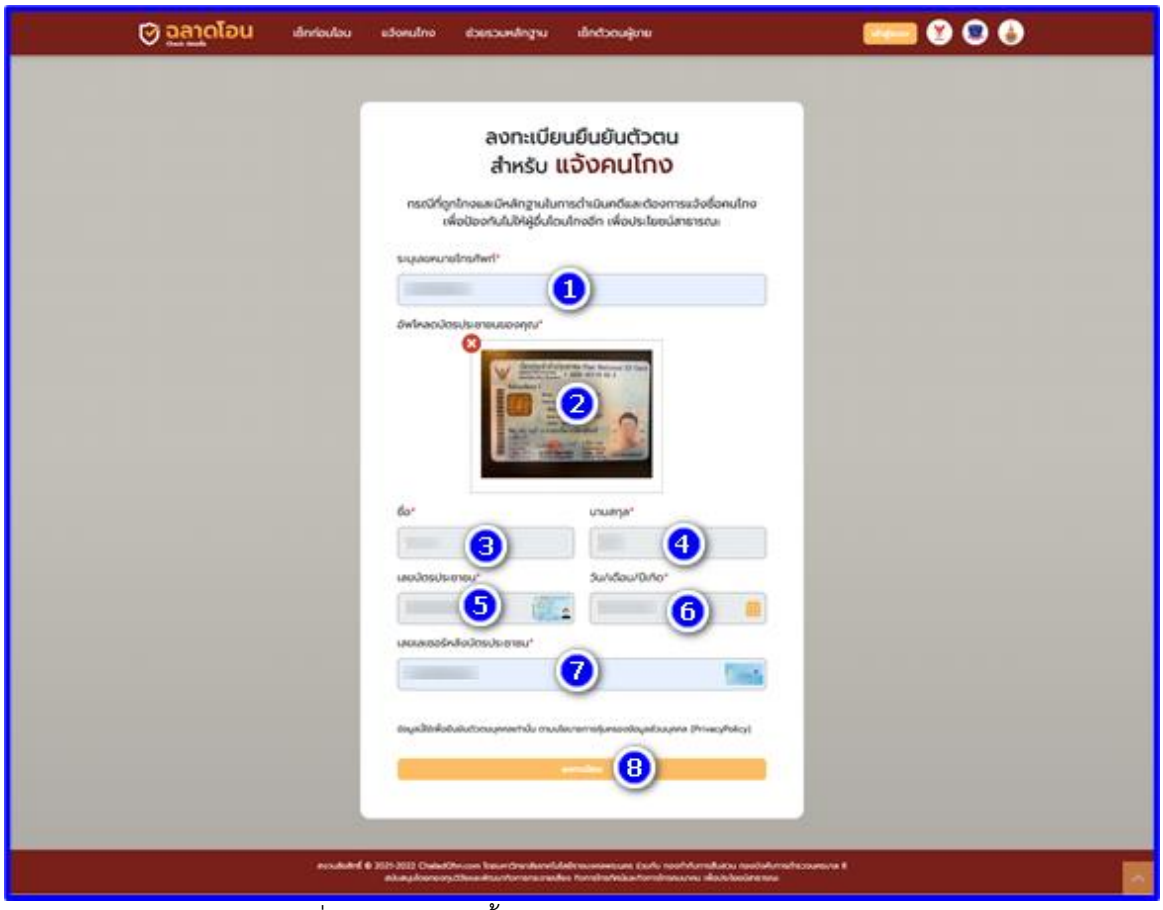
ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	สำหรับระบุเลขหมายโทรศัพท์	Yes		ระบบจะส่งรหัส OTP ไปยังเลขหมายโทรศัพท์ที่ได้กรอกไว้

รูปที่ 7-9 หน้าจอสำหรับกรอกรหัส OTP

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	สำหรับระบุเลข OTP ที่ได้รับ	Yes		ระบบจะตรวจสอบ OTP หากถูกต้อง ก็จะไปยังหน้าจอลงเบียน

รูปที่ 7-10 หน้าจอลงทะเบียนสำหรับแจ้งคนโกง

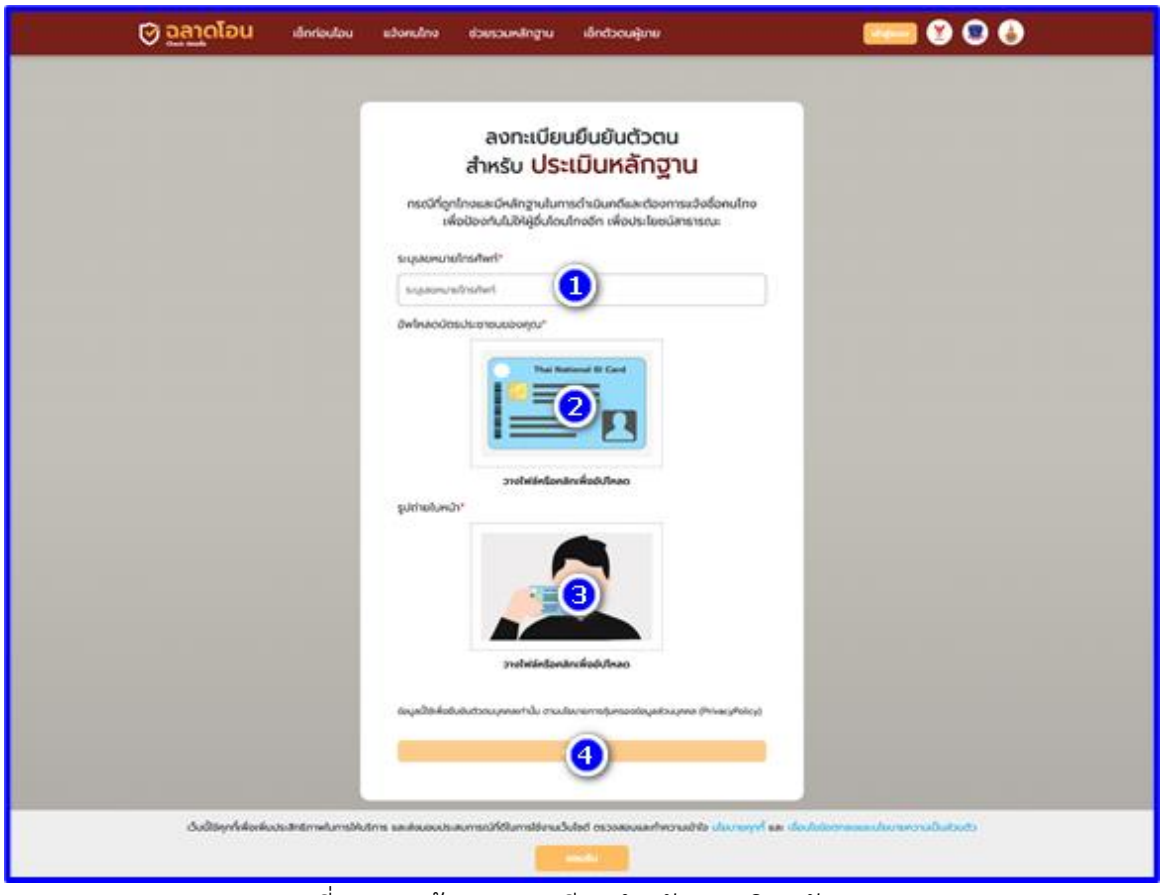
ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	สำหรับระบุเลขหมายโทรศัพท์	Yes		ระบบจะตรวจสอบเลขหมายโทรศัพท์ว่าเคยมีการลงทะเบียนไว้แล้วหรือยัง
2	สำหรับวางไฟล์หรืออัพโหลดไฟล์ภาพใบหน้าคู่กับบัตรประชาชน	Yes		ระบบจะให้อัปโหลดรูปภาพบัตรประชาชนและตรวจสอบว่าเป็นบัตรประชาชนจริงหรือไม่
3	กดเพื่อยืนยันการลงทะเบียน	Yes		



รูปที่ 7-11 หน้าจอขั้นตอนลงทะเบียนสำหรับแจ้งคนโกง

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	สำหรับการยืนยันตัวตนด้วยเลขหมายโทรศัพท์	Yes		ระบบจะแสดงช่องให้กรอกหมายเลขโทรศัพท์
2	สำหรับแสดงบัตรประชาชนของผู้ลงทะเบียน	Yes		
3	สำหรับแสดงชื่อผู้ลงทะเบียน	Yes		
4	สำหรับแสดงนามสกุลของผู้ลงทะเบียน	Yes		
5	สำหรับแสดงเลขบัตรประจำตัวประชาชนของผู้ลงทะเบียน	Yes		
6	สำหรับกรอกเลขเลเซอร์หลังบัตรประจำตัว	Yes		

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
	ประชาชน			
7	สำหรับกรอกเลขวันหมดอายุของบัตรประจำตัวประชาชน	Yes		
8	สำหรับยืนยันการลงทะเบียน			ระบบจะทำการตรวจสอบข้อมูลที่กรอกว่าใช่หรือไม่ ถ้าใช่จะบันทึกเป็นอันเสร็จสิ้นการยืนยันตัวตน ถ้าไม่จะแสดงข้อความว่าไม่ถูกต้อง



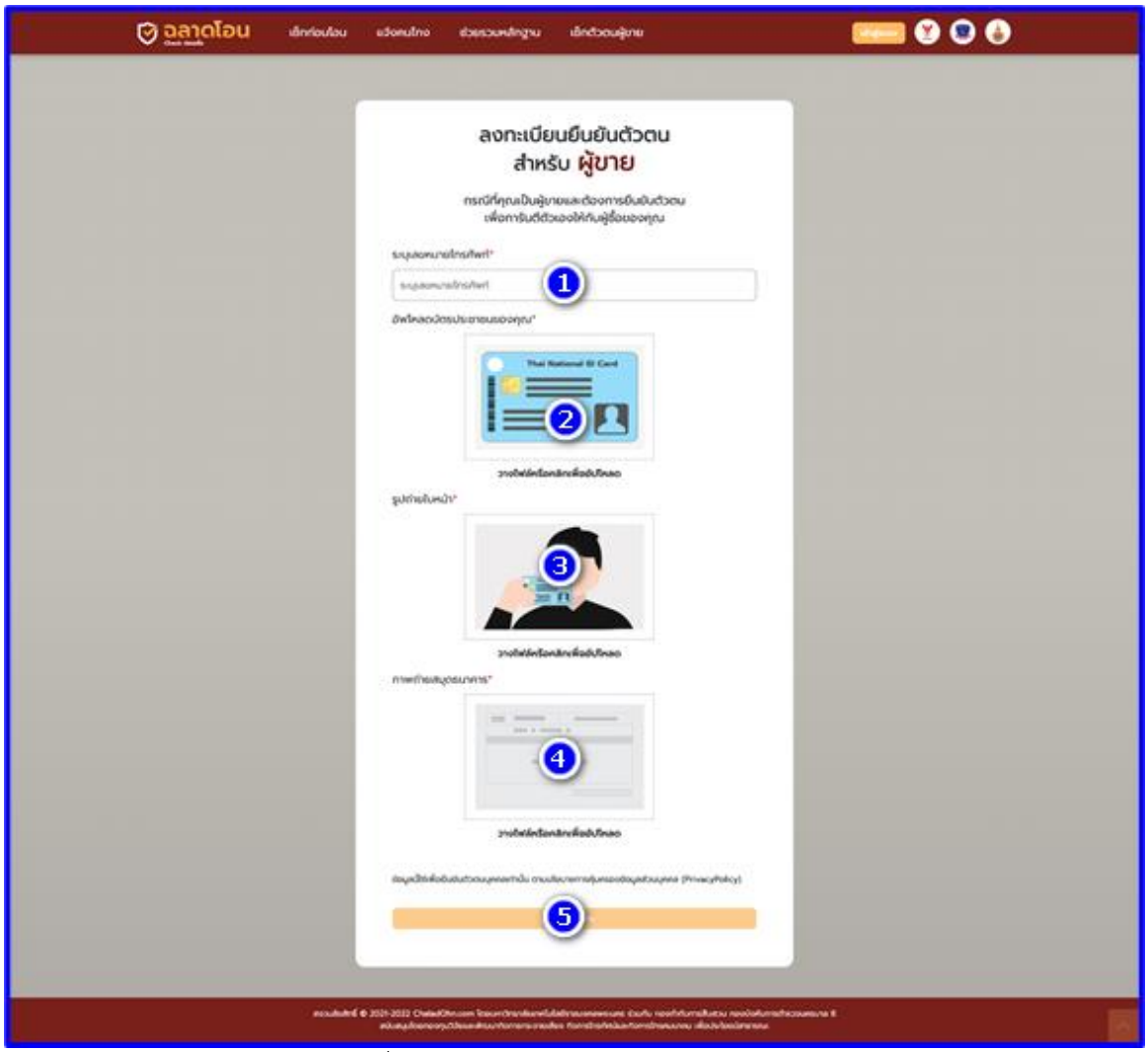
รูปที่ 7-12 หน้าจอลงทะเบียนสำหรับประเมินหลักฐาน

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	สำหรับระบุเลขหมายโทรศัพท์	Yes		ระบบจะตรวจสอบเลขหมายโทรศัพท์ว่าเคยมีการลงทะเบียนไว้แล้วหรือยัง
2	สำหรับวางไฟล์หรืออัพโหลดไฟล์ภาพใบหน้าคู่กับบัตรประชาชน	Yes		ระบบจะให้อัปโหลดรูปภาพบัตรประชาชน และตรวจสอบว่าเป็นบัตรประชาชนจริงหรือไม่
3	สำหรับวางไฟล์หรืออัพโหลดไฟล์ภาพใบหน้าคู่กับบัตรประชาชน	Yes		ระบบจะให้อัปโหลดภาพถ่ายใบหน้า และตรวจสอบว่าเป็นรูปภาพใบหน้าคู่กับบัตรประชาชนจริงหรือไม่
4	กดเพื่อยืนยันการลงทะเบียน	Yes		

รูปที่ 7-13 หน้าจอขั้นตอนลงทะเบียนสำหรับประเมินหลักฐาน

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	สำหรับการยืนยันตัวตนด้วยเลขหมายโทรศัพท์	Yes		ระบบจะแสดงช่องให้กรอกหมายเลขโทรศัพท์
2	สำหรับแสดงบัตรประชาชนของผู้ลงทะเบียน	Yes		
3	สำหรับแสดงภาพถ่ายใบหน้าของผู้ลงทะเบียน	Yes		
4	สำหรับแสดงชื่อผู้	Yes		

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
	ลงทะเบียน			
5	สำหรับแสดงนามสกุลของผู้ลงทะเบียน	Yes		
6	สำหรับแสดงเลขบัตรประจำตัวประชาชนของผู้ลงทะเบียน	Yes		
7	สำหรับกรอกเลขเลเซอร์หลังบัตรประจำตัวประชาชน	Yes		
8	สำหรับกรอกเลขวันหมดอายุของบัตรประจำตัวประชาชน	Yes		
9	สำหรับยืนยันการลงทะเบียน			ระบบจะทำการตรวจสอบข้อมูลที่กรอกว่าใช่หรือไม่ ถ้าใช่จะบันทึกเป็นอันเสร็จสิ้นการยืนยันตัวตน ถ้าไม่จะแสดงข้อความว่าไม่ถูกต้อง



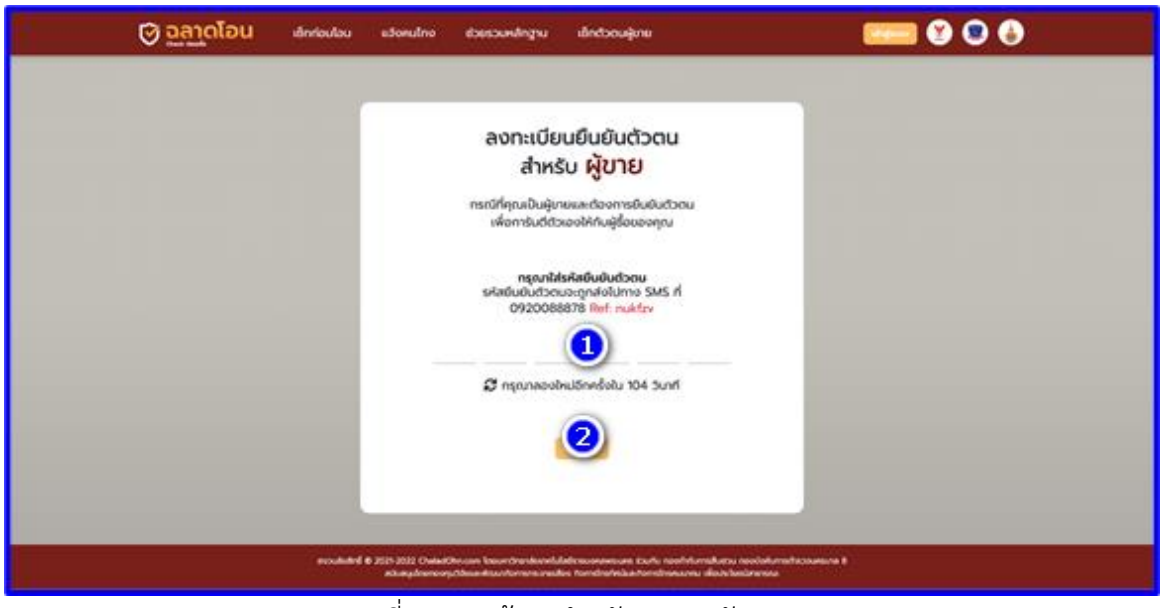
รูปที่ 7-14 หน้าจอลงทะเบียนสำหรับผู้ขาย

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	สำหรับระบุเลขหมายโทรศัพท์	Yes		ระบบจะตรวจสอบเลขหมายโทรศัพท์ว่าเคยมีการลงทะเบียนไว้แล้วหรือยัง
2	สำหรับวางไฟล์หรืออัพโหลดไฟล์ภาพใบหน้าคู่กับบัตรประชาชน	Yes		ระบบจะให้อัปโหลดรูปภาพบัตรประชาชน และตรวจสอบว่าเป็นบัตรประชาชนจริงหรือไม่
3	สำหรับวางไฟล์หรืออัพโหลดไฟล์ภาพใบหน้าคู่กับบัตรประชาชน	Yes		ระบบจะให้อัปโหลดภาพถ่ายใบหน้า และตรวจสอบว่าเป็นรูปภาพใบหน้าคู่กับบัตรประชาชนจริงหรือไม่
4	สำหรับวางไฟล์หรืออัพโหลดไฟล์ภาพสมุดบัญชี	Yes		ระบบจะให้อัปโหลดรูปภาพสมุดบัญชี
5	กดเพื่อยืนยันการลงทะเบียน	Yes		

รูปที่ 7-15 หน้าจอขั้นตอนลงทะเบียนสำหรับผู้ขาย

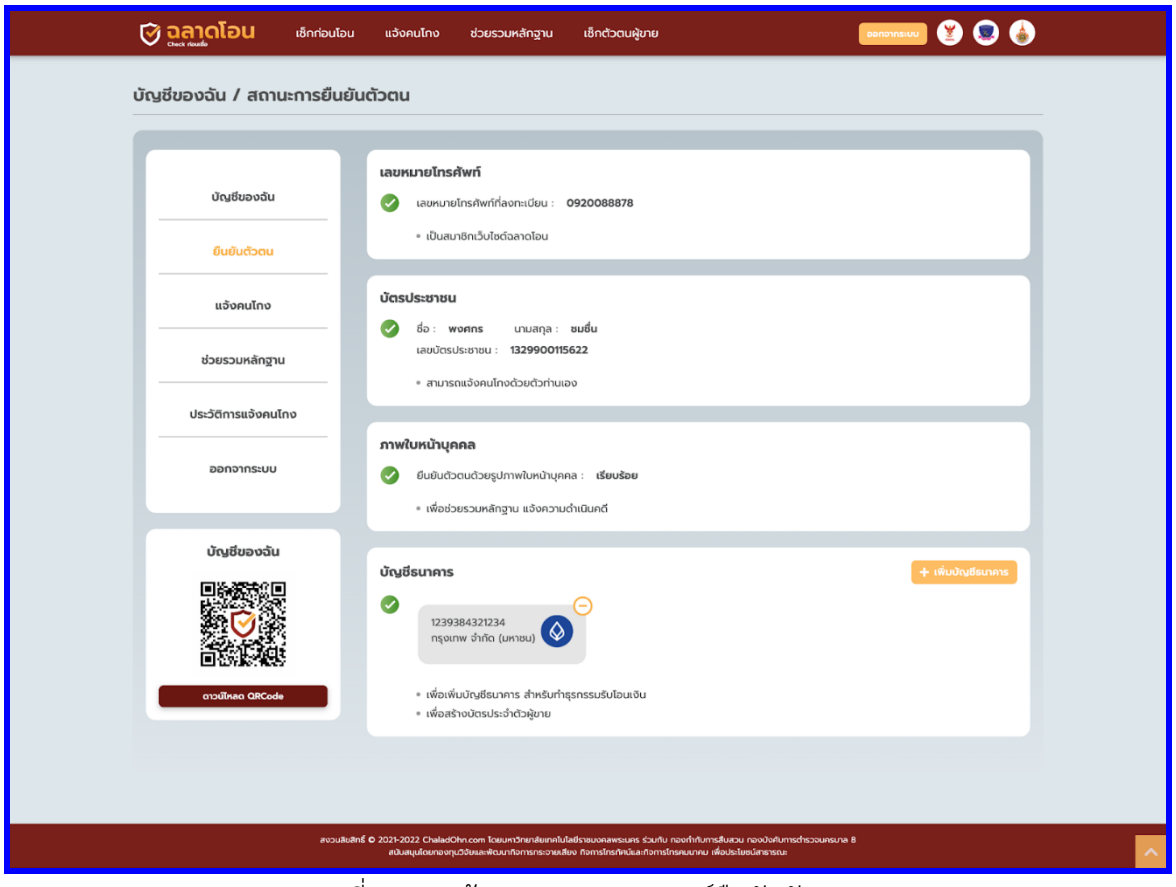
ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	สำหรับการยืนยันตัวตน	Yes		ระบบจะแสดงช่องให้กรอกหมายเลขโทรศัพท์

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
	ด้วยเลขหมายโทรศัพท์			
2	สำหรับแสดงบัตรประชาชนของผู้ลงทะเบียน	Yes		
3	สำหรับแสดงภาพถ่ายสมุดบัญชีของผู้ลงทะเบียน	Yes		
4	สำหรับแสดงภาพถ่ายใบหน้าของผู้ลงทะเบียน	Yes		
5	สำหรับแสดงชื่อผู้ลงทะเบียน	Yes		
6	สำหรับแสดงนามสกุลของผู้ลงทะเบียน	Yes		
7	สำหรับกรอกเลขเลเซอร์หลังบัตร	Yes		
8	สำหรับแสดงเลขบัตรประจำตัวประชาชนของผู้ลงทะเบียน	Yes		
9	สำหรับกรอกเลขที่บัญชีธนาคารของผู้ลงทะเบียน	Yes		
10	สำหรับกรอกเลขที่บัญชีธนาคารของผู้ลงทะเบียน	Yes		
11	สำหรับกรอกชื่อธนาคารของผู้ลงทะเบียน	Yes		
12	สำหรับกรอกชื่อบัญชีธนาคารของผู้ลงทะเบียน	Yes		
13	กดเพื่อยืนยันข้อมูล	Yes		ระบบจะทำการตรวจสอบข้อมูลที่กรอกว่าใช่หรือไม่ ถ้าใช่จะบันทึกเป็นอันเสร็จสิ้นการยืนยันตัวตน ถ้าไม่จะแสดงข้อความว่าไม่ถูกต้อง



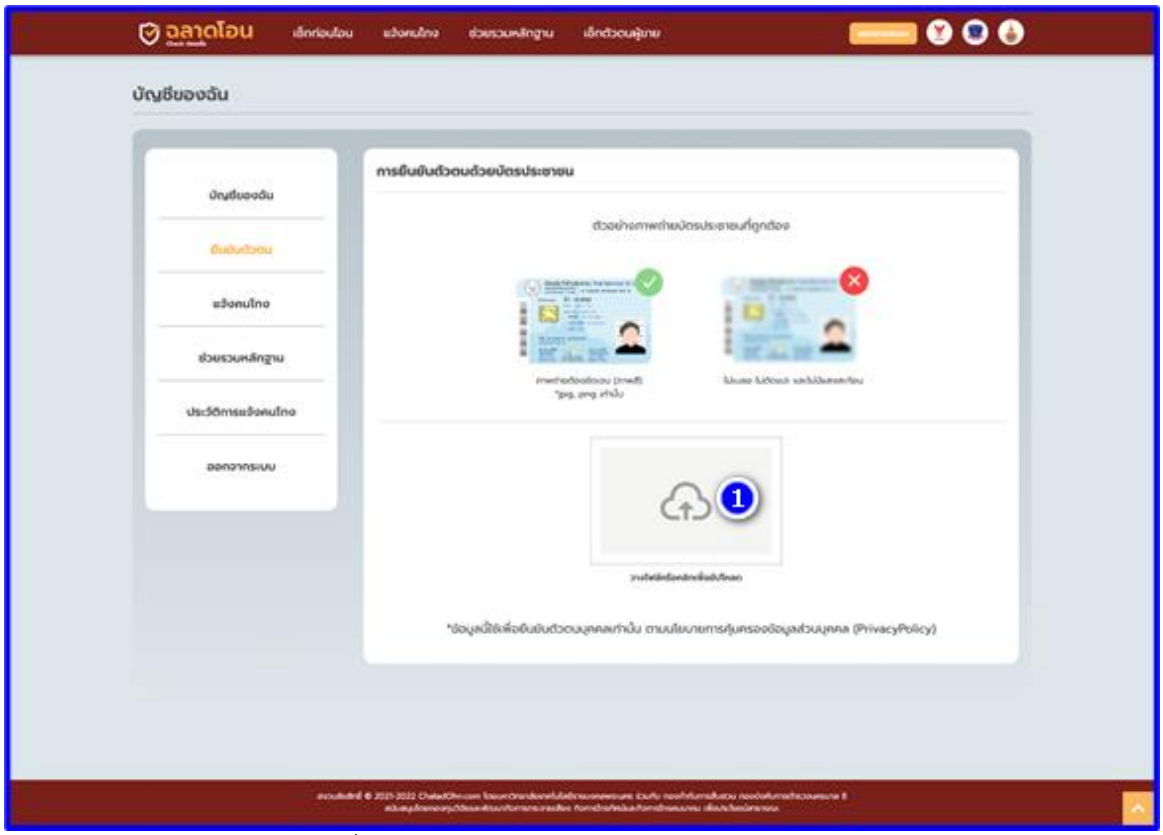
รูปที่ 7-16 หน้าจอสำหรับกรอกรหัส OTP

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	สำหรับระบุเลข OTP	Yes		ระบบจะตรวจสอบเลขหมายโทรศัพท์ว่าเคยมีการลงทะเบียนไว้แล้วหรือยัง
2	กดเพื่อยืนยันการลงทะเบียน	Yes		



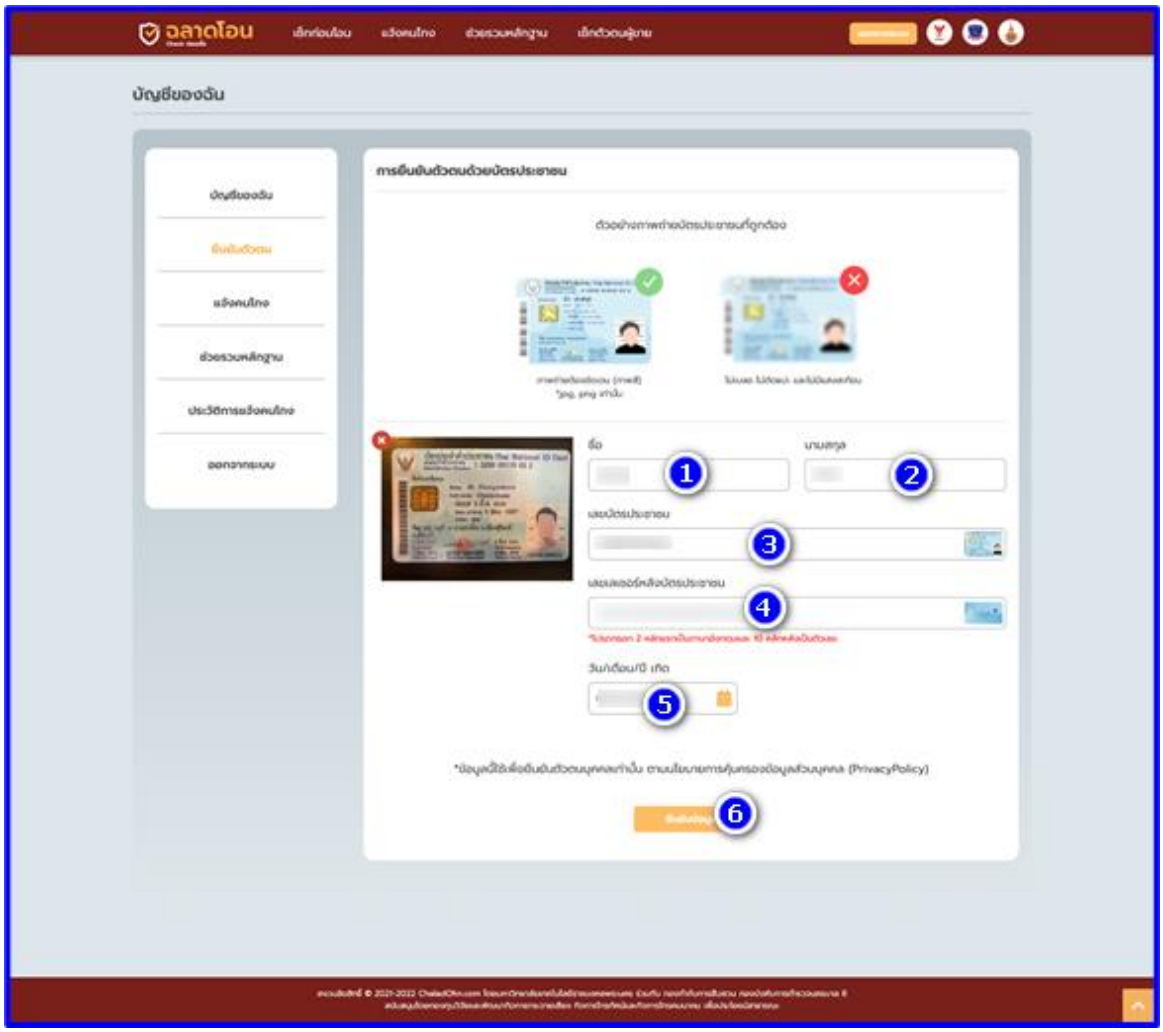
รูปที่ 7-17 หน้าจอแสดงสถานการณ์ยืนยันตัวตน

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	สำหรับการยืนยันตัวตนด้วยเลขหมายโทรศัพท์	Yes		ระบบจะแสดงช่องให้กรอกหมายเลขโทรศัพท์
2	สำหรับการยืนยันตัวตนด้วยบัตรประชาชน	Yes		ระบบจะแสดงภาพตัวอย่างการถ่ายบัตรประชาชนที่ถูกต้องพร้อมกับปุ่มอัปโหลดรูปภาพ สำหรับบัตรประชาชน
3	สำหรับการยืนยันตัวตนด้วยภาพใบหน้าบุคคล	Yes		ระบบจะแสดงภาพตัวอย่างการถ่ายภาพยืนยันตัวตนด้วยใบหน้าบุคคลที่ถูกต้องพร้อมกับปุ่มอัปโหลดรูปภาพ สำหรับการยืนยันตัวตนด้วยภาพใบหน้าบุคคล
4	สำหรับการยืนยันตัวตนด้วยบัญชีธนาคาร	Yes		ระบบจะแสดงภาพตัวอย่างการถ่ายบัญชีธนาคารที่ถูกต้องพร้อมกับปุ่มอัปโหลดรูปภาพ สำหรับบัตรบัญชีธนาคาร



รูปที่ 7-18 หน้าจอยืนยันตัวตนด้วยบัตรประชาชน

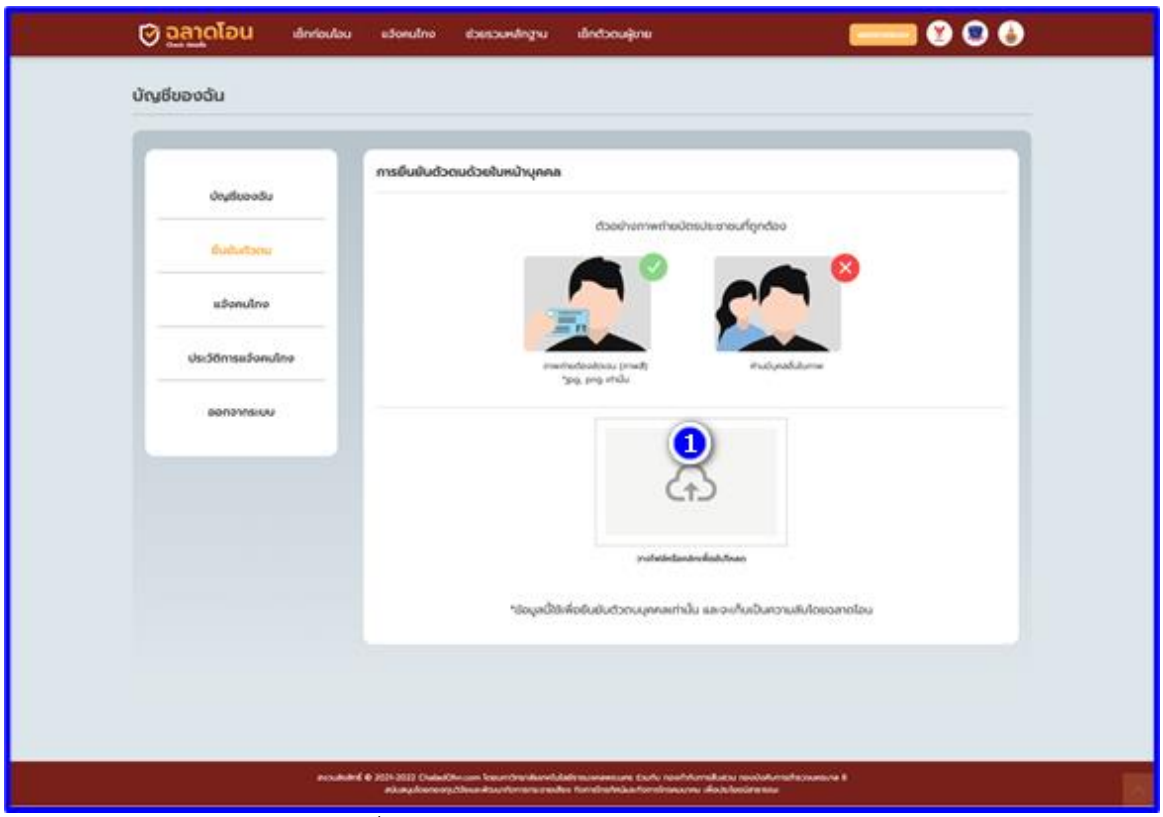
ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	สำหรับวางไฟล์หรืออัพโหลดไฟล์ภาพบัตรประชาชน	Yes		ระบบจะให้อัปโหลดรูปภาพ และตรวจสอบว่าเป็นบัตรประชาชนจริงหรือไม่



รูปที่ 7-19 หน้าจอกรอกรายละเอียดบัตรประชาชน

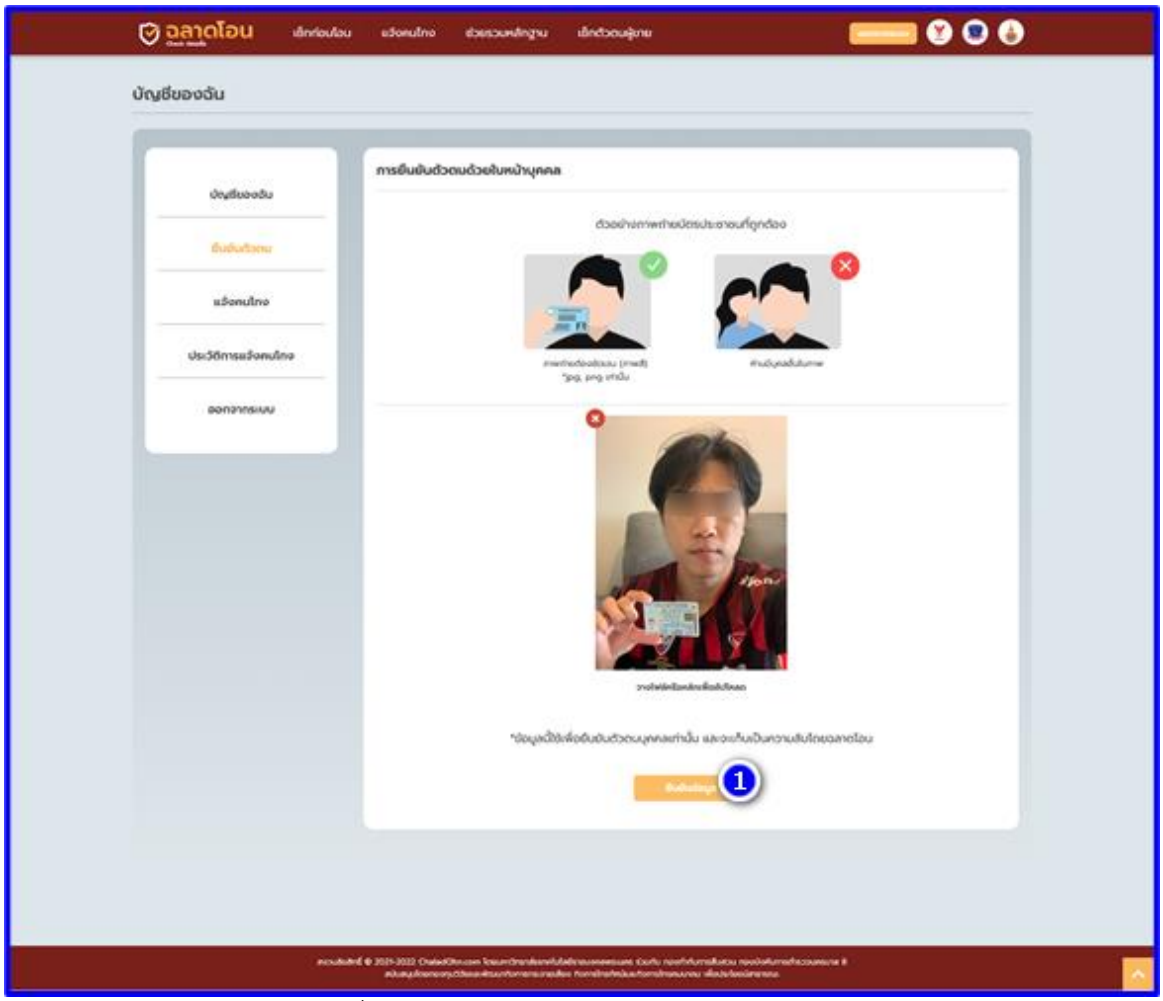
ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	สำหรับแสดงชื่อผู้ลงทะเบียน	Yes		
2	สำหรับแสดงนามสกุลของผู้ลงทะเบียน	Yes		
3	สำหรับแสดงเลขบัตรประจำตัวประชาชนของผู้ลงทะเบียน	Yes		
4	สำหรับกรอกเลขเลเซอร์หลังบัตรประจำตัวประชาชน	Yes		
5	สำหรับกรอกวันเดือนปีเกิดของผู้ลงทะเบียน	Yes		
6	สำหรับยืนยันข้อมูลบัตร			ระบบจะทำการตรวจสอบข้อมูลที่กรอกว่าใช่

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
	ประชาชน			หรือไม่ ถ้าใช่จะบันทึกเป็นอันเสร็จสิ้นการยืนยันตัวตน ถ้าไม่จะแสดงข้อความว่าไม่ถูกต้อง



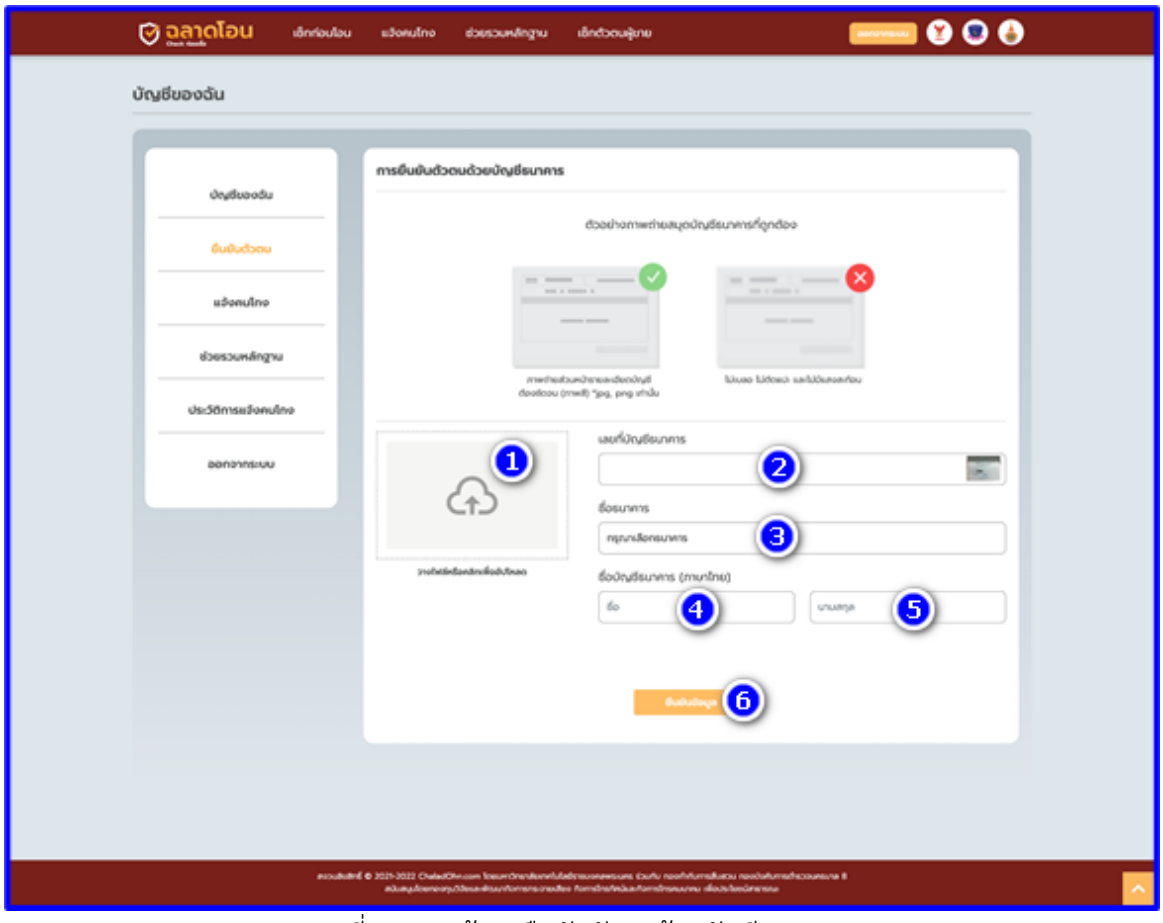
รูปที่ 7-20 หน้าจออัปโหลดภาพใบหน้าบุคคล

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	สำหรับวางไฟล์หรืออัพโหลดไฟล์ภาพใบหน้าคู่กับบัตรประชาชน	Yes		ระบบจะให้อัปโหลดรูปภาพ และตรวจสอบว่าเป็นรูปภาพใบหน้าคู่กับบัตรประชาชนจริงหรือไม่



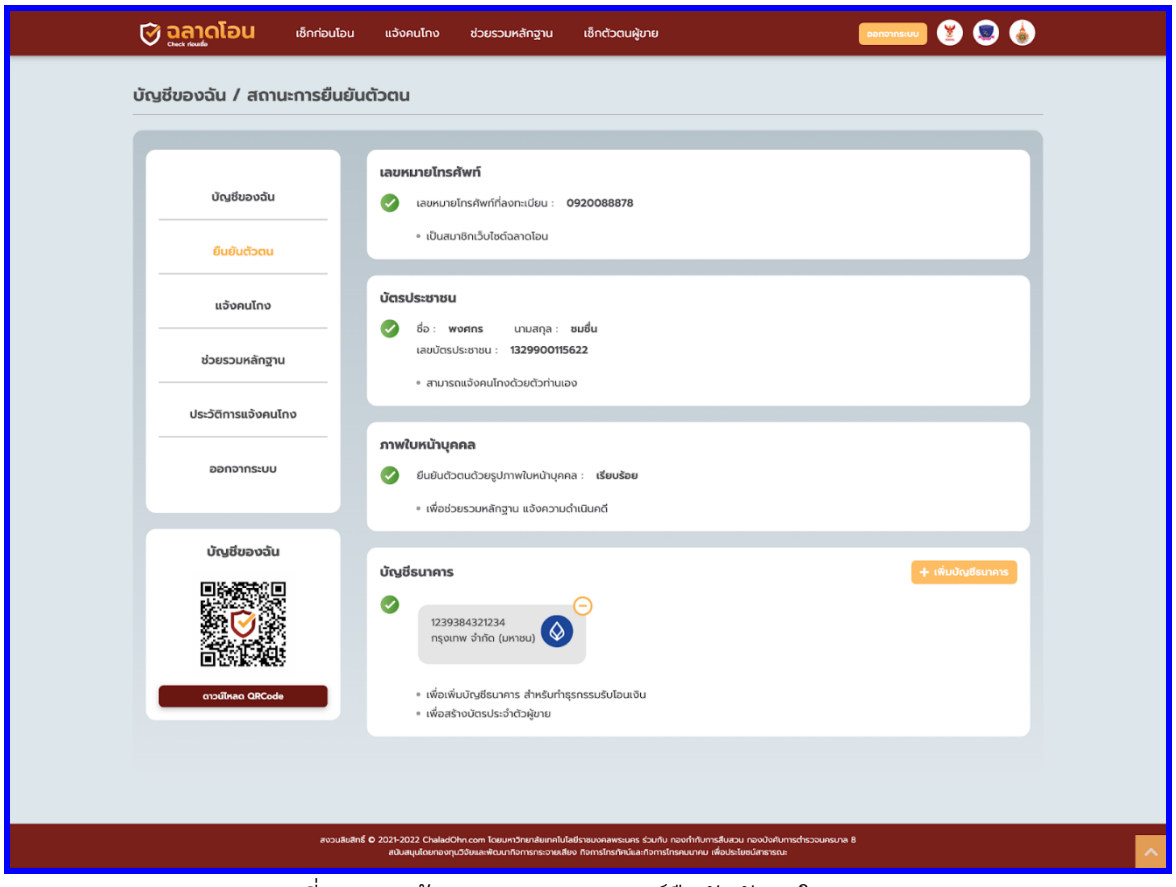
รูปที่ 7-21 หน้าจอยืนยันตัวตนด้วยใบหน้าบุคคล

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	สำหรับยืนยันข้อมูล	Yes		ระบบจะบันทึกข้อมูลสำหรับการยืนยันตัวตนด้วยภาพถ่ายใบหน้าบุคคล



รูปที่ 7-22 หน้าจอยืนยันตัวตนด้วยบัญชีธนาคาร

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	สำหรับวางไฟล์หรืออัพโหลดไฟล์ภาพบัญชีธนาคาร	Yes		ระบบจะให้อัปโหลดรูปภาพ และตรวจสอบว่าเป็นรูปภาพบัญชีธนาคารจริงหรือไม่
2	สำหรับแสดงเลขที่บัญชีธนาคาร			
3	สำหรับแสดงชื่อธนาคาร			
4	สำหรับแสดงชื่อบัญชีธนาคาร			
5	สำหรับแสดงนามสกุลบัญชีธนาคาร			
6	สำหรับบันทึกข้อมูลการยืนยันตัวตนด้วยบัญชีธนาคาร			ระบบจะบันทึกข้อมูลสำหรับการยืนยันตัวตนด้วยเลขบัญชีธนาคาร

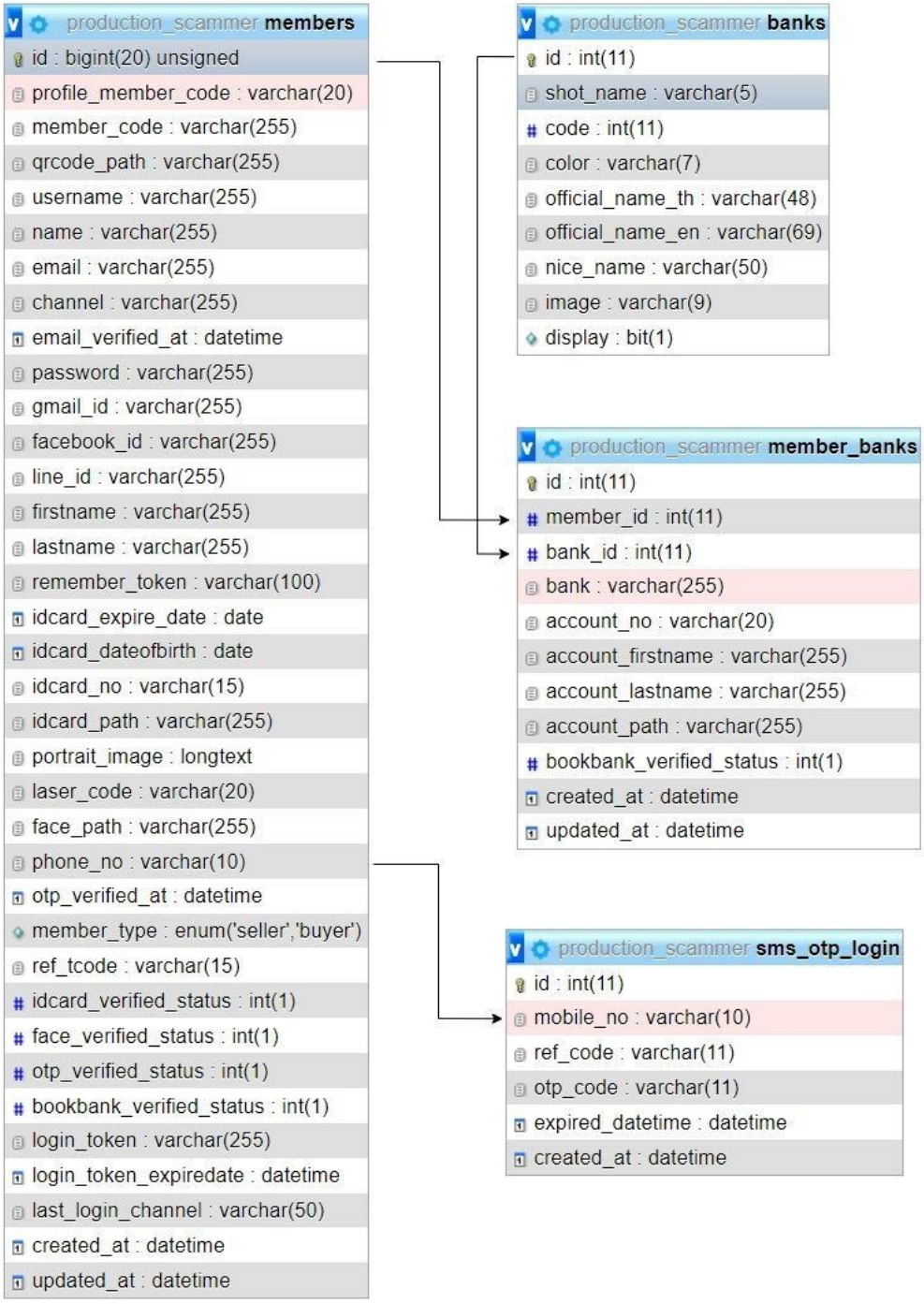


รูปที่ 7-23 หน้าจอแสดงสถานการณ์ยืนยันตัวตนในระบบ

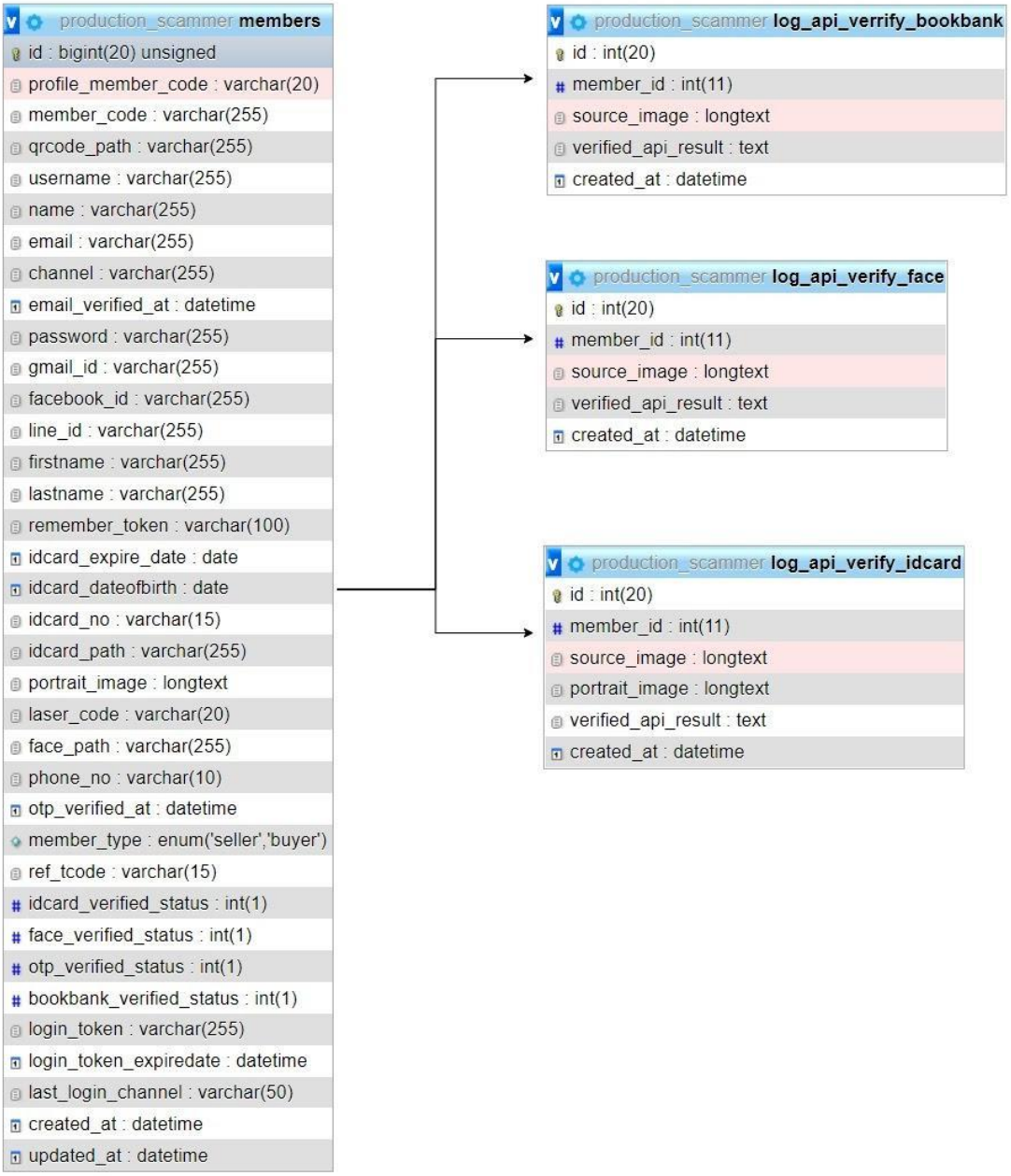
ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	สำหรับดาวน์โหลด QR Code ของผู้ขาย	Yes		ระบบจะทำการสร้างQR Codeและดาวน์โหลดลงบนอุปกรณ์ที่ใช้

7.1.4 ระบบฐานข้อมูล

7.1.4.1 แผนภาพแสดงโครงสร้างการออกแบบฐานข้อมูล (ER-Diagram)



รูปที่ 7-24 ผังแสดงความสัมพันธ์ของระบบลงทะเบียน



รูปที่ 7-25 ผังแสดงความสัมพันธ์ของการยืนยันตัวตน

7.1.4.2 พจนานุกรมข้อมูล (Data Dictionary)

ตารางที่ 7-1 ข้อมูลของตาราง members

Column	Type	Null	Default	Description
id *(Primary)*	bigint(20)	No		คีย์หลัก
profile_member_code	varchar(20)	Yes	*NULL*	รหัสลำดับสมาชิก
member_code	varchar(255)	Yes	*NULL*	รหัสสมาชิก
qrcode_path	varchar(255)	Yes	*NULL*	รูปคิวอาร์โคด
username	varchar(255)	Yes	*NULL*	รหัส
name	varchar(255)	Yes	*NULL*	ชื่อ
email	varchar(255)	Yes	*NULL*	อีเมล
channel	varchar(255)	Yes	*NULL*	'line','facebook','gmail','kiosk'
email_verified_at	datetime	Yes	*NULL*	วันที่ยืนยันอีเมล
password	varchar(255)	Yes	*NULL*	รหัสผ่าน
gmail_id	varchar(255)	Yes	*NULL*	คีย์อีเมล
facebook_id	varchar(255)	Yes	*NULL*	คีย์เฟสบุ๊ค
line_id	varchar(255)	Yes	*NULL*	คีย์ไลน์ไอดี
firstname	varchar(255)	Yes	*NULL*	ชื่อ
lastname	varchar(255)	Yes	*NULL*	นามสกุล
remember_token	varchar(100)	Yes	*NULL*	รหัสโทเคน
idcard_expire_date	date	Yes	*NULL*	วันที่หมดอายุบัตรประชาชน
idcard_dateofbirth	date	Yes	*NULL*	วันเกิดบนบัตรประชาชน
idcard_no	varchar(15)	Yes	*NULL*	หมายเลขบัตรประชาชน
portrait_image	longtext	Yes	*NULL*	รูปภาพใบหน้าบนบัตรประชาชน
face_path	varchar(255)	Yes	*NULL*	รูปภาพใบหน้า
phone_no	varchar(10)	Yes	*NULL*	หมายเลขโทรศัพท์
otp_verified_at	datetime	Yes	*NULL*	วันที่ยืนยัน OTP
member_type	enum('seller', 'buyer')	Yes	*NULL*	ประเภทสมาชิก
ref_tcode	varchar(15)	Yes	*NULL*	
idcard_verified_status	int(1)	No		0=no verify,1=verified
face_verified_status	int(1)	No		0=no verify,1=verified
otp_verified_status	int(1)	No	0	0=no verify,1=verified
bookbank_verified_status	int(1)	No		0=no verify,1=verified

Column	Type	Null	Default	Description
login_token	varchar(255)	Yes	*NULL*	รหัสโทเคนสำหรับตู้ Kiosk
login_token_expiredate	datetime	Yes	*NULL*	วันหมดอายุโทเคน
last_login_channel	varchar(50)	Yes	*NULL*	
created_at	datetime	Yes	*NULL*	วันที่สร้าง
updated_at	datetime	Yes	*NULL*	วันที่แก้ไข

ตารางที่ 7-2 ข้อมูลของตาราง member_banks

Column	Type	Null	Default	Description
id *(Primary)*	int(11)	No		คีย์หลัก
member_id	int(11)	No		คีย์หลักสมาชิก
bank_id	int(11)	No		คีย์หลักธนาคาร
bank	varchar(255)	Yes	*NULL*	ชื่อธนาคาร
account_no	varchar(20)	Yes	*NULL*	หมายเลขบัญชีธนาคาร
account_firstname	varchar(255)	Yes	*NULL*	ชื่อธนาคารบัญชีธนาคาร
account_lastname	varchar(255)	Yes	*NULL*	นามสกุลบัญชีธนาคาร
account_path	varchar(255)	Yes	*NULL*	รูปสมุดบัญชีธนาคาร
bookbank_verified_status	int(1)	No	0	0=no verify,1=verified
created_at	datetime	No		วันที่สร้าง
updated_at	datetime	No		วันที่แก้ไข

ตารางที่ 7-3 ข้อมูลของตาราง banks

Column	Type	Null	Default	Description
id *(Primary)*	int(11)	No		คีย์หลัก
shot_name	varchar(5)	No		ชื่อย่อ
code	int(11)	No		รหัสธนาคาร
color	varchar(7)	Yes	*NULL*	รหัสสี
official_name_th	varchar(48)	No		ชื่อภาษาไทย
official_name_en	varchar(69)	No		ชื่อภาษาอังกฤษ
nice_name	varchar(50)	No		ชื่อเรียก
image	varchar(9)	No		รูปภาพ
display	bit(1)	No		สถานะการแสดง

ตารางที่ 7-4 ข้อมูลของตาราง sms_otp_login

Column	Type	Null	Default	Description
id *(Primary)*	int(11)	No		คีย์หลัก
mobile_no	varchar(10)	No		หมายเลขโทรศัพท์
ref_code	varchar(11)	Yes	*NULL*	รหัสอ้างอิง
otp_code	varchar(11)	No		รหัส OTP
expired_datetime	datetime	No		วันเวลาหมดอายุ OTP
created_at	datetime	No		วันที่สร้าง

ตารางที่ 7-5 ข้อมูลของตาราง log_api_verify_idcard

Column	Type	Null	Default	Description
id *(Primary)*	int(20)	No		คีย์หลัก
member_id	int(11)	Yes	*NULL*	คีย์หลักสมาชิก
source_image	longtext	Yes	*NULL*	รูปภาพ
portrait_image	longtext	Yes	*NULL*	รูปภาพ
verified_api_result	text	Yes	*NULL*	ผลลัพท์การตรวจสอบ
created_at	datetime	No		วันที่แก้ไข

ตารางที่ 7-6 ข้อมูลของตาราง log_api_verrify_bookbank

Column	Type	Null	Default	Description
id *(Primary)*	int(20)	No		คีย์หลัก
member_id	int(11)	Yes	*NULL*	คีย์หลักสมาชิก
source_image	longtext	Yes	*NULL*	รูปภาพ
verified_api_result	text	Yes	*NULL*	ผลลัพท์การตรวจสอบ
created_at	datetime	No		วันที่แก้ไข

ตารางที่ 7-7 ข้อมูลของตาราง log_api_verify_fac

Column	Type	Null	Default	Description
id (Primary)	int(20)	No		
member_id	int(11)	Yes	NULL	
source_image	longtext	Yes	NULL	
verified_api_result	text	Yes	NULL	
created_at	datetime	No		

7.2 การพัฒนาระบบค้นหาข้อมูลผู้กระทำความผิด

ระบบค้นหาข้อมูลผู้กระทำผิด เป็นระบบที่ช่วยให้ผู้ใช้งานระบบต้นแบบฯ สามารถสืบค้นประวัติของผู้กระทำความผิด และข้อมูลผู้ขายที่ได้มีการยืนยันตัวตนกับระบบต้นแบบฯ เพื่อให้ผู้ใช้งานระบบต้นแบบฯ มีข้อมูลประกอบการตัดสินใจในการทำธุรกรรมออนไลน์ รวมถึงสร้างความเชื่อมั่นในการทำธุรกรรมออนไลน์ให้กับผู้ซื้อ ผ่านการที่ผู้ซื้อเข้ามาสืบค้นด้วยรายละเอียดของผู้ขาย อาทิ ข้อมูลชื่อนามสกุล, เลขที่บัญชีธนาคาร, หมายเลขพรอมพ์เพย์, หมายเลขทรูวอลเล็ต หรือเลขหมายโทรศัพท์เคลื่อนที่ จากนั้นระบบจะส่งข้อมูลไปตรวจสอบข้อมูลการกระทำความผิดจากหน่วยงานที่เกี่ยวข้องและข้อมูลการยืนยันตัวตนผู้ขายจากข้อมูลผู้ขายที่มีการยืนยันตัวตนในระบบต้นแบบฯ

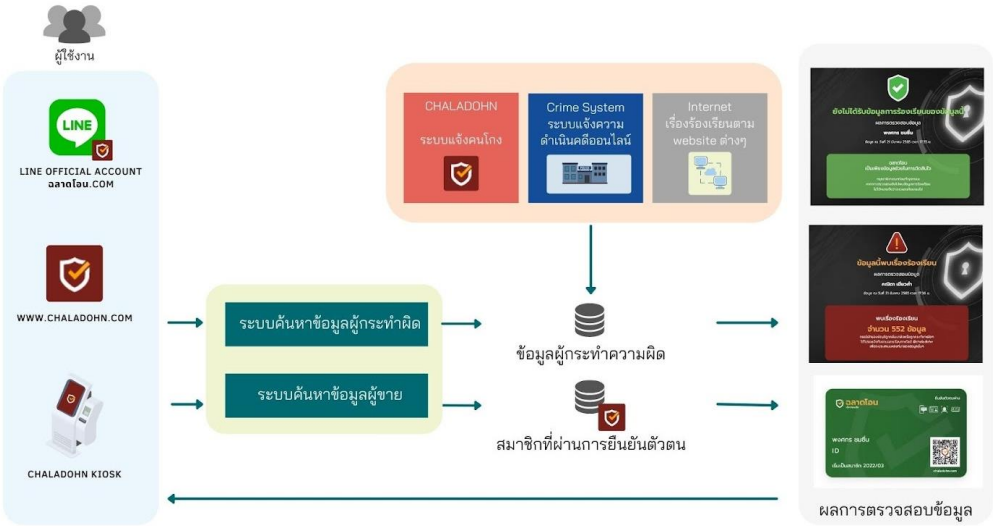
7.2.1 แนวทางการสืบค้นข้อมูลผู้กระทำความผิด

การใช้งานระบบค้นหาข้อมูลผู้กระทำความผิด เพื่อค้นหาประวัติการกระทำความผิดของเจ้าของบัญชีที่ต้องการโอนเงิน หรือประวัติการยืนยันตัวตนกับระบบต้นแบบฯของเจ้าของบัญชีนั้น สามารถใช้งานได้ผ่าน 3 ช่องทาง ได้แก่

1. เว็บไซต์ฉลาดโอนดอทคอม
2. LINE Official Account ฉลาดโอน.com
3. ตู้คีออส

โดยการค้นหาข้อมูลผู้กระทำความผิด จะใช้วิธีการค้นหาในรูปแบบข้อความอัตโนมัติ (Autocomplete) เพื่อให้สะดวกต่อการค้นหาของผู้ใช้งานและป้องกันการค้นหาด้วยคำผิด

นอกจากนี้ผู้ใช้งานระบบต้นแบบฯ ยังสามารถตรวจสอบข้อมูลผู้ขายที่ยืนยันตัวตนในระบบต้นแบบฯ ด้วยคิวอาร์โค้ด เพื่อเพิ่มความมั่นใจต่อการทำธุรกรรมออนไลน์



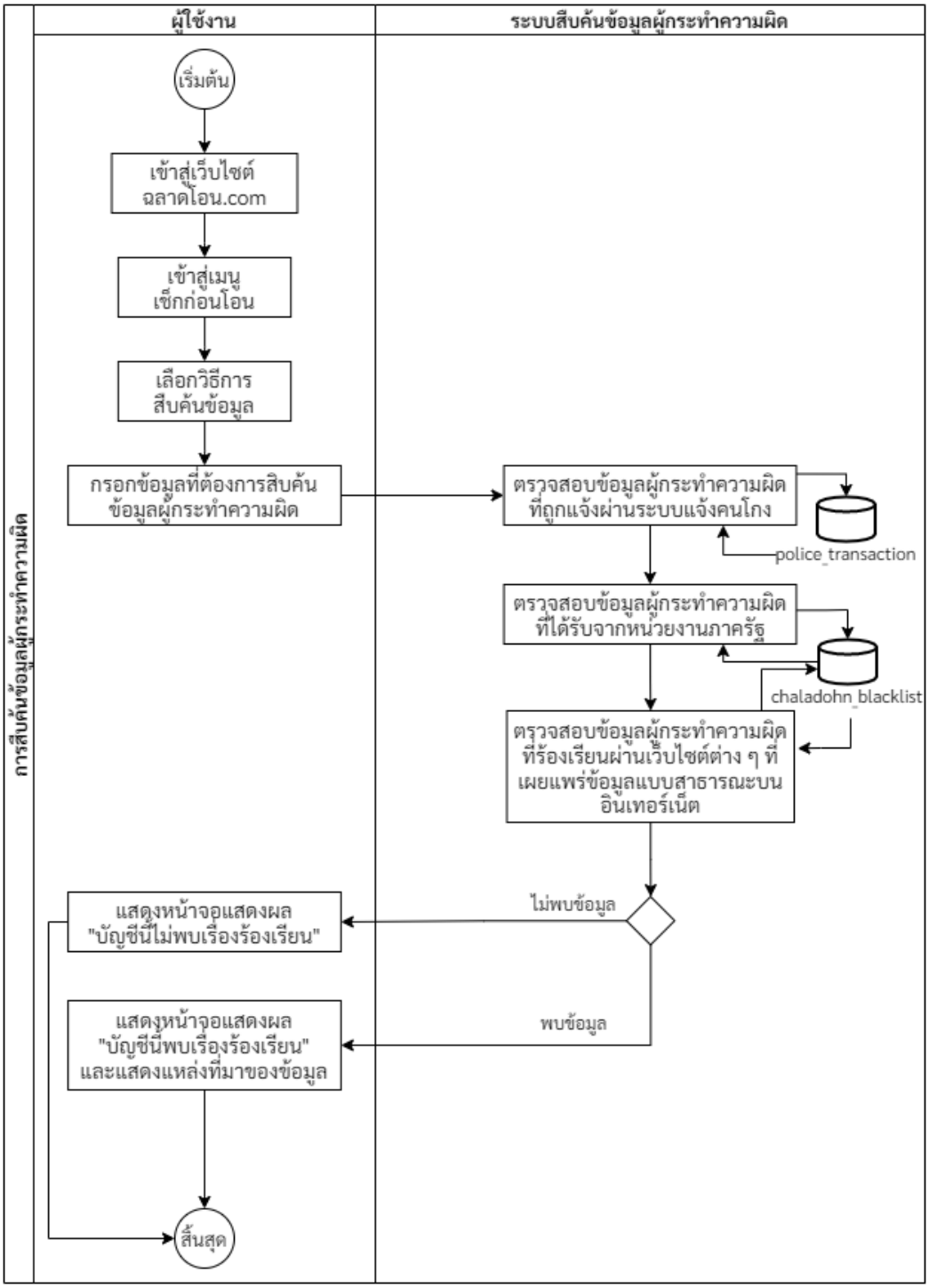
รูปที่ 7-26 ภาพรวมสืบค้นข้อมูลผู้กระทำความผิด

7.2.2 กระบวนการทำงานของระบบ

ผู้ใช้งานสามารถสืบค้นและตรวจสอบข้อมูล ได้ 2 รูปแบบ ได้แก่ (1) การสืบค้นข้อมูลผู้กระทำความผิด และ (2) การตรวจสอบข้อมูลผู้ขายที่ยืนยันตัวตนในระบบต้นแบบฯ

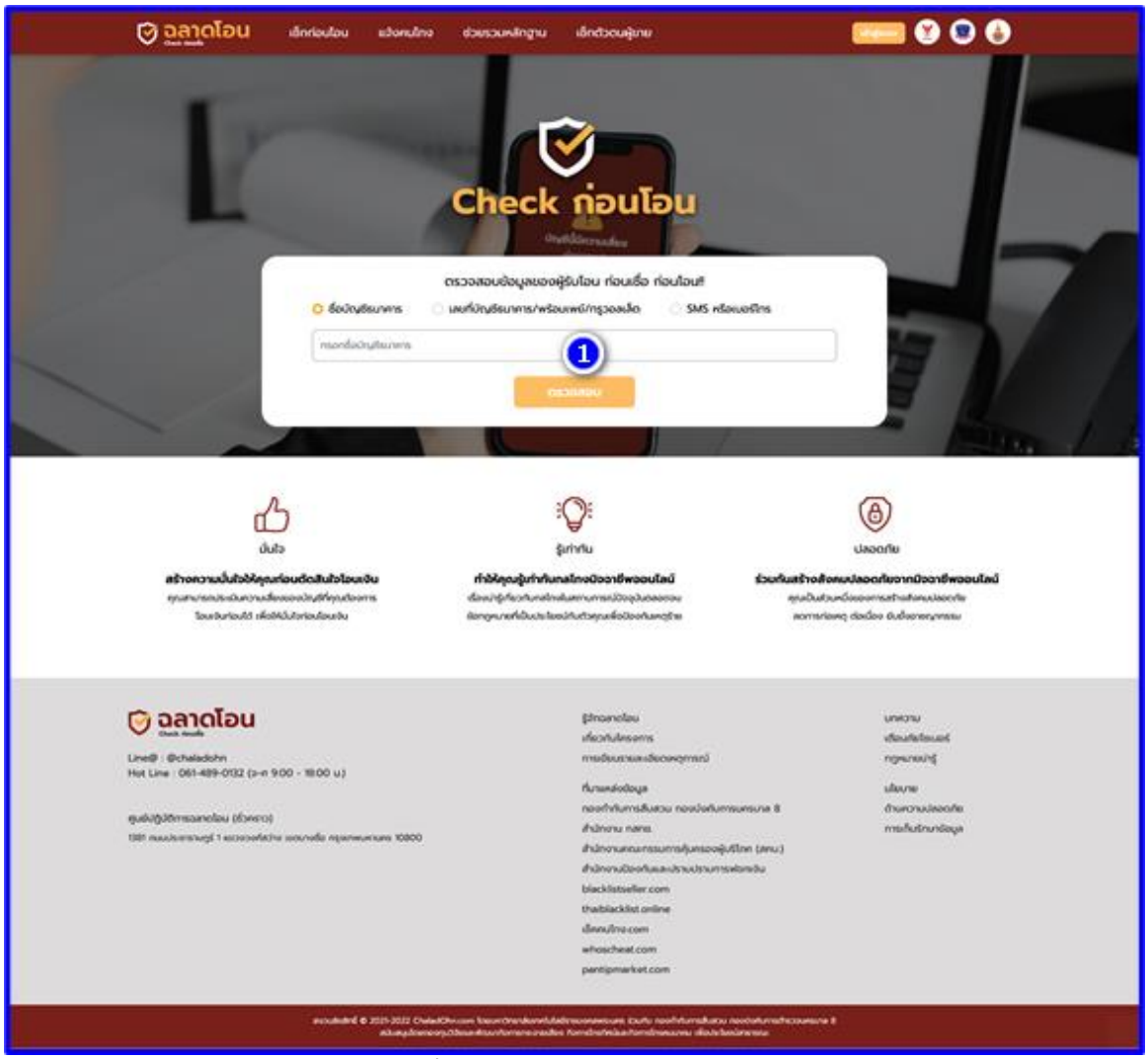
สำหรับรูปแบบที่ 1 ผู้ใช้งานสามารถใช้งานได้ผ่านช่องทางเว็บไซต์ฉลาดโอนดอทคอม , ช่องทางLINE Official Account ฉลาดโอนดอทคอม และตู้คีออส โดยผู้ใช้งานจะกรอกข้อมูลเกี่ยวกับบัญชีธนาคารของผู้ขายหรือผู้รับโอน อาทิ ชื่อบัญชีธนาคาร, เลขที่บัญชีธนาคาร, หมายเลขพรอมพ์เพย์ , ทรูวอลเล็ต หรือเลขหมายโทรศัพท์เคลื่อนที่ จากนั้นระบบจะตรวจสอบข้อมูลจากที่ผู้ใช้งานระบบต้นแบบฯกรอกมาว่าเคยมีประวัติการกระทำความผิดหรือไม่ หากพบรายการกระทำความผิด ระบบต้นแบบฯจะแสดงข้อความว่า “ข้อมูลนี้พบเรื่องร้องเรียน” และแสดงผลลัพธ์เป็นสีแดง นอกจากนี้ยังแสดงถึงแหล่งที่มาของการพบเรื่องร้องเรียนว่าถูกร้องเรียนจากที่ใด

สำหรับรูปแบบที่ 2 ผู้ใช้งานสามารถใช้งานได้ผ่านทางเว็บไซต์ฉลาดโอนดอทคอม และช่องทางLINE Official Account ฉลาดโอน.com เช่นเดียวกันกับการสืบค้นข้อมูลผู้กระทำความผิด โดยผู้ใช้งานสามารถตรวจสอบข้อมูลผู้ขายที่ได้ยืนยันตัวในระบบต้นแบบฯ ด้วยข้อมูลชื่อ นามสกุล หรือเลขที่บัญชีของผู้ขายที่ผู้ใช้งานต้องการตรวจสอบ หากพบว่าผู้ขายรายนั้นได้มีการยืนยันตัวตนกับระบบต้นแบบฯ ระบบจะแสดงข้อมูลของผู้ขาย ได้แก่ ชื่อ นามสกุล , ID ประจำตัวผู้ขาย, ช่วงเวลาที่เริ่มยืนยันตัวตน, วิธีการยืนยันตัวตน และคิวอาร์โค้ดประจำผู้ขาย นอกจากข้อมูลเบื้องต้นนี้ ระบบยังแสดงข้อมูลบัญชีธนาคารที่ผู้ขายได้มีการยืนยันไว้ในระบบต้นแบบฯ เพื่อป้องกันไม่ใช้ผู้ใช้งานที่เข้ามาตรวจสอบข้อมูลผู้ขายในระบบทำธุรกรรมกับบัญชีที่ผู้ขายไม่ได้มีการยืนยัน



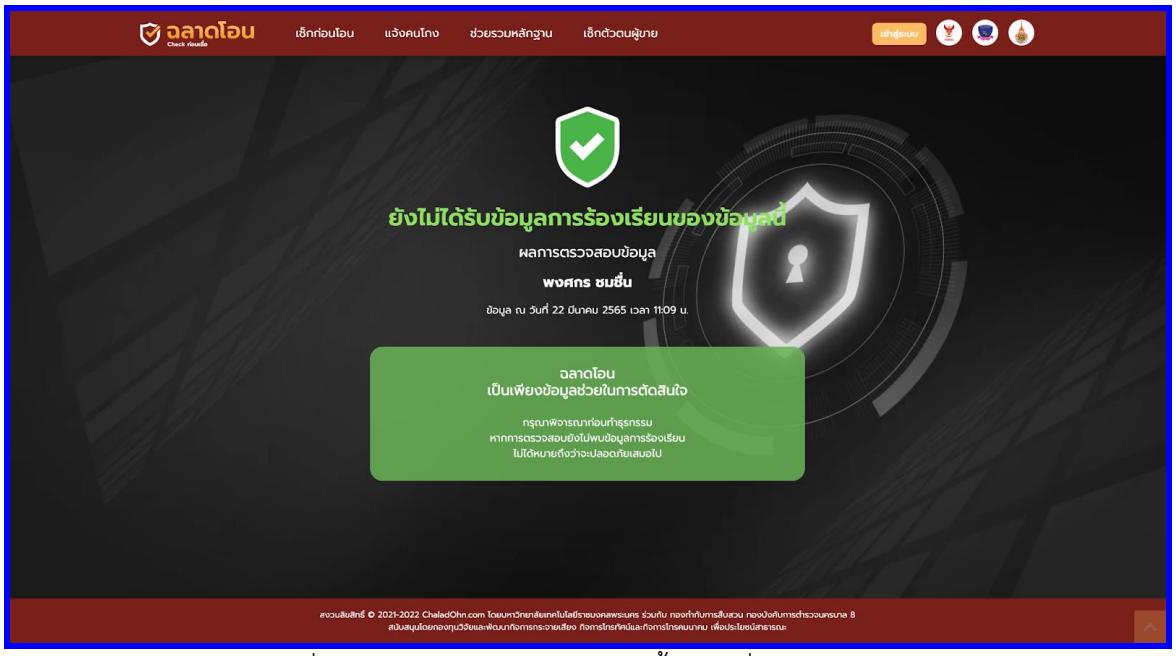
รูปที่ 7-27 ขั้นตอนการสืบค้นข้อมูลผู้กระทำความผิด

7.2.3 หน้าจอแสดงผลและรายละเอียดการทำงาน



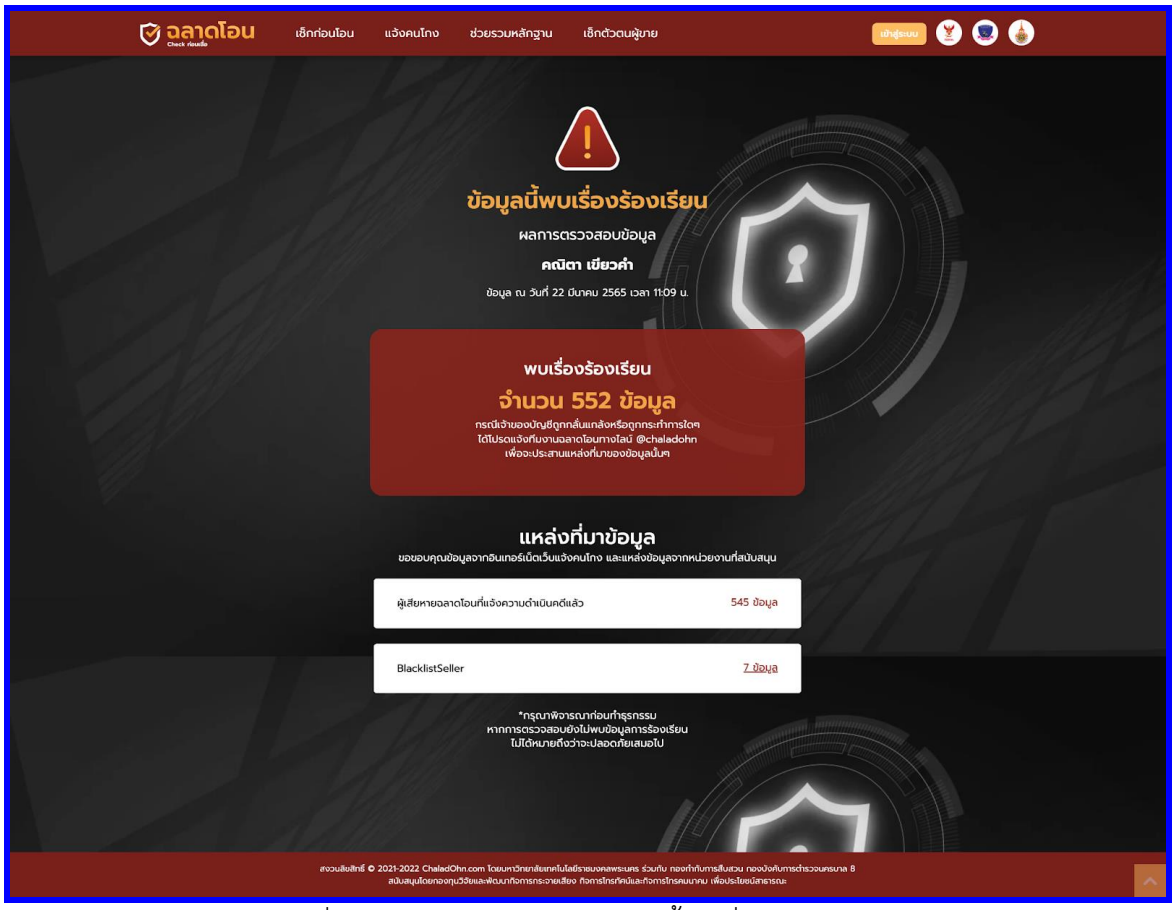
รูปที่ 7-28 หน้าจอสืบค้นข้อมูล

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	สำหรับการกรอกข้อมูลที่ต้องการตรวจสอบ	Yes	Textarea	ระบบจะตรวจสอบข้อมูลจากชื่อบัญชีธนาคาร หรือ เลขที่บัญชีธนาคาร/พร้อมเพย์/ทรูวอลเล็ต ที่ส่งเข้ามา



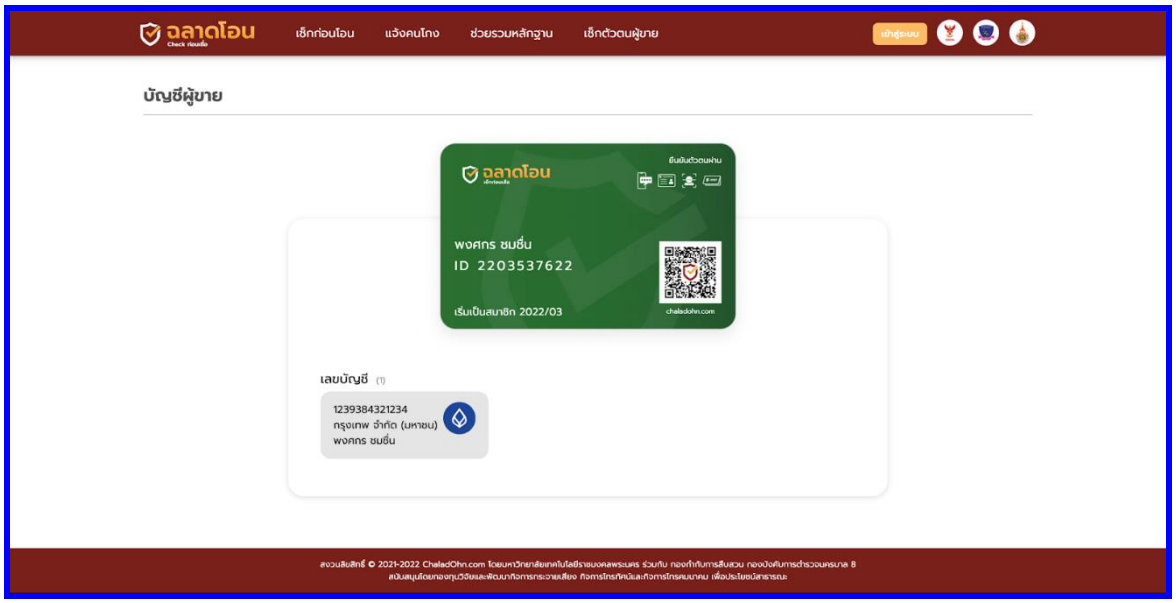
รูปที่ 7-29 หน้าจอแสดงผล “บัญชีนี้ไม่พบเรื่องร้องเรียน”

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	หน้าแสดงผลการสืบค้นข้อมูลบัญชีของผู้รับโอนที่ไม่พบเรื่องร้องเรียน			



รูปที่ 7-30 หน้าจอแสดงผล “บัญชีนี้พบเรื่องร้องเรียน”

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	หน้าแสดงผลการสืบค้นข้อมูลบัญชีของผู้รับโอนที่พบเรื่องร้องเรียน			

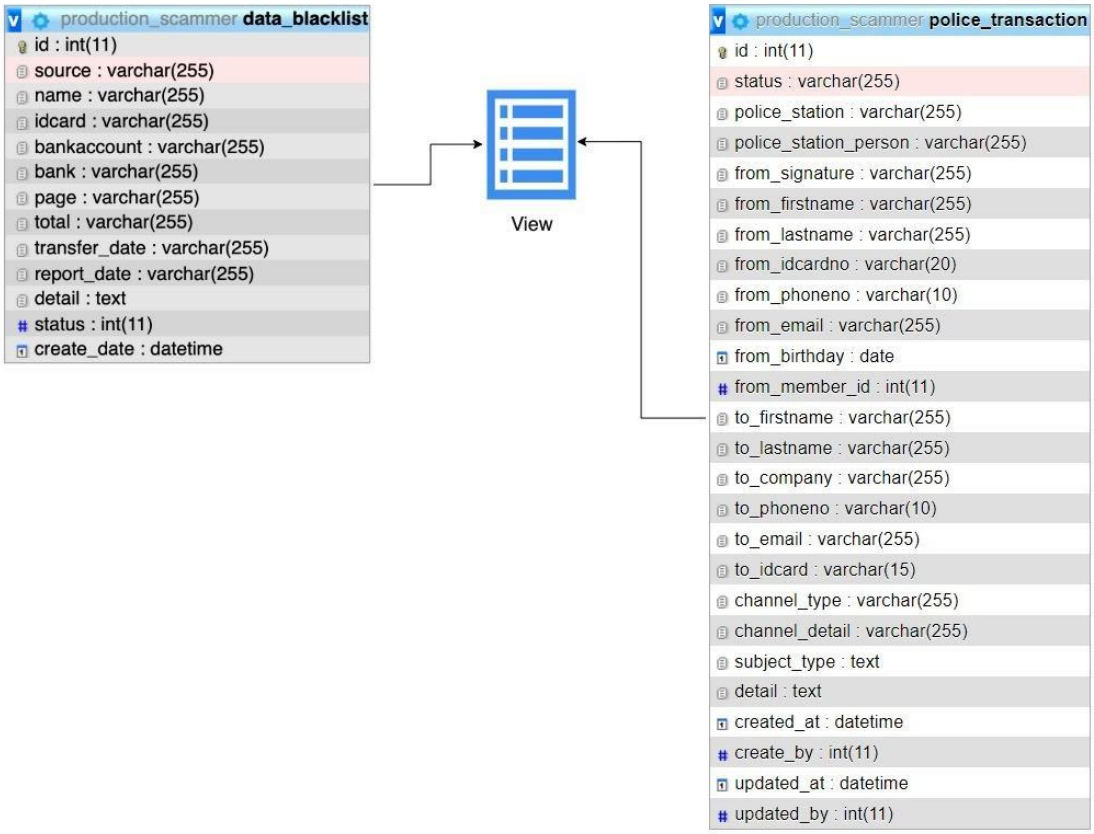


รูปที่ 7-31 หน้าจอแสดงบัญชีของผู้ขาย

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	กดเพื่อดาวน์โหลด QR Code			ระบบจะดาวน์โหลด QR Code มาไว้ที่อุปกรณ์ของผู้ใช้งาน

7.2.4 ระบบฐานข้อมูล

7.2.4.1 แผนภาพแสดงโครงสร้างการออกแบบฐานข้อมูล (ER-Diagram)



รูปที่ 7-32 ผังแสดงความสัมพันธ์ของระบบสืบค้นข้อมูลผู้กระทำความผิด

7.2.4.2 พจนานุกรมข้อมูล (Data Dictionary)

ตารางที่ 7-8 แสดงข้อมูลของตาราง data_blacklist

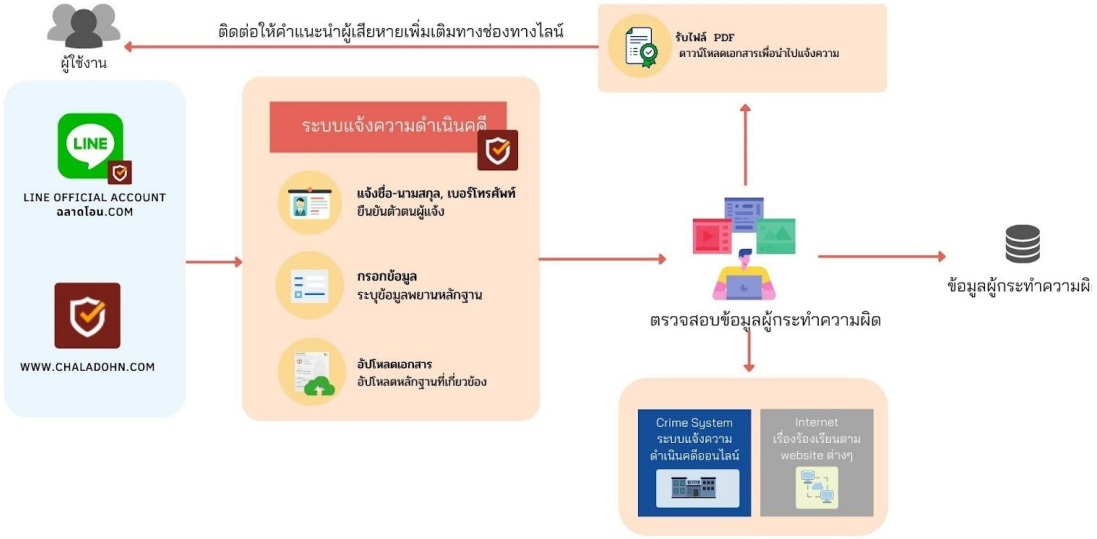
Column	Type	Null	Default	Description
id *(Primary)*	bigint(20)	No		คีย์หลัก
source	varchar(255)	No		ประเภทข้อมูล
name	varchar(255)	No		ชื่อ
id_card	varchar(255)	Yes	*NULL*	หมายเลขบัตรประชาชน
bankaccount	varchar(255)	Yes	*NULL*	เลขที่บัญชี
bank	varchar(255)	Yes	*NULL*	ธนาคาร
page	varchar(255)	Yes	*NULL*	ช่องทางติดต่อกับผู้โกง
total	varchar(255)	Yes	*NULL*	ยอดความเสียหาย
transter_date	varchar(255)	Yes	*NULL*	วันที่โอน
report_date	varchar(255)	Yes	*NULL*	วันที่แจ้ง
detail	text	Yes	*NULL*	รายละเอียด
status	int(11)	Yes	*NULL*	สถานะ

ตารางที่ 7-9 ข้อมูลของตาราง police_transaction

Column	Type	Null	Default	Description
id *(Primary)*	int(11)	No		คีย์หลัก
status	varchar(255)	No	waiting_for_approve	สถานะ
police_station	varchar(255)	Yes	*NULL*	สถานีตำรวจ
police_station_person	varchar(255)	Yes	*NULL*	ตำรวจผู้ดำเนินคดี
from_signature	varchar(255)	Yes	*NULL*	ลายเซ็นผู้แจ้ง
from_firstname	varchar(255)	Yes	*NULL*	ชื่อผู้แจ้ง
from_lastname	varchar(255)	Yes	*NULL*	นามสกุลผู้แจ้ง
from_idcardno	varchar(20)	Yes	*NULL*	หมายเลขบัตรประชาชนผู้แจ้ง
from_phoneno	varchar(10)	Yes	*NULL*	หมายเลขโทรศัพท์ผู้แจ้ง
from_email	varchar(255)	Yes	*NULL*	อีเมลผู้แจ้ง
from_birthday	date	Yes	*NULL*	วันเกิดผู้แจ้ง
from_member_id	int(11)	Yes	*NULL*	คีย์หลักสมาชิก
to_firstname	varchar(255)	Yes	*NULL*	ชื่อผู้กล่าวหา
to_lastname	varchar(255)	Yes	*NULL*	นามสกุลผู้ถูกกล่าวหา
to_phoneno	varchar(10)	Yes	*NULL*	หมายเลขโทรศัพท์ผู้ถูกกล่าวหา
to_email	varchar(255)	Yes	*NULL*	อีเมลผู้ถูกกล่าวหา
to_idcard	varchar(15)	Yes	*NULL*	เลขบัตรประชาชนผู้ถูกกล่าวหา
channel_type	varchar(255)	Yes	*NULL*	ช่องทาง
channel_detail	varchar(255)	Yes	*NULL*	รายละเอียดช่องทาง
subject_type	text	Yes	*NULL*	หัวข้อเรื่อง
detail	text	Yes	*NULL*	รายละเอียด
created_at	datetime	No		วันที่สร้าง
create_by	int(11)	No		สร้างโดย
updated_at	datetime	Yes	*NULL*	วันที่แก้ไข
updated_by	int(11)	Yes	*NULL*	แก้ไขโดย

7.3 การพัฒนาระบบแจ้งความดำเนินคดีมิจฉาชีพออนไลน์ที่ไม่สามารถระบุตัวตนได้

ระบบแจ้งความดำเนินคดีมิจฉาชีพออนไลน์ที่ไม่สามารถระบุตัวตนได้ เป็นระบบที่อำนวยความสะดวกให้กับผู้เสียหาย และพนักงานสอบสวน สามารถใช้ในการประกอบการแจ้งความดำเนินคดีธุรกรรมออนไลน์ที่ไม่สามารถระบุตัวตน รวมถึงเป็นการสรุปพฤติการณ์ ตรวจสอบหลักฐาน และพิจารณาหลักฐานเพื่อใช้ประกอบเอกสารการแจ้งความดำเนินดี ซึ่งจะเป็นการอำนวยความสะดวกต่อผู้ใช้งานและพนักงานสอบสวนในการใช้ประกอบการทำสำนวนคดีเกี่ยวกับธุรกรรมออนไลน์ที่ไม่สามารถระบุตัวตนได้



รูปที่ 7-33 ภาพรวมระบบแจ้งความดำเนินคดีมิจฉาชีพออนไลน์

7.3.1 แนวทางการพัฒนาระบบแจ้งความดำเนินคดีมิจฉาชีพออนไลน์ที่ไม่สามารถระบุตัวตนได้

การใช้งานระบบแจ้งความดำเนินคดีมิจฉาชีพออนไลน์ที่ไม่สามารถระบุตัวตนได้ เพื่อให้ข้อมูลผู้กระทำความผิดในคดีฉ้อโกงออนไลน์ หรือรวบรวมเอกสารประกอบการแจ้งความดำเนินคดีกับมิจฉาชีพออนไลน์ สามารถใช้งานได้ผ่าน 2 ช่องทาง

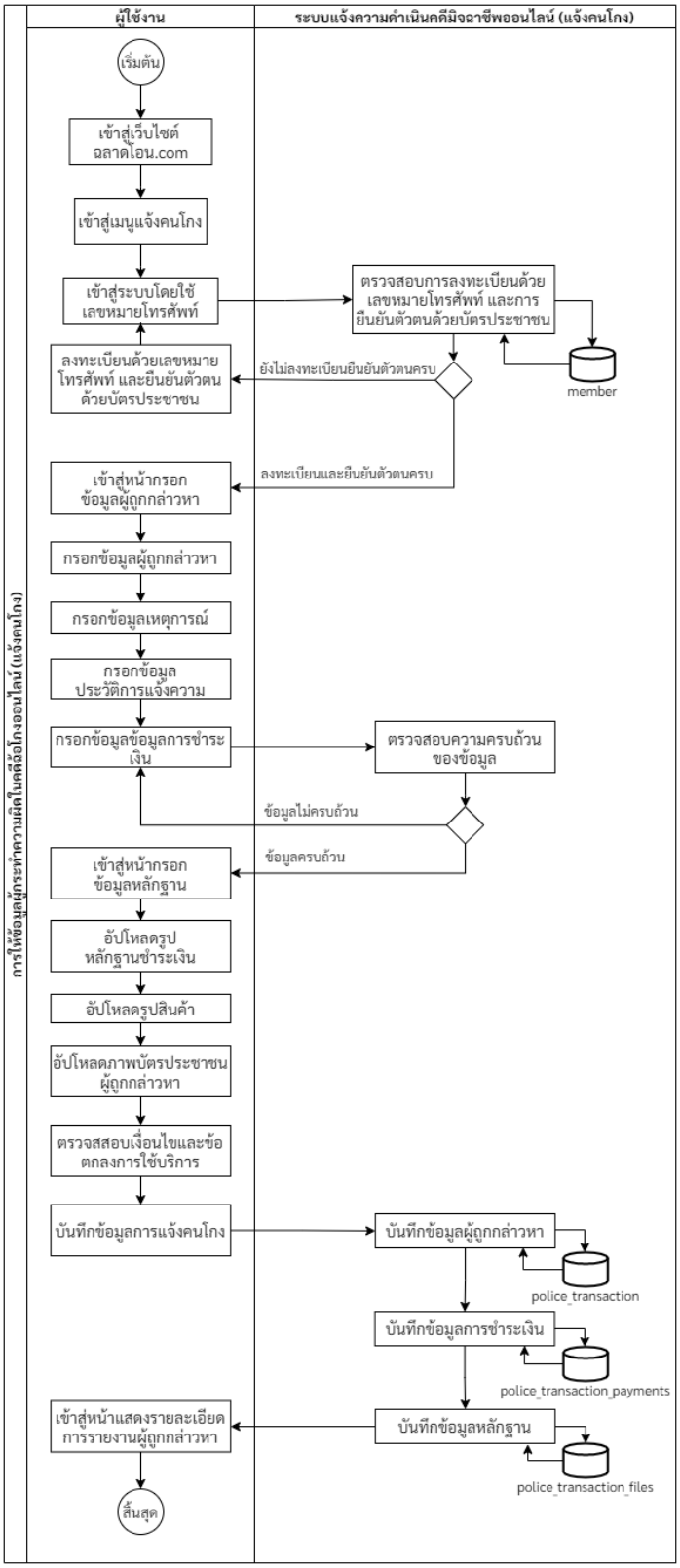
1) เว็บไซต์ฉลาดโอนดอทคอม
2) LINE Official Account ฉลาดโอน.com

โดยระบบจะอนุญาตให้ผู้ใช้งานระบบต้นแบบฯที่ได้มีการยืนยันตัวตนในระดับผู้ให้ข้อมูลผู้กระทำความผิดที่จะให้ข้อมูลเกี่ยวกับการกระทำผิดฐานฉ้อโกงของผู้กระทำผิดได้เท่านั้น และต้องมีการยืนยันตัวตนในระดับผู้เสียหายที่ต้องการแจ้งความดำเนินคดีจึงจะสามมารถรวบรวมเอกสารประกอบการแจ้งความดำเนินคดี เพื่อนำไปใช้สำหรับเป็นเอกสารประกอบการแจ้งความดำเนินคดีกับเจ้าหน้าที่ตำรวจพิจารณารับแจ้งความเพื่อดำเนินคดี

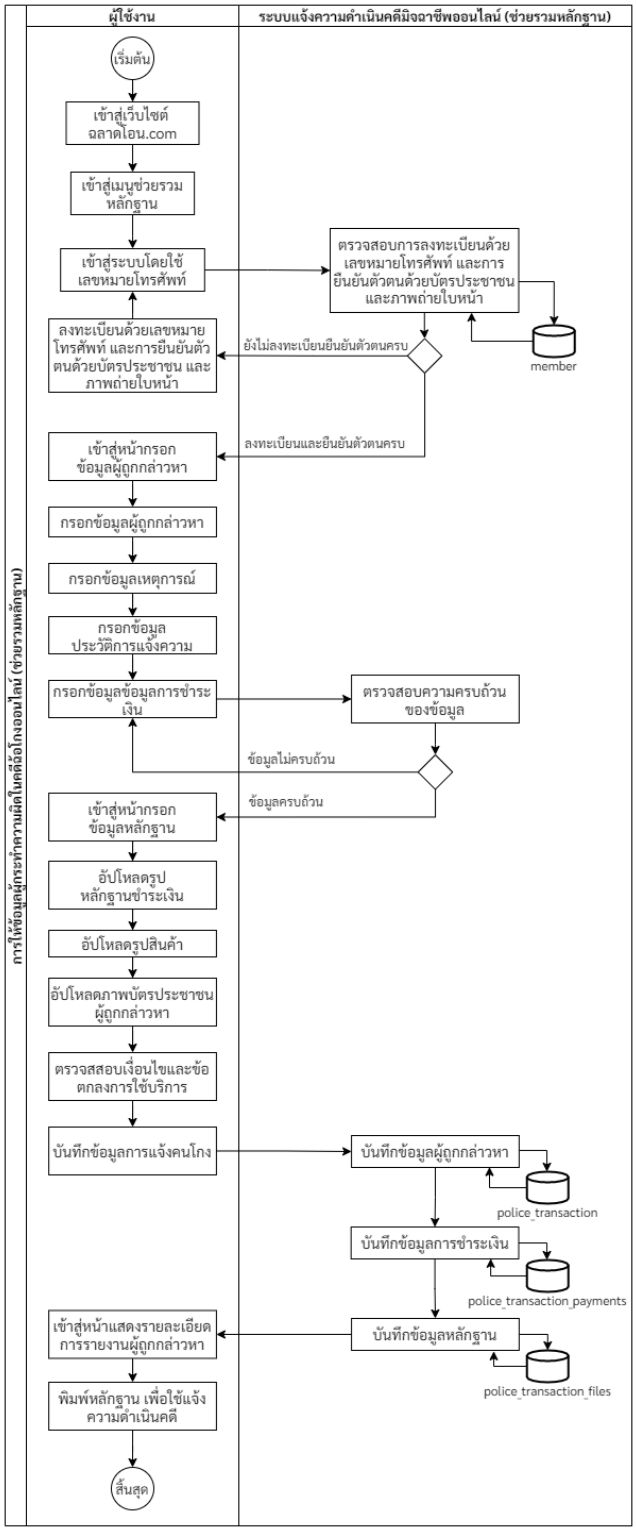
ระบบนี้จะช่วยประกอบเอกสารประกอบการแจ้งความดำเนินคดี เพื่อเพิ่มความสะดวกและรวดเร็วในการทำสำนวนคดี อีกทั้งยังสามารถรวบรวมผู้เสียหายร่วมที่กล่าวหาผู้ถูกกล่าวหาคนเดียวกันในคดีของผู้เสียหายรายอื่นๆ แบบอัตโนมัติ โดยเจ้าหน้าที่ที่เกี่ยวข้องเพียงแค่ค้นหาและตรวจสอบพยานหลักฐานของผู้แจ้งความในเบื้องต้นก่อนตัดสินใจรับแจ้งความ และสามารถตรวจสอบประวัติผู้ถูกกล่าวหาเพื่อพิจารณาแนวทางในการแจ้งอายัดบัญชีธนาคารหรือดำเนินคดีทางอาญาในขั้นตอนที่สูงขึ้นได้ต่อไป

7.3.2 กระบวนการทำงานของระบบ

โดยการให้ข้อมูลผู้กระทำความผิด ผู้ใช้งานจำเป็นต้องลงทะเบียนและยืนยันตัวตนในระดับการให้ข้อมูลผู้กระทำความผิด นั่นคือ การยืนยันตัวตนด้วยเลขหมายโทรศัพท์และบัตรประจำตัวประชาชน เพื่อเป็นการระบุตัวตนของผู้ให้ข้อมูล จากนั้นผู้ใช้งานจะกรอกข้อมูลเกี่ยวกับผู้กระทำความผิด ข้อมูลเกี่ยวกับการถูกฉ้อโกง อาทิ ช่องทางที่พบเห็นการประกาศขาย เหตุการณ์ ข้อมูลการโอนเงิน รวมทั้งหลักฐานการธุรกรรม เช่น หลักฐานการสนทนา หลักฐานการโอนเงิน จากนั้นจะมีเจ้าหน้าที่แอดมินตรวจสอบความถูกต้องและความครบถ้วนของข้อมูล หากเจ้าหน้าที่ตรวจสอบข้อมูลเรียบร้อย และอนุมัติข้อมูล ข้อมูลการแจ้งผู้กระทำความผิดนี้จะถูกบันทึกลงฐานข้อมูลผู้กระทำความผิด เพื่อใช้ตรวจสอบประวัติการกระทำความผิดของบุคคลที่ต้องการทำธุรกรรมออนไลน์ ป้องกันไม่ให้เกิดการฉ้อโกงออนไลน์ นอกจากนี้การรวบรวมเอกสารเพื่อประกอบการแจ้งความดำเนินคดี ผู้ใช้งานจำเป็นต้องยืนยันตัวตนด้วยอัตลักษณ์บุคคลโดยการใช้ภาพถ่ายใบหน้าบุคคลกับบัตรประจำตัวประชาชน จึงจะสามารถออกเอกสารประกอบการแจ้งความได้ ซึ่งมีกระบวนการเช่นเดียวกันกับการให้ข้อมูลผู้กระทำความผิด แต่ภายหลังจากที่เจ้าแอดมินอนุมัติรายละเอียดแล้ว ผู้ใช้งานจะสามารถพิมพ์เอกสารประกอบการแจ้งความในรูปแบบไฟล์PDF ได้ และระบบจะบันทึกข้อมูลการกระทำความผิดนี้ลงฐานข้อมูลผู้กระทำความผิด

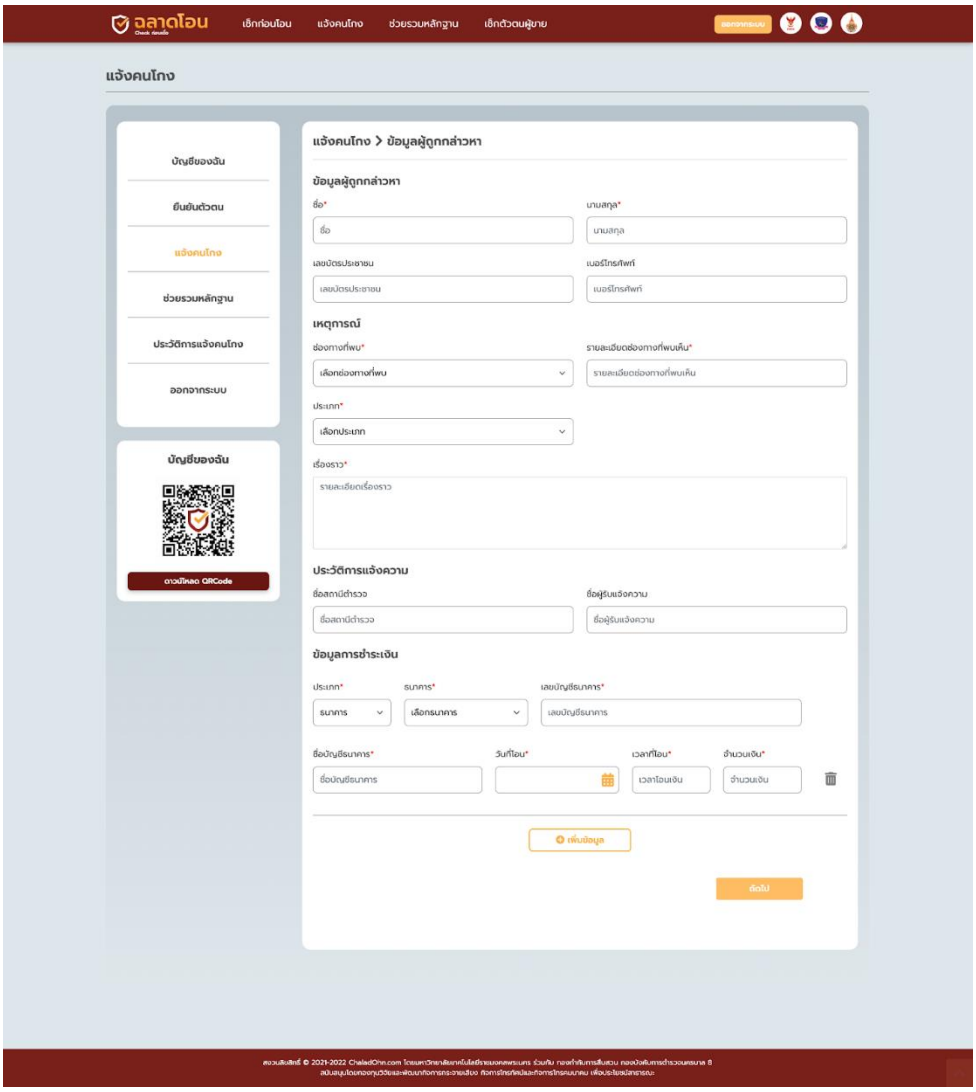


รูปที่ 7-34 ภาพรวมการทำงานของระบบแจ้งความดำเนินคดีมิจฉาชีพออนไลน์ ที่ไม่สามารถระบุตัวตนได้ (แจ้งคนโกง)



รูปที่ 7-35 ภาพรวมการทำงานของระบบแจ้งความดำเนินคดีมิจฉาชีพออนไลน์ ที่ไม่สามารถระบุตัวตนได้ (ช่วยรวมหลักฐาน)

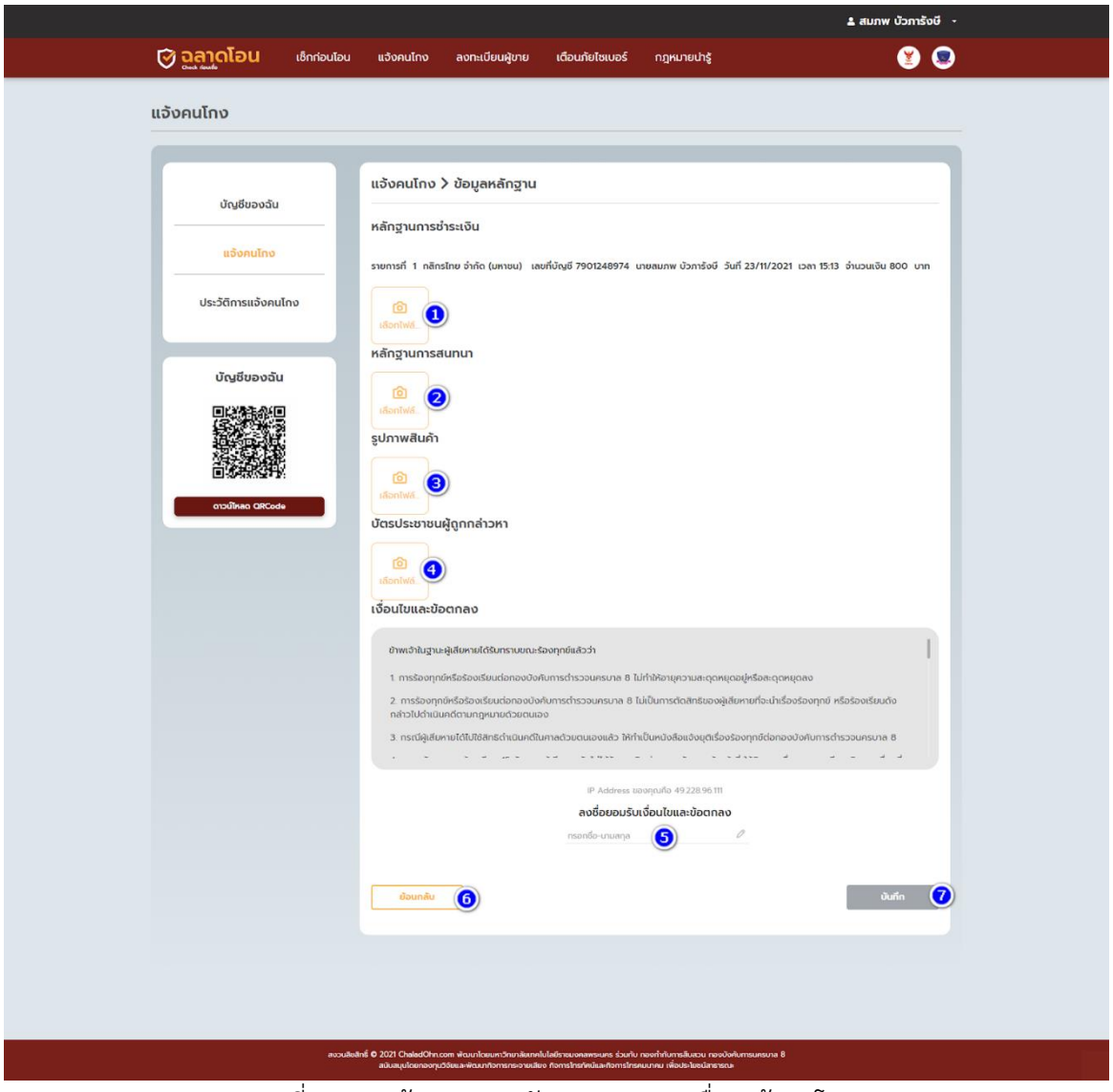
7.3.3 หน้าจอแสดงผลและรายละเอียดการทำงาน



รูปที่ 7-36 หน้าจอสำหรับกรอกข้อมูลผู้ถูกกล่าวหา

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	สำหรับระบุชื่อของผู้ถูกกล่าวหา	Yes	Text	
2	สำหรับระบุนามสกุลผู้ถูกกล่าวหา	Yes	Text	
3	หมายเลขบัตรประจำตัวประชาชนของผู้ถูกกล่าวหา		Numeric	
4	หมายเลขเบอร์โทรศัพท์ของผู้ถูกกล่าวหา		Numeric	
5	เลือกช่องทางที่พบเจอผู้ถูกกล่าวหา	Yes	Select	
6	กรอกรายละเอียดของช่องทางที่พบเจอผู้ถูกกล่าวหา	Yes	Text	
7	เลือกรูปแบบของการถูกโกง	Yes	Select	

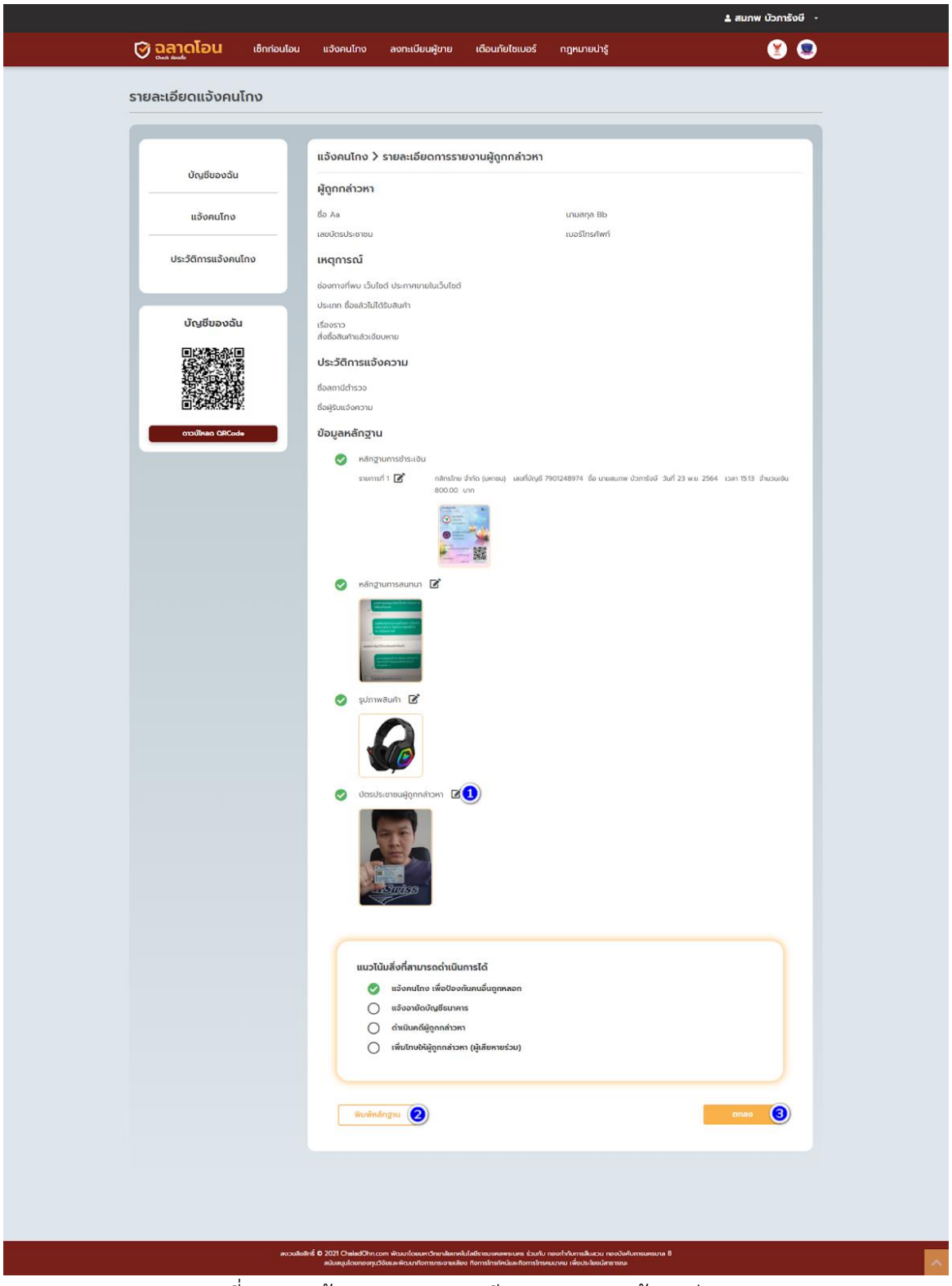
ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
8	กรอกเรื่องราวระหว่างตัวเองกับผู้ถูกกล่าวหา	Yes	Textarea	
9	กรอกชื่อสถานีตำรวจ	No	Text	
10	กรอกชื่อผู้รับแจ้งความ	No	Text	
11	เลือกประเภทของข้อมูลการชำระเงินของผู้ถูกกล่าวหา	Yes	Select	
12	เลือกธนาคารของผู้ถูกกล่าวหา	Yes	Select	
13	กรอกหมายเลขบัญชีธนาคารของผู้ถูกกล่าวหา	Yes	Numeric	
14	กรอกชื่อบัญชีธนาคารของผู้ถูกกล่าวหา	Yes	Text	
15	เลือกวันที่ ที่ทำรายการโอน	Yes	Date	
16	เลือกเวลา ที่ทำรายการโอน	Yes	Time	
17	กรอกจำนวนเงินที่ทำให้การโอนให้กับผู้ถูกกล่าวหา	Yes	Numeric	
18	กดเพื่อทำการลบข้อมูลเกี่ยวกับการชำระเงิน		Button	
19	กดเพื่อเพิ่มข้อมูลเกี่ยวกับการชำระเงิน		Button	
20	กดเพื่อไปยังหน้าเพิ่มข้อมูลหลักฐาน	Yes	Button	กดปุ่มเพื่อเข้าสู่ขั้นตอนต่อไป



รูปที่ 7-37 หน้าจอแนบหลักฐานประกอบเรื่องแจ้งคนโกง

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	กดเพื่อทำการเพิ่มหลักฐานเกี่ยวกับการชำระเงิน		Image	
2	กดเพื่อทำการเพิ่มหลักฐานเกี่ยวกับการสนทนา		Image	
3	กดเพื่อทำการเพิ่มหลักฐานเกี่ยวกับรูปสินค้า		Image	
4	กดเพื่อทำการเพิ่มหลักฐานเกี่ยวกับบัตรประจำตัวประชาชนของผู้ถูกกล่าวหา		Image	
5	ลงชื่อยอมรับเงื่อนไขและข้อตกลงเพื่อทำการแจ้งคนโกง	Yes	Text	

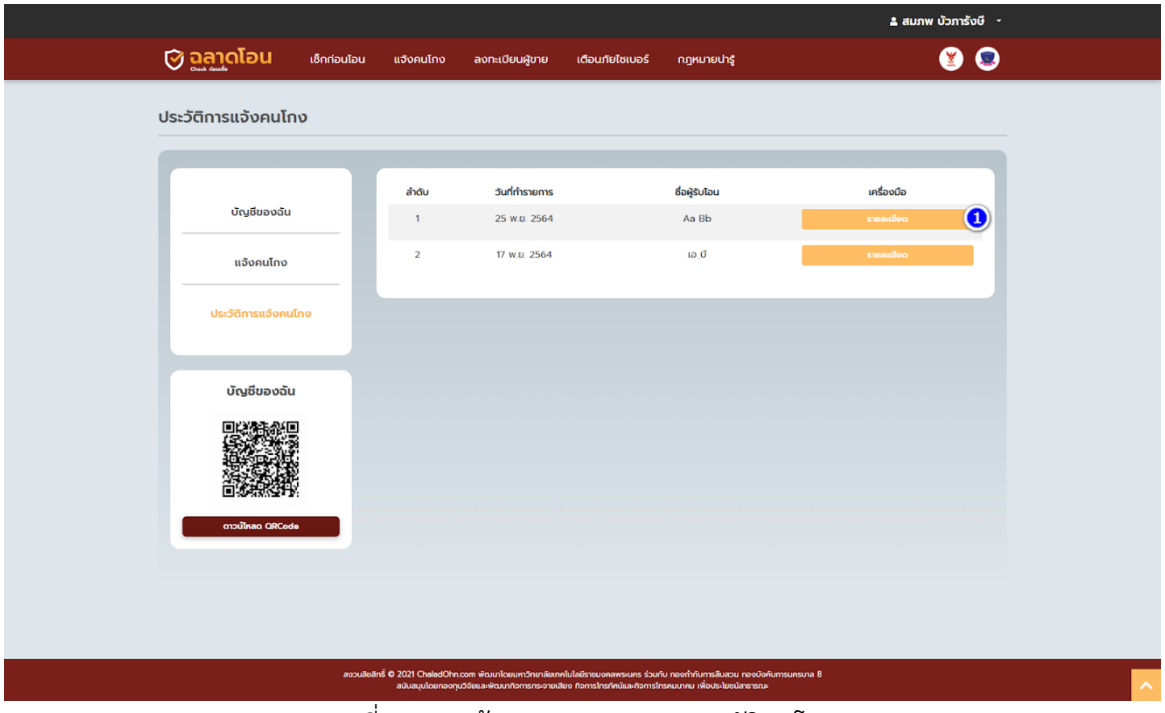
ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
6	กดเพื่อย้อนกลับไปแก้ไขข้อมูลในหน้าแรก		Button	ย้อนกลับไปหน้าแรกเพื่อทำการดูหรือแก้ไขข้อมูลของผู้ถูกกล่าวหา
7	กดเพื่อทำการบันทึกข้อมูลการแจ้งคนโกง	Yes	Button	บันทึกข้อมูลการแจ้งคนโกงเสร็จสิ้น



รูปที่ 7-38 หน้าจอแสดงรายละเอียดการรายงานผู้ถูกกล่าวหา

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	แก้ไขข้อมูลหลักฐานของผู้ถูกกล่าวหา		Button	
2	พิมพ์หลักฐานของผู้ถูกกล่าวหา		Button	

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
3	ปุ่มกดเพื่อทำการแจ้งเรื่องคนโกง	Yes	Button	แจ้งเรื่องคนโกงเสร็จสมบูรณ์

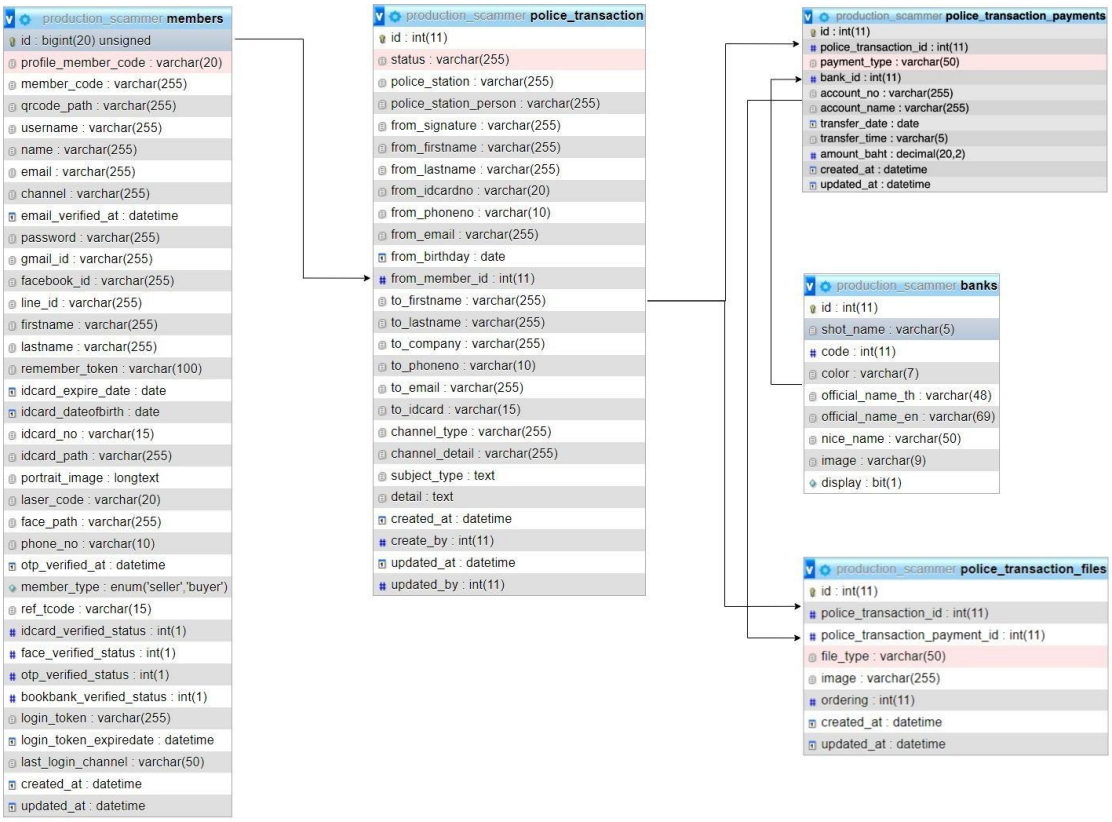


รูปที่ 7-39 หน้าจอแสดงรายการประวัติคนโกง

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	แสดงรายละเอียดเกี่ยวกับการแจ้งคนโกง		Button	หน้าต่างแสดงรายละเอียดทั้งหมดเกี่ยวกับการแจ้งคนโกง

7.3.4 ระบบฐานข้อมูล

7.3.4.1 แผนภาพแสดงโครงสร้างการออกแบบฐานข้อมูล (ER-Diagram)



รูปที่ 7-40 ผังแสดงความสัมพันธ์ของระบบแจ้งความดำเนินคดีมิจฉาชีพออนไลน์ที่ไม่สามารถระบุตัวตนได้

7.3.4.2 พจนานุกรมข้อมูล (Data Dictionary)

ตารางที่ 7-10 ข้อมูลของตาราง members

Column	Type	Null	Default	Description
id *(Primary)*	bigint(20)	No		คีย์หลัก
profile_member_code	varchar(20)	Yes	*NULL*	รหัสลำดับสมาชิก
member_code	varchar(255)	Yes	*NULL*	รหัสสมาชิก
qrcode_path	varchar(255)	Yes	*NULL*	รูปคิวอาร์โคด
username	varchar(255)	Yes	*NULL*	รหัส
name	varchar(255)	Yes	*NULL*	ชื่อ
email	varchar(255)	Yes	*NULL*	อีเมล
channel	varchar(255)	Yes	*NULL*	'line','facebook','gmail','kiosk'
email_verified_at	datetime	Yes	*NULL*	วันที่ยืนยันอีเมล
password	varchar(255)	Yes	*NULL*	รหัสผ่าน
gmail_id	varchar(255)	Yes	*NULL*	คีย์อีเมล
facebook_id	varchar(255)	Yes	*NULL*	คีย์เฟสบุ๊ค
line_id	varchar(255)	Yes	*NULL*	คีย์ไลน์ไอดี
firstname	varchar(255)	Yes	*NULL*	ชื่อ
lastname	varchar(255)	Yes	*NULL*	นามสกุล
remember_token	varchar(100)	Yes	*NULL*	รหัสโทเคน
idcard_expire_date	date	Yes	*NULL*	วันที่หมดอายุบัตรประชาชน
idcard_dateofbirth	date	Yes	*NULL*	วันเกิดบนบัตรประชาชน
idcard_no	varchar(15)	Yes	*NULL*	หมายเลขบัตรประชาชน
portrait_image	longtext	Yes	*NULL*	รูปภาพใบหน้าบนบัตรประชาชน
face_path	varchar(255)	Yes	*NULL*	รูปภาพใบหน้า
phone_no	varchar(10)	Yes	*NULL*	หมายเลขโทรศัพท์
otp_verified_at	datetime	Yes	*NULL*	วันที่ยืนยัน OTP
member_type	enum('seller', 'buyer')	Yes	*NULL*	ประเภทสมาชิก
ref_tcode	varchar(15)	Yes	*NULL*	
idcard_verified_status	int(1)	No		0=no verify,1=verified
face_verified_status	int(1)	No		0=no verify,1=verified
otp_verified_status	int(1)	No	0	0=no verify,1=verified
bookbank_verified_status	int(1)	No		0=no verify,1=verified
login_token	varchar(255)	Yes	*NULL*	รหัสโทเคนสำหรับตู้ Kiosk
login_token_expiredat	datetime	Yes	*NULL*	วันหมดอายุโทเคน

Column	Type	Null	Default	Description
e				
last_login_channel	varchar(50)	Yes	*NULL*	
created_at	datetime	Yes	*NULL*	วันที่สร้าง
updated_at	datetime	Yes	*NULL*	วันที่แก้ไข

ตารางที่ 7-11 ข้อมูลของตาราง police_transaction

Column	Type	Null	Default	Description
id *(Primary)*	int(11)	No		คีย์หลัก
status	varchar(255)	No	waiting_for_approve	สถานะ
police_station	varchar(255)	Yes	*NULL*	สถานีตำรวจ
police_station_person	varchar(255)	Yes	*NULL*	ตำรวจผู้ดำเนินคดี
from_signature	varchar(255)	Yes	*NULL*	ลายเซ็นผู้แจ้ง
from_firstname	varchar(255)	Yes	*NULL*	ชื่อผู้แจ้ง
from_lastname	varchar(255)	Yes	*NULL*	นามสกุลผู้แจ้ง
from_idcardno	varchar(20)	Yes	*NULL*	หมายเลขบัตรประชาชนผู้แจ้ง
from_phoneno	varchar(10)	Yes	*NULL*	หมายเลขโทรศัพท์ผู้แจ้ง
from_email	varchar(255)	Yes	*NULL*	อีเมลผู้แจ้ง
from_birthday	date	Yes	*NULL*	วันเกิดผู้แจ้ง
from_member_id	int(11)	Yes	*NULL*	คีย์หลักสมาชิก
to_firstname	varchar(255)	Yes	*NULL*	ชื่อผู้กล่าวหา
to_lastname	varchar(255)	Yes	*NULL*	นามสกุลผู้ถูกกล่าวหา
to_phoneno	varchar(10)	Yes	*NULL*	หมายเลขโทรศัพท์ผู้ถูกกล่าวหา
to_email	varchar(255)	Yes	*NULL*	อีเมลผู้ถูกกล่าวหา
to_idcard	varchar(15)	Yes	*NULL*	เลขบัตรประชาชนผู้ถูกกล่าวหา
channel_type	varchar(255)	Yes	*NULL*	ช่องทาง
channel_detail	varchar(255)	Yes	*NULL*	รายละเอียดช่องทาง
subject_type	text	Yes	*NULL*	หัวข้อเรื่อง
detail	text	Yes	*NULL*	รายละเอียด
created_at	datetime	No		วันที่สร้าง
create_by	int(11)	No		สร้างโดย
updated_at	datetime	Yes	*NULL*	วันที่แก้ไข
updated_by	int(11)	Yes	*NULL*	แก้ไขโดย

ตารางที่ 7-12 ข้อมูลของตาราง police_transaction_payments

Column	Type	Null	Default	Description
id *(Primary)*	int(11)	No		คีย์หลัก
police_transaction_id	int(11)	No		คีย์หลักการแจ้ง
payment_type	varchar(50)	Yes	*NULL*	ประเภทการโอน
bank_id	int(11)	Yes	*NULL*	คีย์หลักธนาคาร
account_no	varchar(255)	Yes	*NULL*	เลขบัญชีธนาคาร
account_name	varchar(255)	Yes	*NULL*	ชื่อบัญชีธนาคาร
transfer_date	date	Yes	*NULL*	วันที่โอน
transfer_time	varchar(5)	Yes	*NULL*	เวลาที่โอน
amount_baht	decimal(20,2)	Yes	*NULL*	จำนวนเงิน
created_at	datetime	Yes	*NULL*	วันที่สร้าง
updated_at	datetime	Yes	*NULL*	วันที่แก้ไข

ตารางที่ 7-13 ข้อมูลของตาราง banks

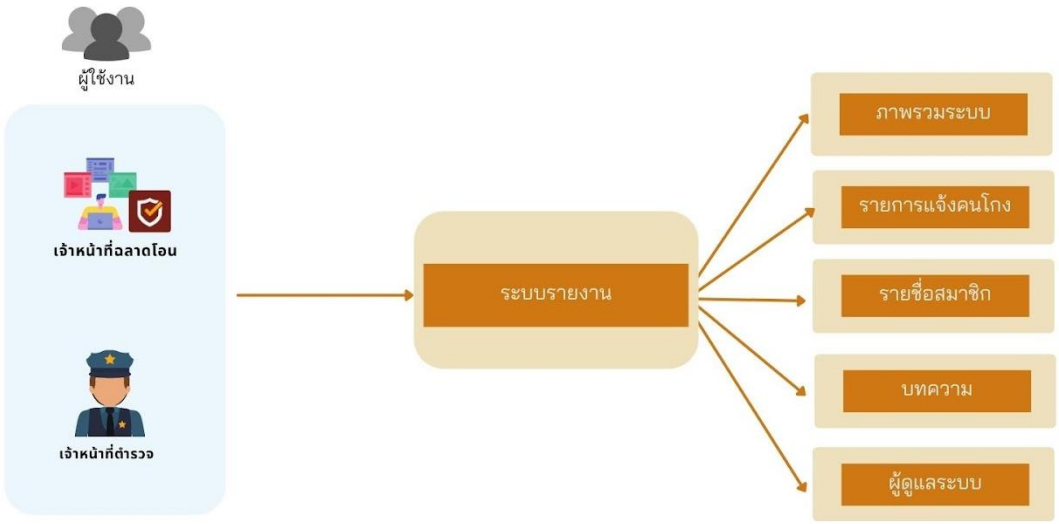
Column	Type	Null	Default	Description
id *(Primary)*	int(11)	No		คีย์หลัก
shot_name	varchar(5)	No		ชื่อย่อ
code	int(11)	No		รหัสธนาคาร
color	varchar(7)	Yes	*NULL*	รหัสสี
official_name_th	varchar(48)	No		ชื่อภาษาไทย
official_name_en	varchar(69)	No		ชื่อภาษาอังกฤษ
nice_name	varchar(50)	No		ชื่อเรียก
image	varchar(9)	No		รูปภาพ
display	bit(1)	No		สถานะการแสดง

ตารางที่ 7-14 ข้อมูลของตาราง police_transaction_files

Column	Type	Null	Default	Description
id *(Primary)*	int(11)	No		คีย์หลัก
police_transaction_id	int(11)	No		คีย์หลักการแจ้ง
police_transaction_payment_id	int(11)	Yes	*NULL*	คีย์หลักการโอนเงิน
file_type	varchar(50)	Yes	*NULL*	ประเภทไฟล์
image	varchar(255)	Yes	*NULL*	รูปภาพ
ordering	int(11)	Yes	0	ลำดับ
created_at	datetime	Yes	*NULL*	วันที่สร้าง
updated_at	datetime	Yes	*NULL*	วันที่แก้ไข

7.4 การพัฒนาระบบแสดงผลรายงาน

ระบบแสดงผลรายงาน เป็นระบบที่แสดงผลรายงานและสถิติต่าง ๆ สำหรับผู้บริหาร และผู้ที่เกี่ยวข้อง รวมถึงรายละเอียดข้อมูลการลงทะเบียนยืนยันตัวตนของผู้ใช้งานระบบต้นแบบฯ ตลอดจนรายละเอียดข้อมูลการแจ้งข้อมูลผู้กระทำความผิด และข้อมูลสำหรับประกอบเอกสารการแจ้งความดำเนินคดี นอกจากนี้ระบบแสดงผลรายงานนี้ยังใช้บริหารจัดการเว็บไซต์ส่วนของบทความอีกด้วย



รูปที่ 7-41 ภาพรวมระบบรายงาน

การแสดงผลรายงาน และข้อมูลสถิติการใช้งานระบบต้นแบบฯ เป็นส่วนสำคัญในการกำหนดทิศทางของการปรับปรุง ออกแบบ และพัฒนาระบบต้นแบบฯนี้ให้มีประสิทธิภาพต่อผู้ใช้งาน ทั้งนี้ การออกแบบและพัฒนาระบบแสดงผลรายงานนั้น คณะผู้วิจัยได้พัฒนาให้ระบบแสดงผลรายงานนี้ แสดงผลข้อมูลและสถิติต่างๆ ที่เกี่ยวข้องออกมาในรูปแบบของตัวเลขและกราฟ โดยระบบแสดงผลรายงานจะแบ่งออกเป็น 5 ส่วน ได้แก่

1. ภาพรวมระบบ
2. รายงานแจ้งคนโกง
3. บทความ
4. รายชื่อสมาชิก
5. ผู้ดูแลระบบ

ภาพรวมระบบ

ภาพรวมระบบเป็นการแสดงข้อมูลในส่วนของผลลัพธ์การใช้งานที่มีความเกี่ยวข้องกับระบบต้นแบบฯ โดยแสดงข้อมูลเกี่ยวกับสมาชิกที่มีการลงทะเบียนและการยืนยันตัวตนที่มีการจำแนกตามการยืนยันตัวตนและสิทธิ์การใช้งานระบบต้นแบบฯ รวมถึงสถิติเกี่ยวกับการใช้งานระบบต้นแบบฯของผู้ใช้งานที่ได้มีการเข้ามาใช้งานระบบต้นแบบฯ อาทิ การตรวจสอบข้อมูลผู้กระทำความผิด การตรวจสอบผู้ขายที่มีการยืนยันตัวตนในระบบต้นแบบฯ การให้ข้อมูลผู้กระทำความผิด ตลอดจนการรวบรวมเอกสารเพื่อประกอบการแจ้งความดำเนินคดี

รายงานแจ้งคนโกง

รายงานแจ้งคนโกงเป็นส่วนของการแสดงรายการรายงานแจ้งคนโกงที่มีผู้ใช้งานแจ้งข้อมูลเข้ามาในระบบ โดยแสดงถึงรายละเอียดของผู้แจ้งหรือผู้ให้ข้อมูล ตลอดจนข้อมูลเกี่ยวกับผู้กระทำความผิด พฤติการณ์การกระทำความผิด และหลักฐานที่มีความเกี่ยวข้องกับการฉ้อโกง อาทิ หลักฐานการสนทนา หลักฐานการโอนเงิน

บทความ

สำหรับระบบแสดงผลรายงานนี้ สามารถบริหารจัดการในส่วนของบทความบนเว็บไซต์ได้อีกด้วย ซึ่งการบริหารจัดการในส่วนนี้ ระบบจะสามารถจัดหมวดหมู่ของบทความ ตลอดจนการสร้าง หรือแก้ไขบทความที่ต้องการเผยแพร่บนเว็บไซต์

รายชื่อสมาชิก

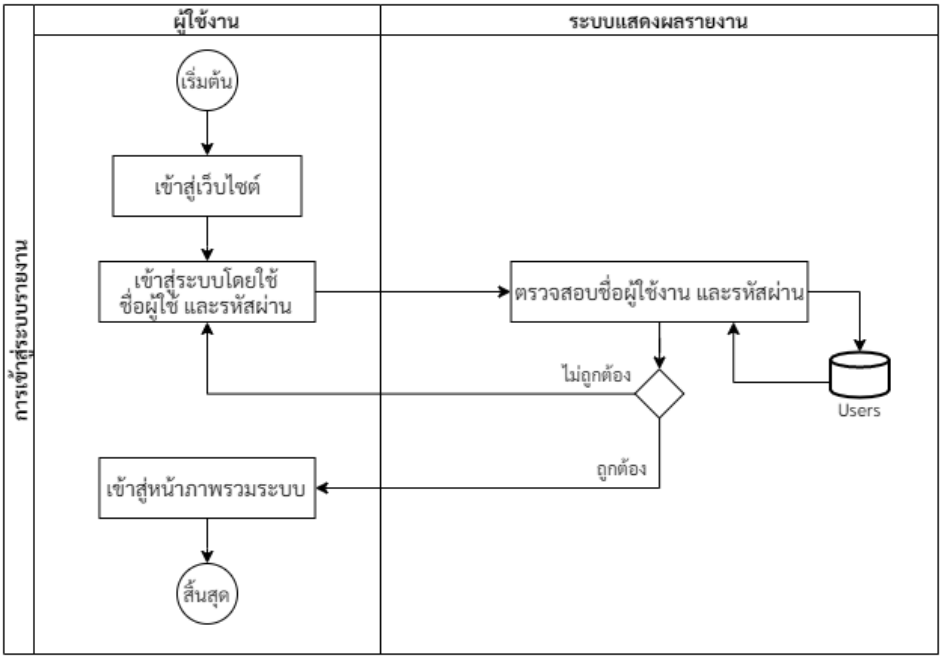
รายชื่อสมาชิกเป็นส่วนของการแสดงผลรายละเอียดเกี่ยวกับผู้ลงทะเบียนและยืนยันตัวตนในระบบต้นแบบฯ โดยแสดงข้อมูลเกี่ยวกับจำนวนสมาชิกที่มีการลงทะเบียนยืนยันตัวตน รวมทั้งรายละเอียดชื่อ นามสกุล, หลักฐานที่ใช้สำหรับยืนยันตัวตน และวันที่มีการลงทะเบียนในระบบต้นแบบฯ ครั้งแรก

ผู้ดูแลระบบ

สำหรับส่วนผู้ดูแลระบบ ในส่วนนี้จะแสดงรายละเอียดเกี่ยวกับผู้ที่มีสิทธิ์ในการใช้งานระบบแสดงผลรายงาน โดยมีการแสดงข้อมูล อาทิ ชื่อ นามสกุล, สถานะการใช้งาน และสิทธิ์การใช้งานระบบของแต่ละบัญชี

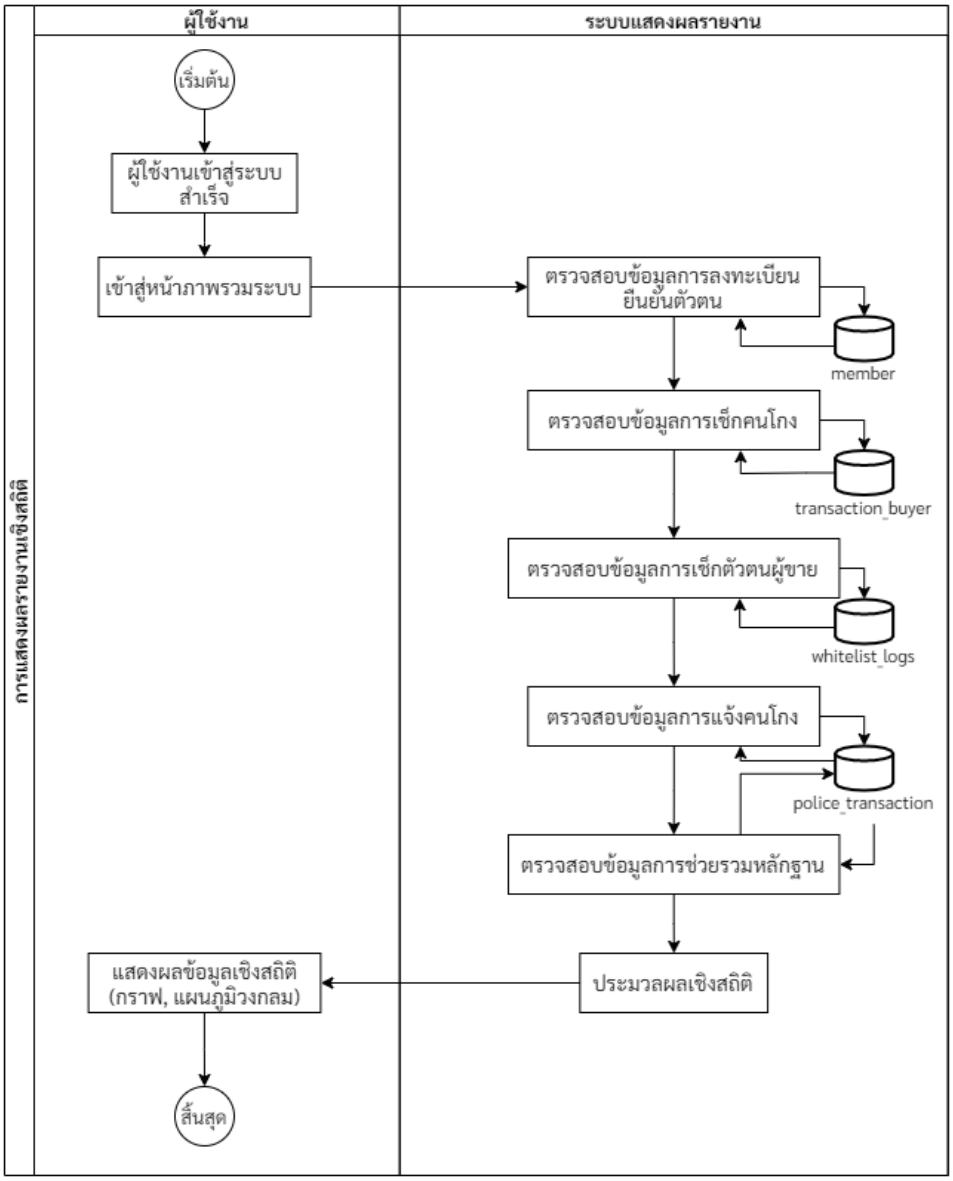
7.4.2 กระบวนการทำงานของระบบแสดงรายงาน

ผู้ใช้งานสามารถเข้าใช้งานระบบแสดงผลรายงานได้ผ่านทางเว็บไซต์ โดยผู้ใช้งานจำเป็นต้องเข้าสู่ระบบผ่านการกรอกข้อมูลชื่อผู้ใช้งาน และรหัสผ่านสำหรับเข้าใช้งาน หลังจากนั้นระบบจะตรวจสอบความถูกต้องของชื่อผู้ใช้งานและรหัสผ่านสำหรับเข้าสู่ระบบ ในกรณีที่ไม่ถูกต้องจะต้องมีการแสดงข้อความแจ้งเตือนเพื่อให้ผู้ใช้งานกรอกข้อมูลใหม่อีกครั้ง หากระบบตรวจสอบแล้วข้อมูลชื่อผู้ใช้งาน และรหัสผ่านผู้ใช้งาน ถูกต้องจะทำการเข้าสู่ระบบให้ผู้ใช้งานสำเร็จและแสดงหน้าภาพรวมระบบ ดังรูป 7-42



รูปที่ 7-42 ภาพรวมการทำงานของการเข้าสู่ระบบแสดงรายงาน

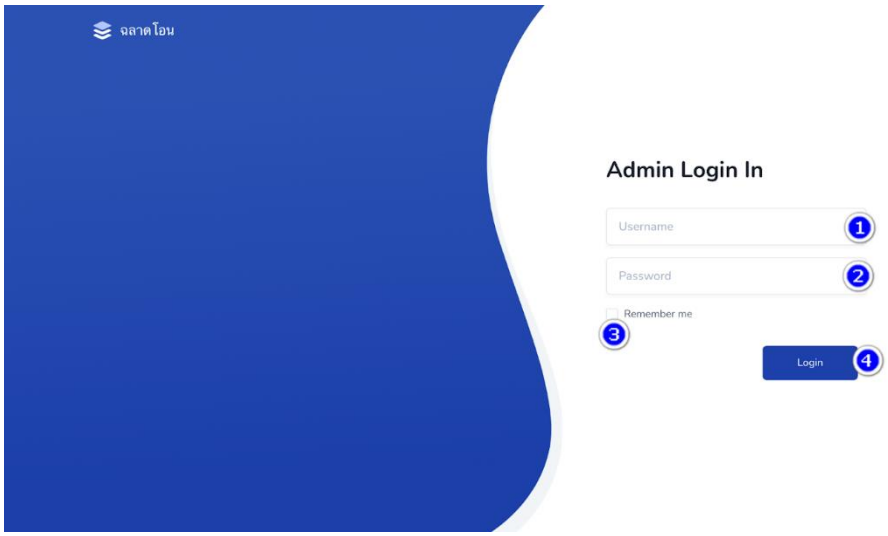
เมื่อผู้ใช้งานเข้าสู่ระบบสำเร็จ ระบบจะนำข้อมูลจากฐานข้อมูลที่เกี่ยวข้อง อาทิ การตรวจสอบข้อมูลผู้กระทำความผิด, การตรวจสอบข้อมูลผู้ขายที่ได้มีการยืนยันตัวตนในระบบต้นแบบฯ , การให้ข้อมูลผู้กระทำความผิด และการรวบรวมเอกสารเพื่อนำไปประกอบการแจ้งความดำเนินคดี และแสดงผลที่ส่วนของภาพรวมระบบในรูปแบบตัวเลข แผนภูมิเส้น และแผนภูมิวงกลม ดังรูป 7-43



รูปที่ 7-43 ภาพรวมการทำงานของระบบแสดงผลรายงาน

7.4.3 หน้าจอแสดงผลและรายละเอียดการทำงาน

เมื่อเข้ามาที่ระบบ จะแสดงหน้าจอสำหรับการล็อกอินเข้าสู่ระบบ โดยจะต้องกรอก Username และ Password ให้ถูกต้อง และกดปุ่มล็อกอิน (Login) เพื่อเข้าสู่ระบบ ดังรูปที่ 7-44



รูปที่ 7-44 หน้าจอเข้าสู่ระบบฉลาดโอน

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	สำหรับระบุชื่อผู้ใช้งาน	Yes	Text	
2	สำหรับระบุรหัสผ่าน	Yes	Text	
3	สำหรับจดจำเข้าสู่ระบบ	No	Checkbox	
4	ปุ่ม Login	Yes	Button	ระบบจะตรวจสอบข้อมูล ชื่อผู้ใช้งานและรหัสผ่านผู้ใช้งานก่อน ในกรณีที่ไม่ถูกต้องจะต้องมีการแสดงข้อความแจ้งเตือนเพื่อให้ผู้ใช้งานกรอกข้อมูลใหม่อีกครั้ง

เมื่อผู้ใช้งานล็อกอินเข้าสู่ระบบมาแล้ว จะพบกับหน้าบัญชีการใช้งาน ซึ่งจะเป็นหน้าของภาพรวม โดยแบ่งออกเป็น 5 ส่วน ได้แก่

1) ภาพรวมระบบ
2) รายการแจ้งคนโกง
3) บทความ
4) รายชื่อสมาชิก
5) ผู้ดูแลระบบ

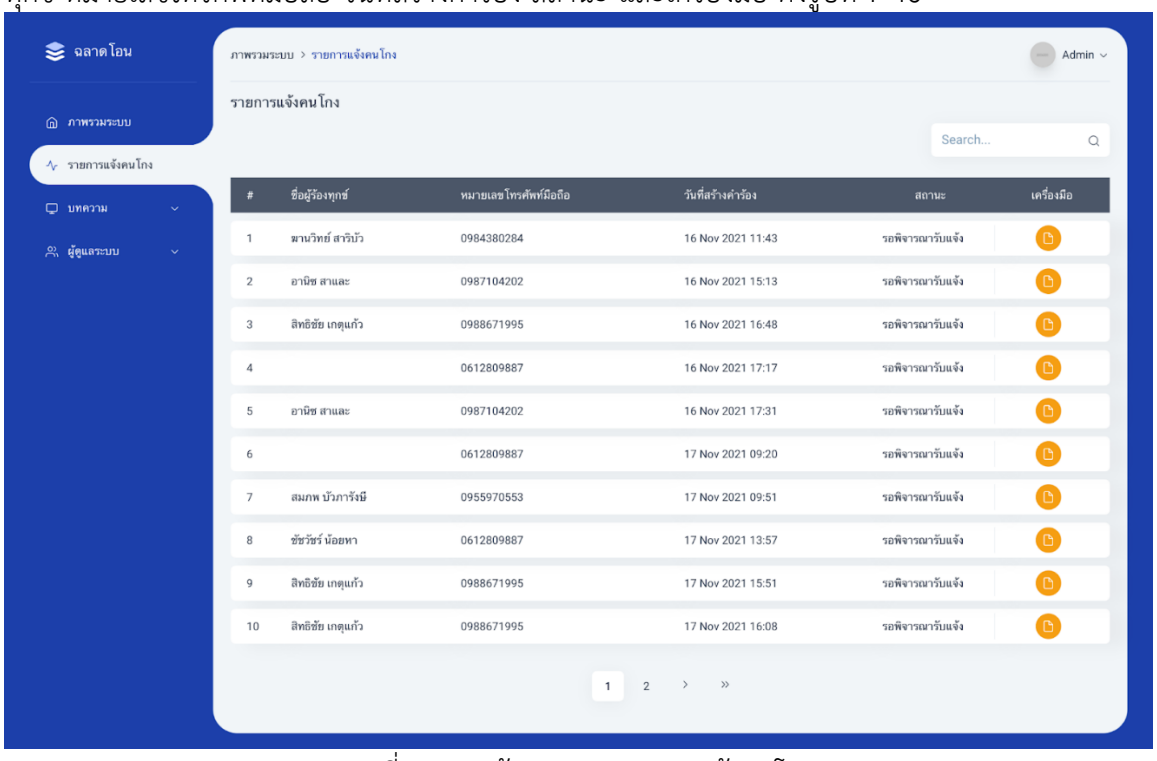
ภาพรวมระบบ

หน้าภาพรวมระบบจะแสดงข้อมูลสถิติต่างๆ ทั้งหมด เช่น จำนวนสมาชิกทั้งหมด จำนวนผู้ที่ยังไม่ได้ยืนยันตัวตน จำนวนผู้ที่ยืนยันตัวตนแล้ว จำนวนรายการแจ้งคนโกงทั้งหมด จำนวนรายการเช็กก่อนโอน และจำนวนรายการแจ้งโอนผ่านระบบ เป็นต้น แสดงดังรูปที่ 7-45

รูปที่ 7-45 หน้าจอแสดงภาพรวมระบบ

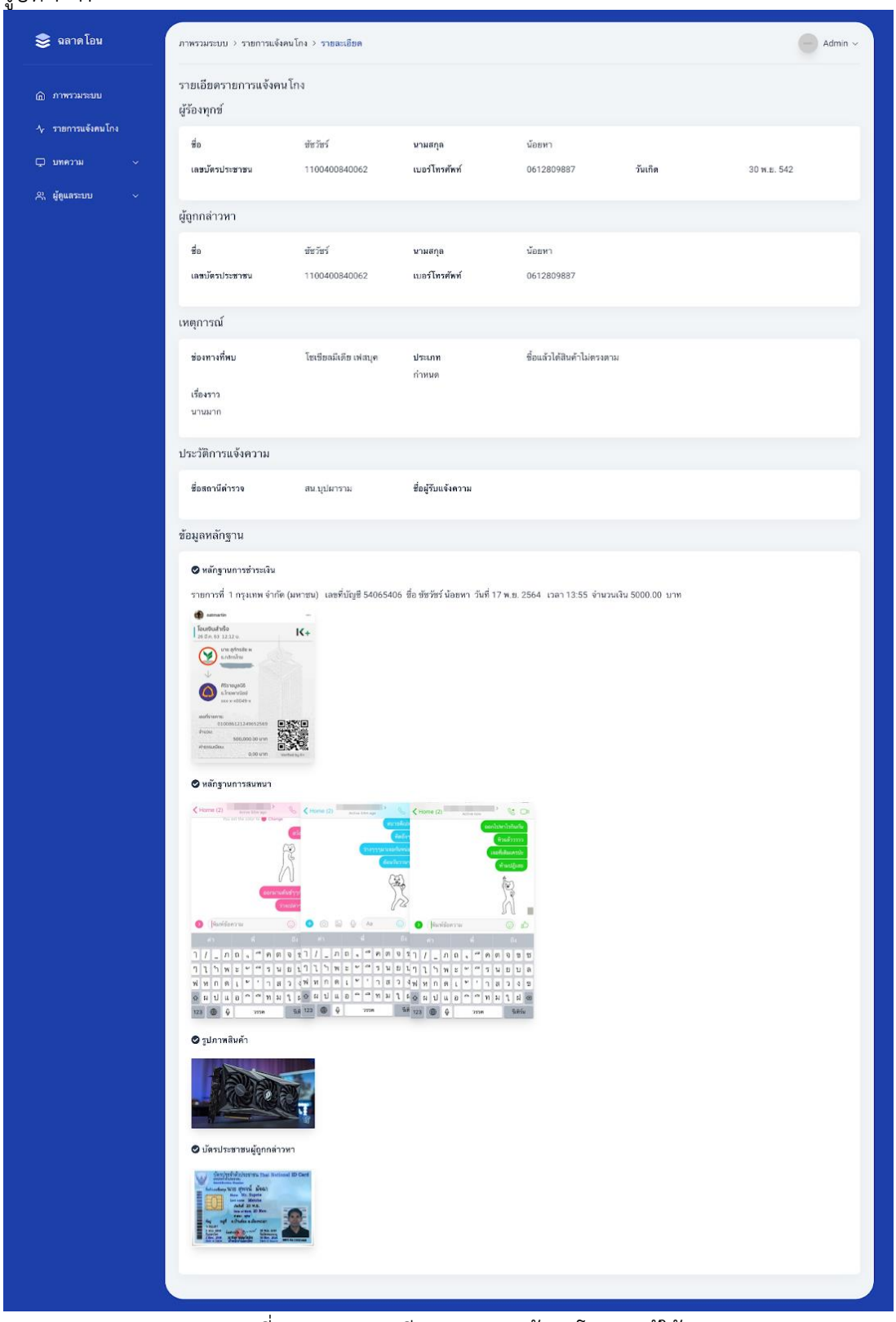
รายการแจ้งคนโกง

ในส่วนของรายการแจ้งคนโกงจะแสดงรายการที่มีการแจ้งเข้ามาในระบบ ประกอบด้วยชื่อผู้ร้องทุกข์ หมายเลขโทรศัพท์มือถือ วันที่สร้างคำร้อง สถานะ และเครื่องมือ ดังรูปที่ 7-46



รูปที่ 7-46 หน้ารายงานรายการแจ้งคนโกง

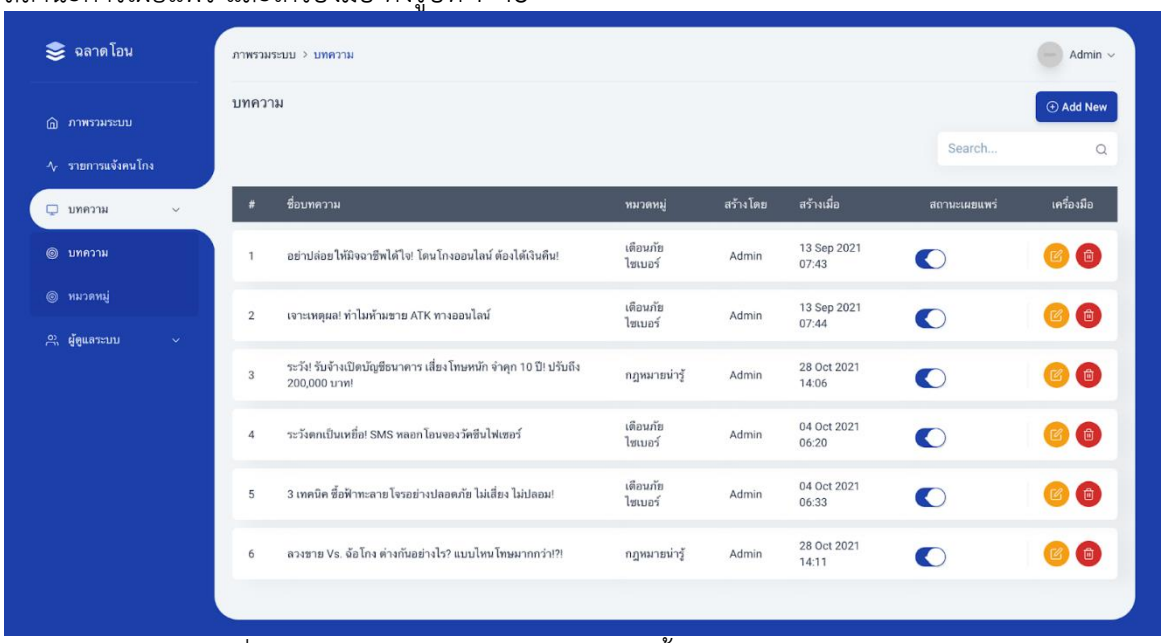
ผู้ใช้งานสามารถกดเพิ่มดูรายละเอียดรายการแจ้งคนโกง ได้จากแถบเครื่องมือ และแสดงข้อมูลดังรูปที่ 7-47



รูปที่ 7-47 รายละเอียดของการแจ้งคนโกงของผู้ใช้งาน

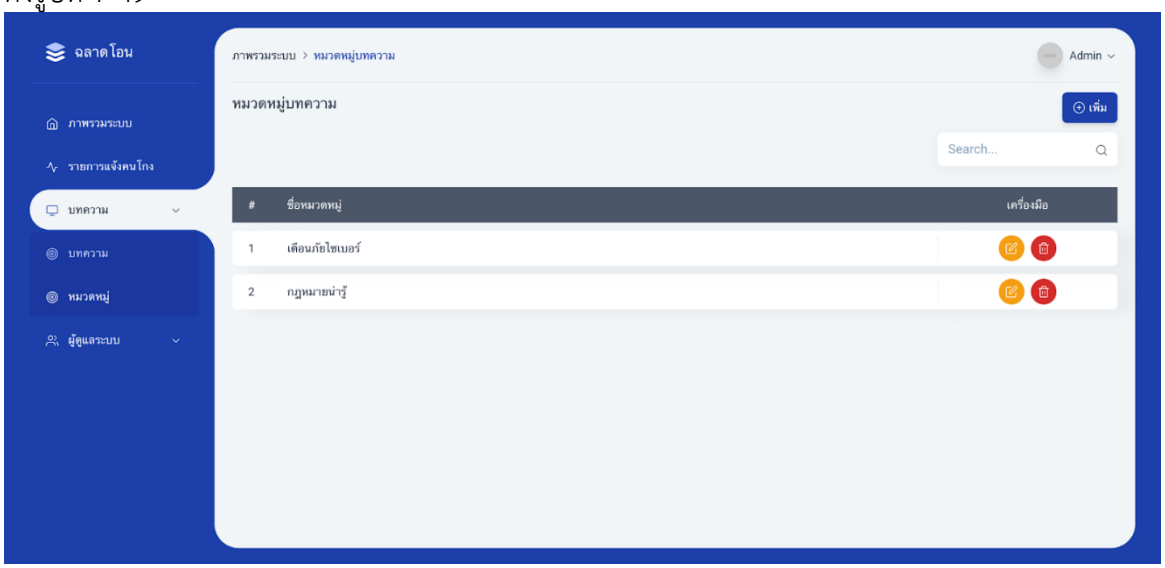
บทความ

หน้าบทความจะแบ่งเป็น 2 ส่วนคือ บทความและหมวดหมู่ ส่วนแรกเป็นบทความต่าง ๆ ที่ได้มีการเขียนไว้ทั้งหมด แสดงรายละเอียดเป็นตารางประกอบด้วย ชื่อบทความ หมวดหมู่ สร้างโดย สร้างเมื่อ สถานะการเผยแพร่ และเครื่องมือ ดังรูปที่ 7-48



รูปที่ 7-48 หน้าจอแสดงรายการบทความทั้งหมดบนเว็บไซต์ฉลาดโอน

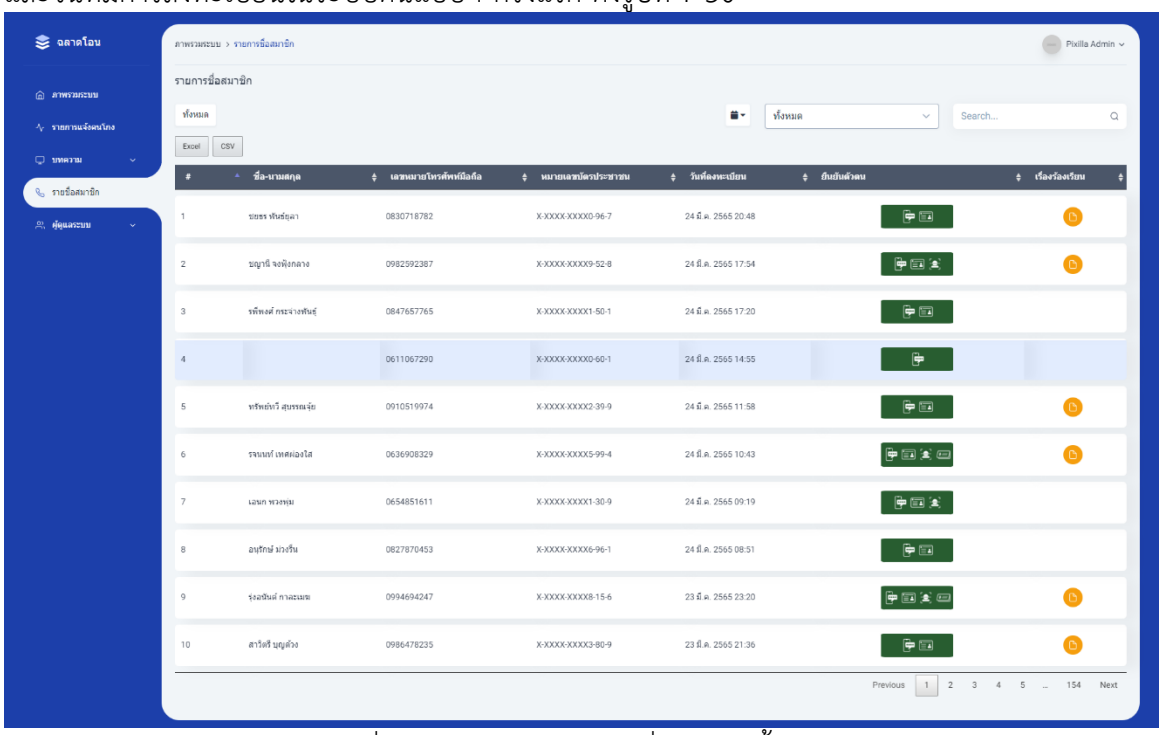
ในส่วนของหมวดหมู่บทความจะแสดงหมวดหมู่ของบทความที่มีอยู่และสามารถเพิ่ม หรือแก้ไขได้ ดังรูปที่ 7-49



รูปที่ 7-49 หน้าจอแสดงหมวดหมู่ของบทความบนเว็บไซต์ฉลาดโอน

รายชื่อสมาชิก

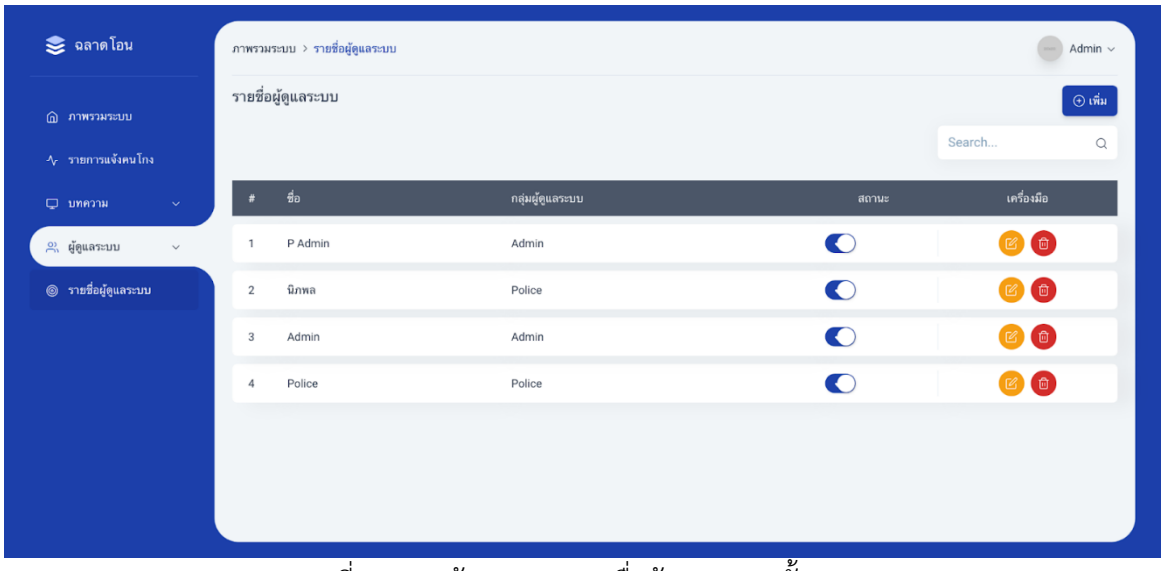
ในส่วนของรายชื่อสมาชิกเป็นส่วนของการแสดงผลรายละเอียดเกี่ยวกับข้อมูลเกี่ยวกับจำนวนสมาชิกที่มีการลงทะเบียนยืนยันตัวตน รวมทั้งรายละเอียดชื่อ นามสกุล, หลักฐานที่ใช้สำหรับยืนยันตัวตน และวันที่มีการลงทะเบียนในระบบต้นแบบฯ ครั้งแรก ดังรูปที่ 7-50



รูปที่ 7-50 หน้าจอแสดงรายชื่อสมาชิกทั้งหมด

ผู้ดูแลระบบ

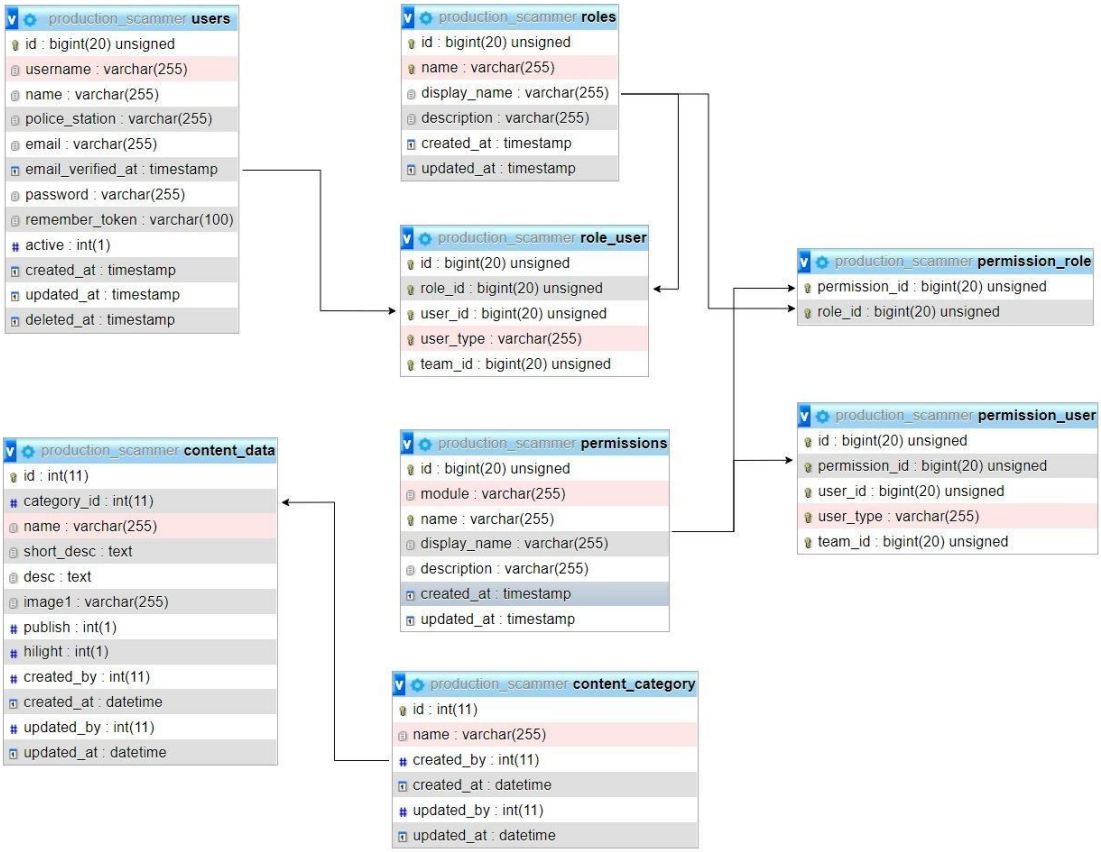
ในส่วนของผู้ดูแลระบบประกอบไปด้วยรายชื่อผู้ดูแลระบบ โดยจะแสดงรายละเอียดต่างๆ ในรูปแบบตาราง สามารถเพิ่ม แก้ไขหรือลบได้ ดังรูปที่ 7-51



รูปที่ 7-51 หน้าจอแสดงรายชื่อผู้ดูแลระบบทั้งหมด

7.4.4 ระบบฐานข้อมูล

7.4.4.1 แผนภาพแสดงโครงสร้างการออกแบบฐานข้อมูล (ER-Diagram)



รูปที่ 7-52 ผังแสดงความสัมพันธ์ของระบบ

7.4.4.2 พจนานุกรมข้อมูล (Data Dictionary)

ตารางที่ 7-15 ข้อมูลของตาราง users

Column	Type	Null	Default	Description
id *(Primary)*	bigint(20)	No		คีย์หลัก
username	varchar(255)	No		รหัสผู้ใช้งาน
name	varchar(255)	No		ชื่อผู้ใช้งาน
police_station	varchar(255)	Yes	*NULL*	สถานีตำรวจ
email	varchar(255)	No		อีเมล
email_verified_at	timestamp	Yes	*NULL*	วันที่ยืนยันอีเมล
password	varchar(255)	No		รหัสผ่าน
remember_token	varchar(100)	Yes	*NULL*	โทเคน
active	int(1)	No	0	สถานะ
created_at	timestamp	Yes	*NULL*	วันที่สร้าง
updated_at	timestamp	Yes	*NULL*	วันที่แก้ไข
deleted_at	timestamp	Yes	*NULL*	วันที่ลบ

ตารางที่ 7-16 ข้อมูลของตาราง content_category

Column	Type	Null	Default	Description
id *(Primary)*	int(11)	No		คีย์หลัก
name	varchar(255)	Yes	*NULL*	ชื่อ
created_by	int(11)	No		สร้างโดย
created_at	datetime	No		วันที่สร้าง
updated_by	int(11)	No		แก้ไขโดย

ตารางที่ 7-17 ข้อมูลของตาราง content_data

Column	Type	Null	Default	Description
id *(Primary)*	int(11)	No		คีย์หลัก
category_id	int(11)	No		คีย์หลักหมวดหมู่
name	varchar(255)	Yes	*NULL*	ชื่อ
short_desc	text	Yes	*NULL*	รายละเอียดขนาดสั้น
desc	text	Yes	*NULL*	รายละเอียด
image1	varchar(255)	Yes	*NULL*	รูปภาพ
publish	int(1)	No	1	สถานะการแสดง
hilight	int(1)	No	0	สถานะไฮไลท์
created_by	int(11)	No		สร้างโดย
created_at	datetime	No		วันที่สร้าง

Column	Type	Null	Default	Description
updated_by	int(11)	No		แก้ไขโดย
updated_at	datetime	No		วันที่แก้ไข

ตารางที่ 7-18 ข้อมูลของตาราง roles

Column	Type	Null	Default	Description
id *(Primary)*	bigint(20)	No		คีย์หลัก
name	varchar(255)	No		ชื่อ
display_name	varchar(255)	Yes	*NULL*	ชื่อที่ใช้แสดง
description	varchar(255)	Yes	*NULL*	รายละเอียด
created_at	timestamp	Yes	*NULL*	วันที่สร้าง
updated_at	timestamp	Yes	*NULL*	วันที่แก้ไข

ตารางที่ 7-19 ข้อมูลของตาราง role_user

Column	Type	Null	Default	Description
id *(Primary)*	bigint(20)	No		คีย์หลัก
role_id	bigint(20)	No		คีย์หลัก Roles
user_id	bigint(20)	No		คีย์หลักผู้ใช้งาน
user_type	varchar(255)	No		ประเภทผู้ใช้งาน

ตารางที่ 7-20 ข้อมูลของตาราง permissions

Column	Type	Null	Default	Description
id *(Primary)*	bigint(20)	No		คีย์หลัก
module	varchar(255)	No		โมดูล
name	varchar(255)	No		ชื่อ
display_name	varchar(255)	Yes	*NULL*	ชื่อที่แสดง
description	varchar(255)	Yes	*NULL*	รายละเอียด
created_at	timestamp	Yes	*NULL*	วันที่สร้าง
updated_at	timestamp	Yes	*NULL*	วันที่แก้ไข

ตารางที่ 7-21 ข้อมูลของตาราง permissions_role

Column	Type	Null	Default	Description
permission_id *(Primary)*	bigint(20)	No		คีย์หลัก permission
role_id *(Primary)*	bigint(20)	No		คีย์หลัก role

ตารางที่ 7-22 ข้อมูลของตาราง permission_user

Column	Type	Null	Default	Description
id *(Primary)*	bigint(20)	No		คีย์หลัก
permission_id	bigint(20)	No		คีย์หลัก permission
user_id	bigint(20)	No		คีย์หลัก ผู้ใช้งานน
user_type	varchar(255)	No		ประเภทผู้ใช้งาน

7.5 LINE Official Account “ฉลาดโอน.com”

เพื่ออำนวยความสะดวกให้กับประชาชนในการใช้บริการฉลาดโอน ทางคณะผู้วิจัยจึงได้เปิด LINE Official Account ขึ้นเพื่อให้ความช่วยเหลือกับประชาชนที่ต้องการใช้บริการผ่านฉลาดโอน รวมถึงการให้ความช่วยเหลือในกรณีที่ผู้ใช้งานติดปัญหาหรือมีข้อซักถาม โดยการใช้บริการฉลาดโอนผ่านช่องทาง LINE Official Account “ฉลาดโอน.com”นี้ ผู้ใช้บริการจำเป็นต้องลงทะเบียนด้วยบัญชีไลน์ของตนเองก่อนเพื่อรับบริการจากฉลาดโอน ทั้งนี้ การลงทะเบียนด้วยบัญชีไลน์ ถือว่าเป็นการลงทะเบียนด้วยเลขหมายโทรศัพท์ที่ใช้ยืนยันตัวตนกับไลน์, ชื่อ , รูปภาพ และLINE ID โดยรูปแบบการให้บริการ แบ่งออกเป็น 6 รูปแบบ

1. เช็กหลักฐาน
2. เช็กตัวตนผู้ขาย
3. ประเมินบัญชีโซเชียล
4. ช่วยรวมหลักฐาน
5. แจ้งคนโกง
6. เช็กคนโกง

เช็กคนโกง

การบริการเช็กคนโกง คือบริการที่เจ้าหน้าที่แอดมินอำนวยความสะดวกให้กับประชาชนในการตรวจสอบข้อมูลผู้กระทำความผิด ว่าข้อมูลของผู้ขายหรือผู้รับโอนนั้นมีประวัติการกระทำความผิดจากหน่วยงานใดหรือไม่

เช็กหลักฐาน

การเช็กหลักฐาน คือบริการตรวจสอบข้อมูลเพิ่มเติมของผู้ขาย ผ่านไอพีแอดเดรสในกรณีที่ต้องการทราบว่าผู้ขายรายนั้นอาศัยอยู่ในประเทศไทยหรือไม่

เช็กตัวตนผู้ขาย

การเช็กตัวตนผู้ขาย คือบริการตรวจสอบข้อมูลว่าผู้ขายรายนั้นยืนยันตัวตน หรือเลขที่บัญชีธนาคารนั้นได้มีการลงทะเบียนไว้ในระบบต้นแบบฯหรือไม่ เพื่อเป็นข้อมูลสำหรับผู้ใช้บริการประกอบการตัดสินใจในการทำธุรกรรมออนไลน์

ประเมินบัญชีโซเชียล

การประเมินบัญชีโซเชียล คือบริการที่เจ้าหน้าที่แอดมินจะตรวจสอบข้อมูลบัญชีโซเชียลมีเดียนั้น ๆ ว่าพบประวัติเรื่องร้องเรียนหรือการกระทำความผิดจากหน่วยงานใดหรือไม่

ช่วยรวมหลักฐาน

บริการช่วยรวมหลักฐาน คือบริการที่เจ้าหน้าที่จะอำนวยความสะดวกในกรณีที่ผู้เสียหายต้องการให้ช่วยเตรียมเอกสารเพื่อใช้ประกอบการแจ้งความดำเนินคดีในคดีฉ้อโกงออนไลน์ โดยการลำดับเหตุการณ์ สรุปพฤติการณ์ และสร้างไฟล์เอกสารประกอบการแจ้งความในรูปแบบ Portable Document Format (PDF) เพื่อให้ผู้เสียหายนำไปแจ้งความดำเนินคดี และสะดวกต่อเจ้าหน้าที่ตำรวจในการรวบรวมข้อมูลเพื่อทำสำนวนคดี หรือพิจารณารับแจ้งความดำเนินคดี

แจ้งคนโกง

บริการแจ้งคนโกง เป็นบริการให้ข้อมูลผู้กระทำผิด เพื่อป้องกันไม่ให้ผู้อื่นตกเป็นเหยื่อของมิจฉาชีพออนไลน์ต่อไป โดยการบันทึกข้อมูลลงฐานข้อมูลผู้กระทำความผิดในระบบต้นแบบฯ

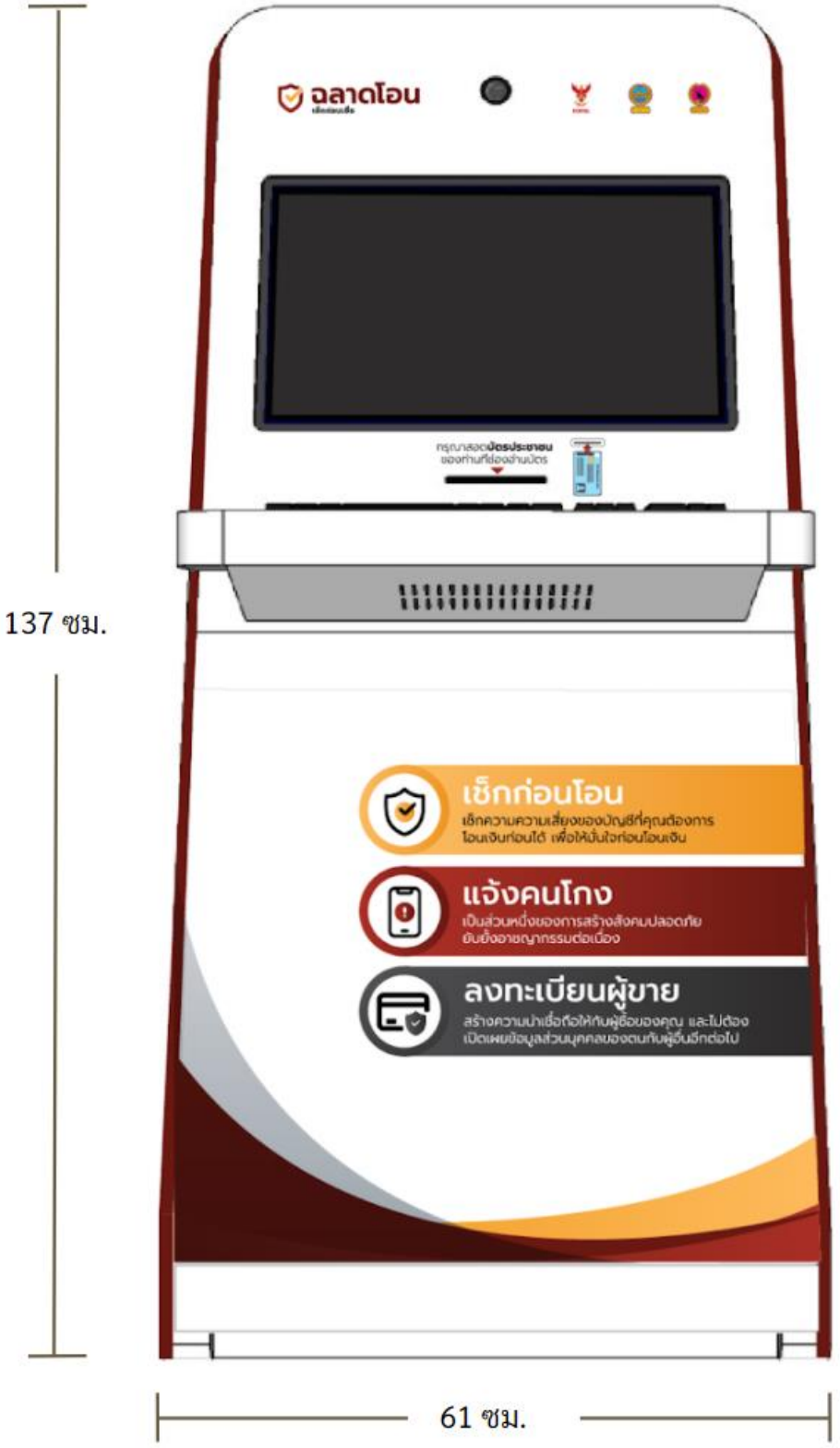
7.6 การพัฒนาระบบที่เกี่ยวข้องผ่านตู้คีออส

การออกแบบและพัฒนาตู้คีออส ถูกออกแบบให้มีความสอดคล้องและรองรับการทำงานของฟังก์ชันต่างๆ ตามความต้องการของผู้ใช้งาน อันประกอบไปด้วยระบบค้นหาข้อมูลผู้กระทำความผิดในส่วนของการสืบค้นข้อมูลผู้กระทำความผิด , ระบบแจ้งความดำเนินคดีมิจฉาชีพออนไลน์ที่ไม่สามารถระบุตัวตนได้ ในส่วนของการให้ข้อมูลผู้กระทำความผิด และการลงทะเบียนยืนยันตัวตนสำหรับผู้ขายที่ต้องการยืนยันตัวตน โดยที่การออกแบบและพัฒนาในส่วนนี้ จะถูกออกแบบให้ดำเนินการตามกระบวนการงานที่ตู้คีออสในส่วนหนึ่ง และสามารถไปดำเนินการต่อจนเสร็จสิ้นได้ผ่านทางเว็บไซต์ฉลาดโอนดอทคอม

7.6.1 การออกแบบตู้คีออส

จากการสัมภาษณ์ และสอบถามความต้องการของผู้ใช้งาน ทั้งผู้ซื้อและผู้ขายสินค้าออนไลน์พบว่าในปัจจุบัน การใช้งานโทรศัพท์เคลื่อนที่ มีการใช้งานอย่างแพร่หลาย คณะผู้วิจัยจึงเล็งเห็นและได้ออกแบบตู้คีออสให้มีความสอดคล้องและรองรับการทำงานของฟังก์ชันต่างๆ โดยให้ผู้ใช้งานสามารถตรวจสอบชื่อบัญชีธนาคารหรือเลขที่บัญชีธนาคารของผู้กระทำความผิด แจ้งเรื่องคนโกง (ผู้กระทำความผิด) และลงทะเบียนยืนยันตัวตนกับทางโครงการ ซึ่งการร้องเรียนผู้กระทำความผิดและการลงทะเบียนยืนยันตัวตนนั้น ผู้ใช้งานจำเป็นต้องลงทะเบียนและยืนยันตัวตนด้วยบัตรประชาชน อัตลักษณ์บุคคล และเลขหมายโทรศัพท์เพื่อรับรหัส OTP โดยจะได้รับคิวอาร์โค้ดเพื่อไปดำเนินการต่อบนเว็บไซต์ฉลาดโอนดอทคอม นอกจากนี้ตู้คีออสยังสามารถใช้ในการประชาสัมพันธ์โครงการ และขยายผลต่อไปในพื้นที่อื่นๆ ได้อีกด้วย

ด้วยฟังก์ชันของตู้คีออสที่ถูกออกแบบให้สามารถลงทะเบียนยืนยันตัวตนได้เป็นระบบหลักนั้น ตู้คีออสจึงมีคุณลักษณะของการรับข้อมูลผ่านทางการสัมผัสหน้าจอ (Touch Screen) เพื่ออำนวยความสะดวกในการโต้ตอบกับคอมพิวเตอร์โดยการสัมผัสบริเวณต่างๆบนหน้าจอ และมีช่องสำหรับสอดบัตรประชาชน รวมถึงกล้องสำหรับถ่ายภาพใบหน้า เพื่อตรวจสอบการยืนยันตัวอันเป็นฟังก์ชันหลักของตู้คีออส โดยแสดงตัวอย่างตู้คีออสได้ดังรูปที่ 7-53 และรูปที่ 7-54



รูปที่ 7-53 ภาพตัวอย่างตู้คีออส (ด้านหน้า)

รูปที่ 7-54 ภาพการออกแบบตู้คีออส (ด้านข้าง)

รายละเอียดคุณลักษณะเฉพาะของตู้คีออส แสดงดังตารางที่ 7-23

ตารางที่ 7-23 แสดงคุณลักษณะเฉพาะของตู้คีออส

คุณลักษณะเฉพาะของหน้าจอแสดงภาพ	
ขนาด	ขนาด 21.5 นิ้ว
ความละเอียดหน้าจอ	1920 x 1080 พิกเซล
อุปกรณ์ระบบสัมผัส	แบบ Multi-Finger Touch Sampling Rate 60Hz
คุณลักษณะเฉพาะด้านอื่น ๆ ของอุปกรณ์	
หน่วยประมวลผลกลาง (CPU)	Intel Core i3-10110U
หน่วยความจำหลัก (RAM)	ขนาดความจุ 8 GB DDR4
หน่วยจัดเก็บข้อมูล (Hard Disk)	ขนาดความจุ 256 GB ประเภท SSD
กล้องดิจิทัล	กล้องดิจิทัลแบบเว็บแคม ยี่ห้อ Logitech รุ่น Web Cam C615
เครื่องอ่านบัตรประชาชน	ชุดเครื่องอ่านและกรอกข้อมูลบัตรประชาชนอัตโนมัติแบบวางนอน รุ่น TFK2700R

7.6.2 กระบวนการทำงานของตู้คีออส

กระบวนการทำงานของตู้คีออส จะแบ่งออกเป็น 3 ส่วน ดังนี้

1) เช็กก่อนโอน

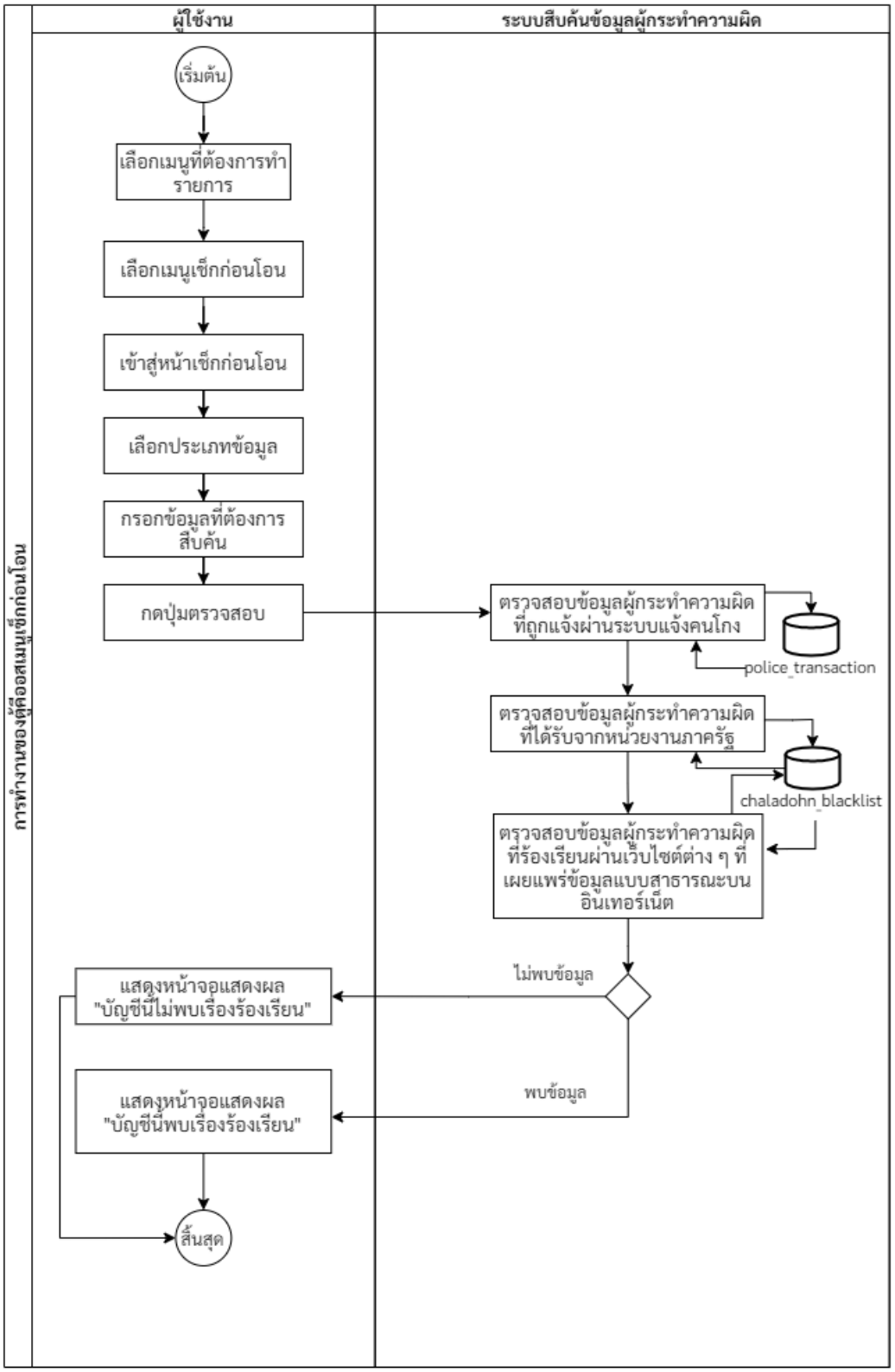
เมนูสำหรับ ตรวจสอบความน่าเชื่อถือของผู้ขายที่เราต้องการทำธุรกรรมด้วย ว่าเคยถูกผู้ซื้อรายใด ร้องเรียนเข้ามาหรือไม่ เพื่อให้ผู้ตรวจสอบมีความเชื่อมั่นในการทำธุรกรรมกับผู้ขายรายนั้น ๆ แสดงขั้นตอนการทำงาน ดังรูป 7-3

2) แจ้งคนโกง

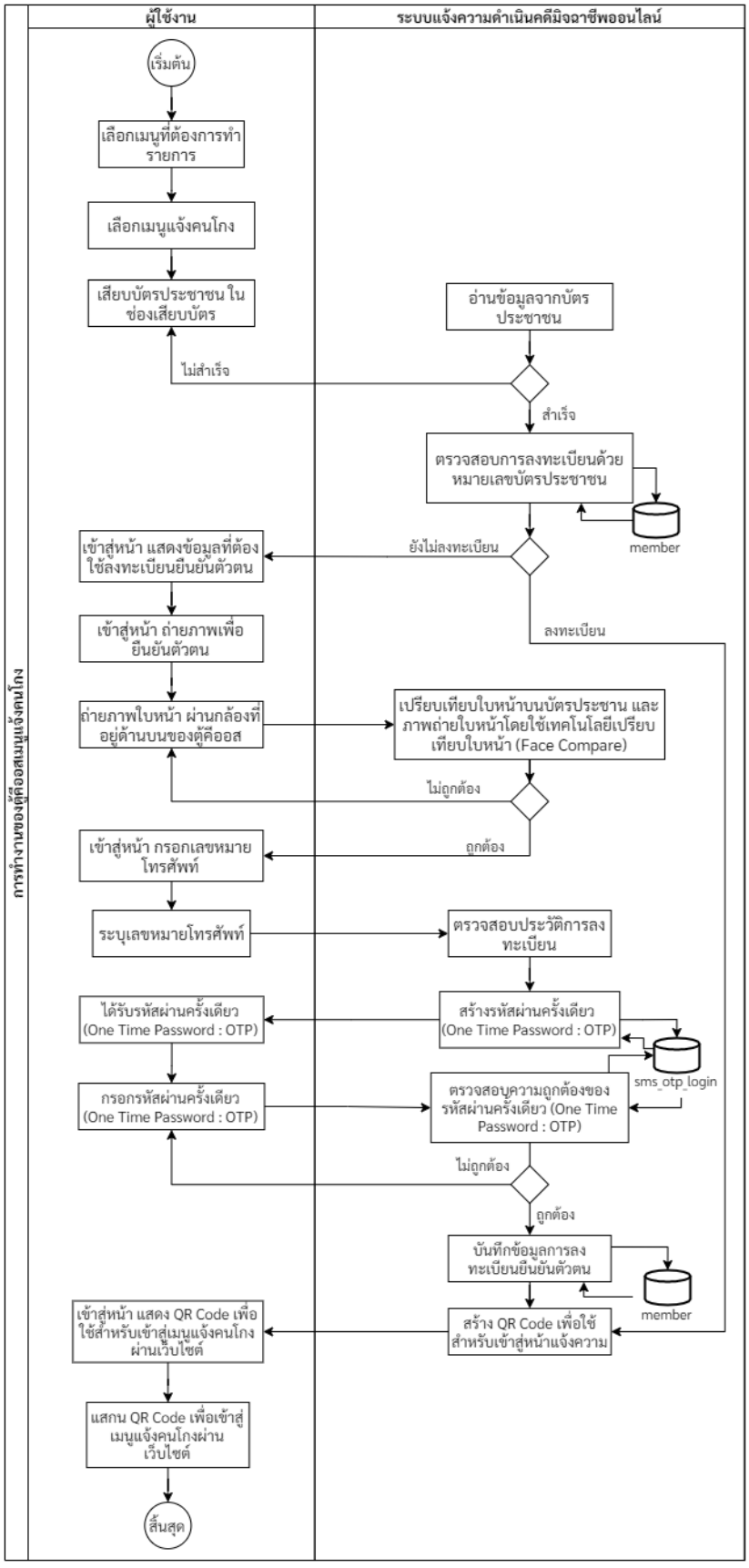
ส่วนของการแจ้งคนโกง จะมีไว้สำหรับผู้เสียหายที่ต้องการแจ้งเรื่องร้องเรียน เพื่อแจ้งเตือนประชาชนคนอื่น ๆ หรือแจ้งเพื่อดำเนินคดีกับผู้ถูกกล่าวหาต่อไป แสดงขั้นตอนการทำงาน ดังรูป 7-4

3) ลงทะเบียนผู้ขาย

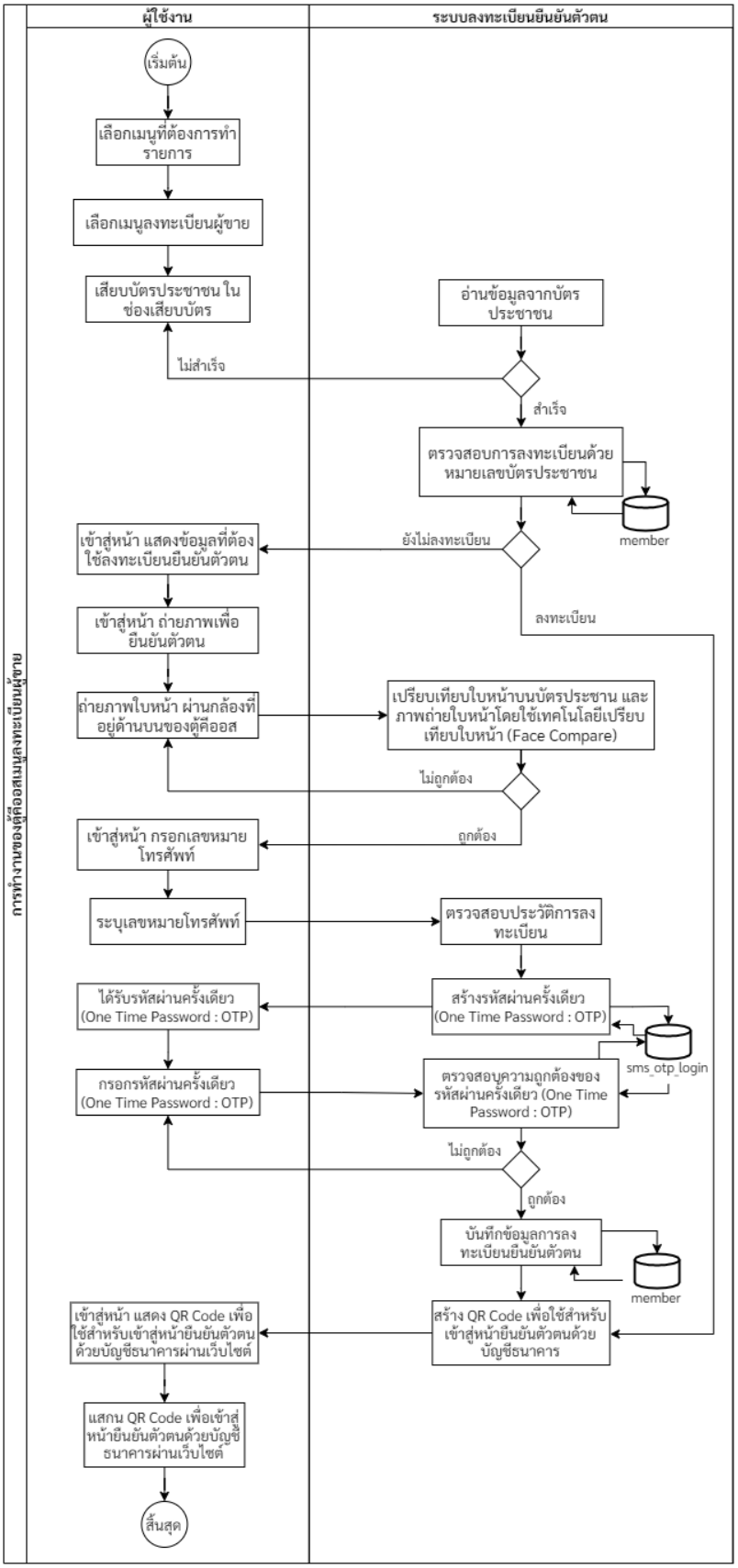
เมนูการลงทะเบียนผู้ขาย มีไว้สำหรับลงทะเบียนเพื่อยืนยันตัวตนของผู้ใช้งาน เพื่อเพิ่มความน่าเชื่อถือในการทำธุรกรรมระหว่างผู้ซื้อและผู้ขาย แสดงขั้นตอนการทำงาน ดังรูป 7-55



รูปที่ 7-55 ภาพรวมการทำงานของตู้คีออสเมนูเช็กก่อนโอน



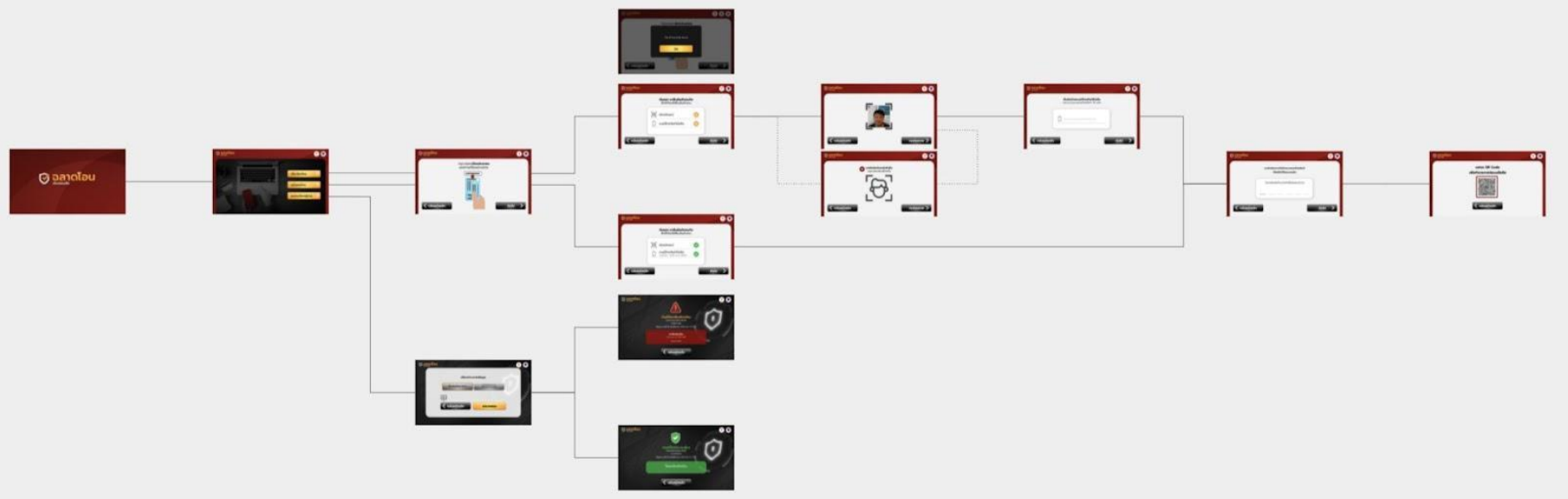
รูปที่ 7-56 ภาพรวมการทำงานของตู้คีออสเมนูแจ้งคนโกง



รูปที่ 7-57 ภาพรวมการทำงานของตู้คีออสเมนูลงทะเบียนผู้ขาย

7.6.3 หน้าจอแสดงผลและรายละเอียดการทำงาน

หน้าจอแสดงผลทั้งหมดของตู้คีออส แสดงภาพรวมได้ดังรูปที่ 7-58



รูปที่ 7-58 หน้าจอทั้งหมดบนตู้คีออส

รูปที่ 7-59 หน้าแรกของตู้คีออส

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1		Yes		แสดงโลโก้ของระบบแบบอัตโนมัติ

รูปที่ 7-60 หน้าจอแสดงเมนูของตู้คีออส

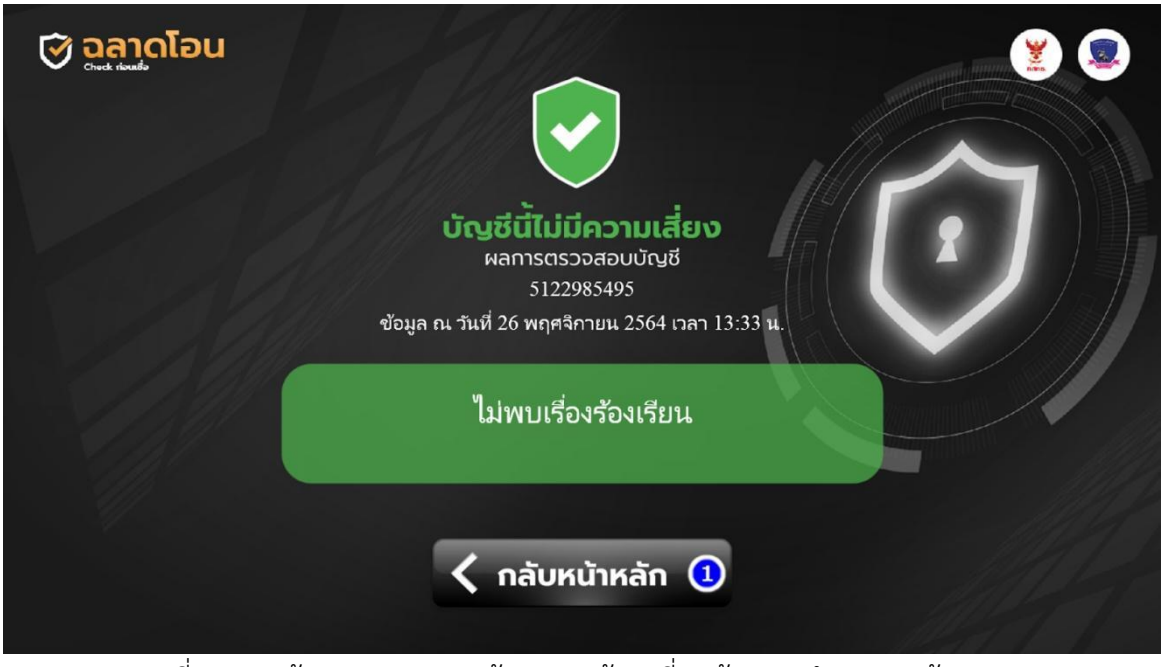
ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	ปุ่มเช็กก่อนโอน	Yes		เข้าสู่หน้าจอสำหรับตรวจสอบชื่อบัญชี หรือเลขที่บัญชีของผู้ขาย ที่เราต้องการทำธุรกรรมด้วย
2	ปุ่มแจ้งคนโกง	Yes		เข้าสู่หน้าจอการยืนยันตัวตนด้วยอัตลักษณ์และเบอร์โทรศัพท์มือถือ
3	ปุ่มลงทะเบียนผู้ขาย	Yes		เข้าสู่หน้าจอการยืนยันตัวตนด้วยอัตลักษณ์

- เช็กก่อนโอน

เมื่อเข้ามาจะพบหน้าจอสำหรับเลือกประเภทข้อมูลที่ต้องการตรวจสอบ แบ่งเป็น ชื่อบัญชีธนาคาร และเลขที่บัญชีธนาคาร/พร้อมเพย์/ทรูวอลเล็ต แสดงดังรูปที่ 7-61

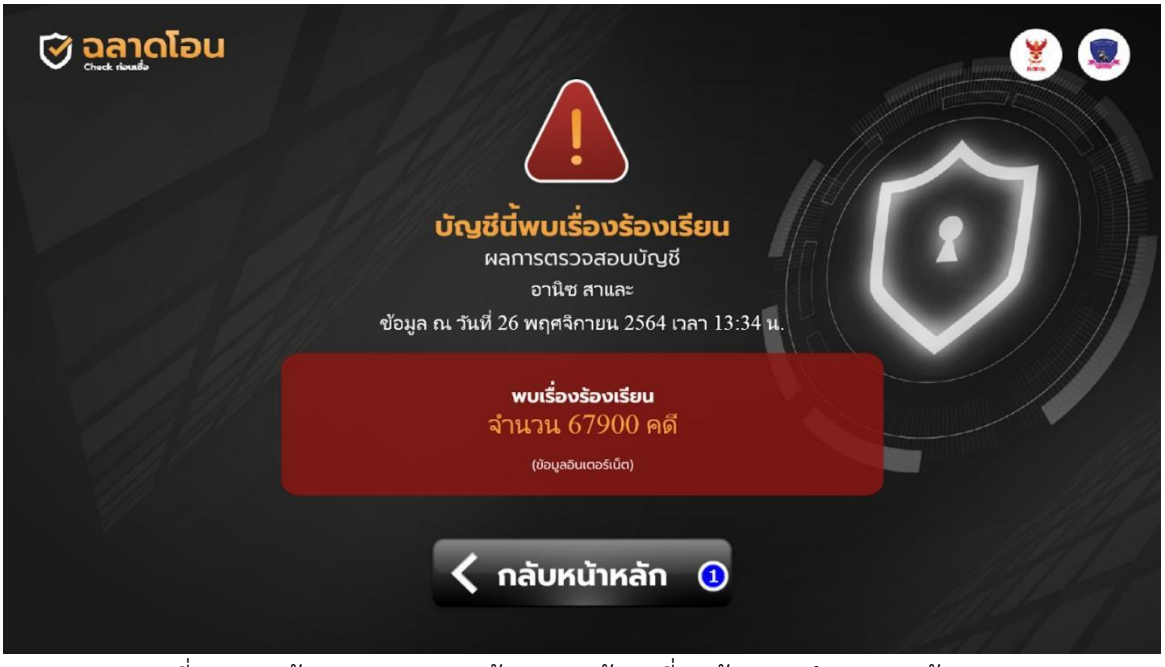
รูปที่ 7-61 หน้าจอสำหรับตรวจสอบชื่อบัญชี หรือเลขที่บัญชีของผู้ขาย ที่เราต้องการทำธุรกรรมด้วย

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	ปุ่มชื่อบัญชีธนาคาร	Yes		เลือกในกรณีที่ต้องการตรวจสอบข้อมูลที่เป็นชื่อบัญชีธนาคาร
2	ปุ่มเลขที่บัญชีธนาคาร/ พร้อมเพย์/ทรูวอลเล็ต	Yes		เลือกในกรณีที่ต้องการตรวจสอบข้อมูลเลขที่บัญชีธนาคาร พร้อมเพย์ ทรูวอลเล็ต
3	ปุ่มกรอกชื่อบัญชีธนาคาร	Yes		กรอกข้อมูลตามประเภทของข้อมูลที่เลือกไว้ให้ถูกต้อง
4	ปุ่มกลับหน้าหลัก	Yes		กลับสู่หน้าจอเมนูของตู้คีออส
5	ปุ่มตรวจสอบ			เข้าสู่การตรวจสอบข้อมูลและแสดงผลการค้นหาของผู้ขายที่เราต้องการทำธุรกรรมด้วย



รูปที่ 7-62 หน้าจอแสดงผลการค้นหาของผู้ขายที่เราต้องการทำธุรกรรมด้วยแบบ “ไม่พบเรื่องร้องเรียน”

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	ปุ่มกลับสู่หน้าแรก	Yes		กลับสู่หน้าจอเมนูของตู้คีออส

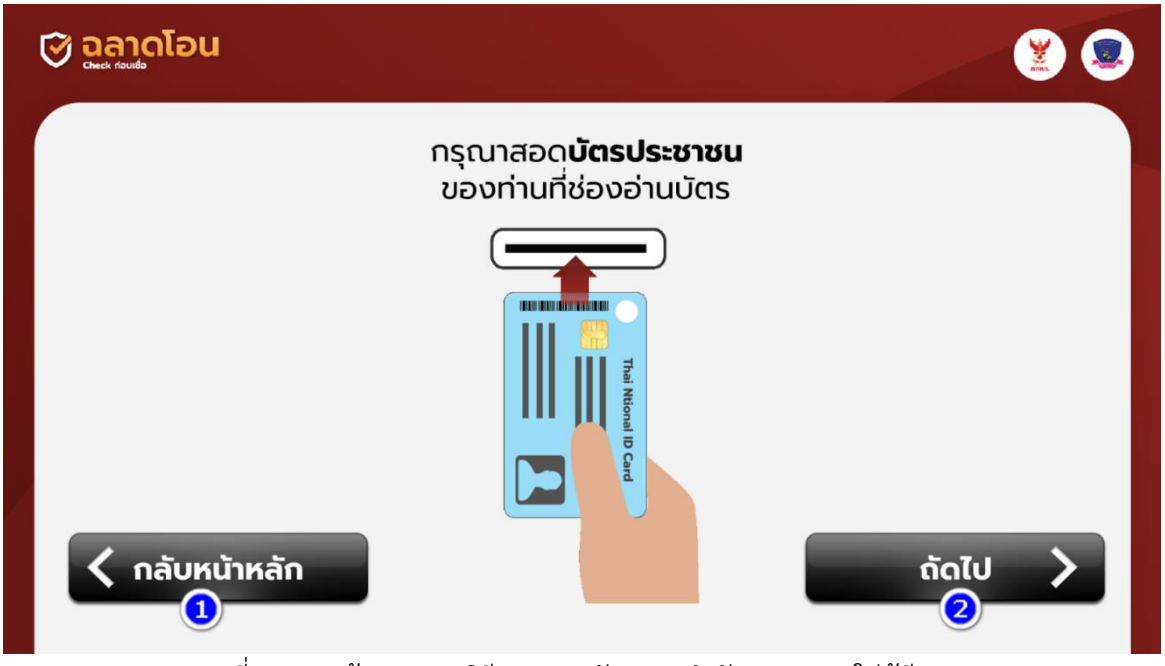


รูปที่ 7-63 หน้าจอแสดงผลการค้นหาของผู้ขายที่เราต้องการทำธุรกรรมด้วยแบบ “พบเรื่องร้องเรียน”

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	ปุ่มกลับสู่หน้าแรก	Yes		กลับสู่หน้าจอเมนูของตู้คีออส

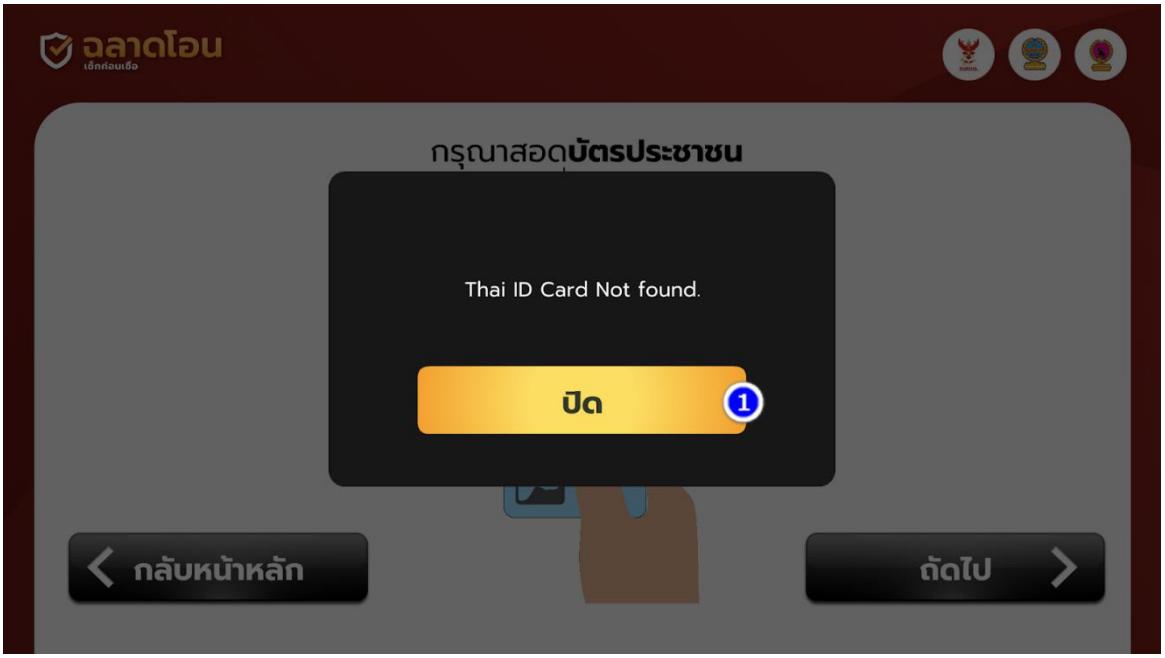
- แจ้งคนโกง

เมื่อเข้าใช้งานในเมนูนี้ ระบบจะแสดงหน้าจอให้สอดบัตรประจำตัวประชาชนใส่ตู้คีออส แสดงดังรูปที่ 7-64 จากนั้นระบบจะอ่านข้อมูลจากบัตรประจำตัวประชาชน ในกรณีระบบไม่สามารถอ่านบัตรประจำตัวประชาชนได้ จะแสดงหน้าจอดังรูปที่ 7-65 ให้ผู้ใช้งานดำเนินการดึงบัตรประจำตัวประชาชนออกแล้วสอดบัตรเข้าไปอีกครั้ง



รูปที่ 7-64 หน้าจอแสดงวิธีการสอดบัตรประจำตัวประชาชนใส่ตู้คีออส

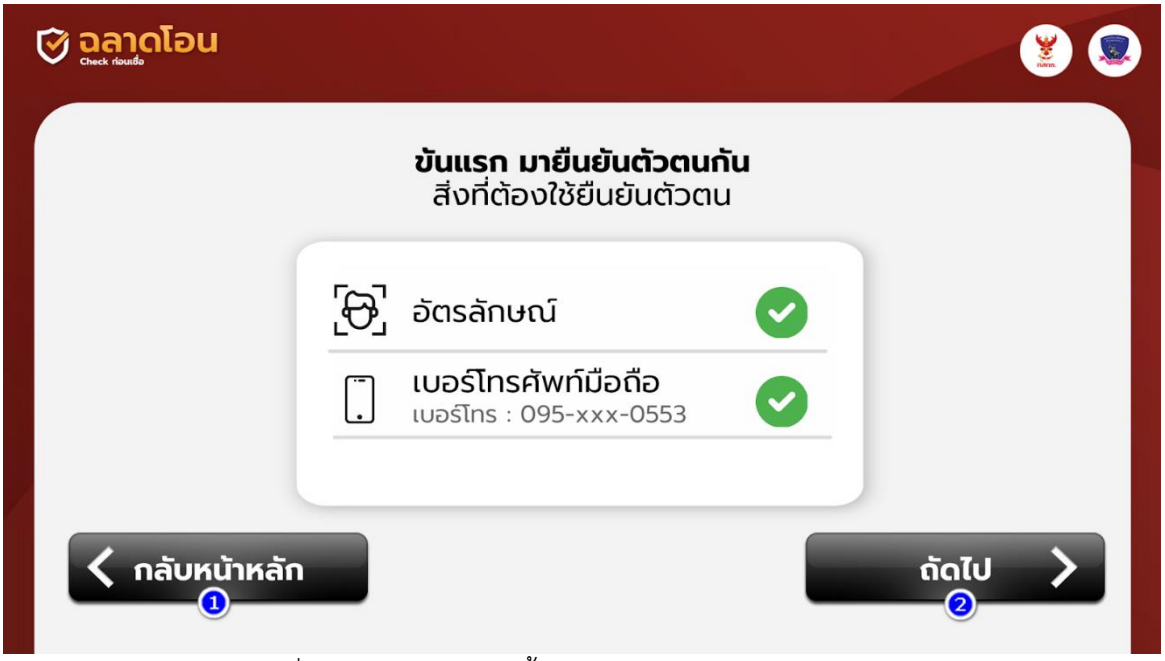
ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	ปุ่มกลับสู่หน้าหลัก	Yes		กลับสู่หน้าจอเมนูของตู้คีออส
2	ปุ่มถัดไป	Yes		เข้าสู่หน้าจอการยืนยันตัวตนด้วยอัตลักษณ์



รูปที่ 7-65 หน้าจอแสดงผลการอ่านบัตรประจำตัวประชาชน

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	ปุ่มปิดเพื่อทำรายการอีกครั้ง	Yes		กดเพื่อทำการสอดบัตรประจำตัวประชาชนอีกครั้ง

เมื่อระบบสามารถอ่านข้อมูลจากบัตรประจำตัวประชาชนได้สำเร็จ จะพบหน้าจอแสดงผลการยืนยันตัวตนของผู้ใช้งาน แสดงดังรูปที่ 7-66 (ในกรณีที่ยังไม่เคยลงทะเบียนมาก่อน ให้ทำการลงทะเบียนสมัครผ่านหน้าเว็บมาก่อน โดยจะอธิบายในหัวข้อถัดไป) โดยขั้นแรกจะเป็นยืนยันตัวผ่านอัตลักษณ์



รูปที่ 7-66 หน้าจอแสดงขั้นตอนการยืนยันตัวตนผ่านตู้คีออส

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	ปุ่มย้อนกลับ	Yes		ย้อนกลับสู่หน้าจอเมนูของตู้คีออส
2	ปุ่มถัดไป	Yes		ระบบจะส่ง OTP ให้ผู้ใช้งาน เพื่อเข้าสู่ขั้นตอนแจ้งคนโกง

จากนั้นให้ผู้ใช้งานกรอกรหัส OTP ที่ได้รับเพื่อยืนยันตัวตนกับระบบฉลาดโอน แสดงดังรูปที่ 7-67 เมื่อกรอกแล้วระบบจะแสดง QR Code เพื่อทำรายการต่อบนโทรศัพท์ แสดงได้ดังรูป 7-68

รูปที่ 7-67 หน้าจอแสดงผล สำหรับกรอกรหัส OTP ตามที่ได้แจ้งเลขหมายโทรศัพท์ไว้

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	ปุ่มย้อนกลับ	Yes		ย้อนกลับสู่หน้าจอเมนูของตู้คีออส
2	ปุ่มถัดไป	Yes		ระบบจะส่ง OTP ให้ผู้ใช้งาน เพื่อเข้าสู่ขั้นตอนแจ้งคนโกง

รูปที่ 7-68 หน้าจอแสดง QR Code เพื่อให้ผู้แจ้งเรื่อง เข้าไปกรอกข้อมูลเรื่องร้องเรียน และอัปโหลดหลักฐานผ่านมือถือ

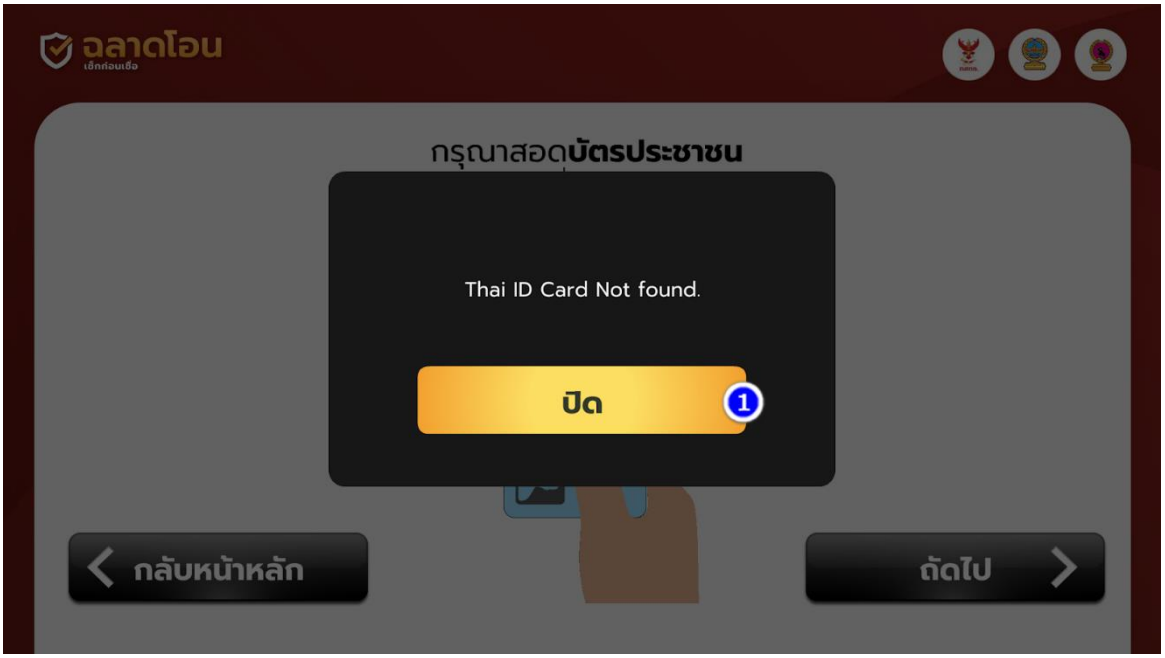
ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	ปุ่มย้อนกลับ	Yes		ย้อนกลับสู่หน้าจอเมนูของตู้คีออส
2	ปุ่มถัดไป	Yes		ระบบจะส่ง OTP ให้ผู้ใช้งาน เพื่อเข้าสู่ขั้นตอนแจ้งคนโกง

- ลงทะเบียนผู้ขาย

เมนูนี้ สำหรับผู้ใช้งานที่ต้องการลงทะเบียนผู้ขาย ระบบจะเริ่มต้นด้วยการให้ผู้ใช้งานสอดบัตรประจำตัวประชาชนที่ช่องอ่านบัตร แสดงดังรูปที่ 7-69 กรณีที่ตู้คีออส ไม่สามารถอ่านบัตรประจำตัวประชาชนได้ จะข้อความบนหน้าจอ แสดงดังรูปที่ 7-70

รูปที่ 7-69 หน้าจอแสดงวิธีการสอดบัตรประจำตัวประชาชนใส่ตู้คีออส

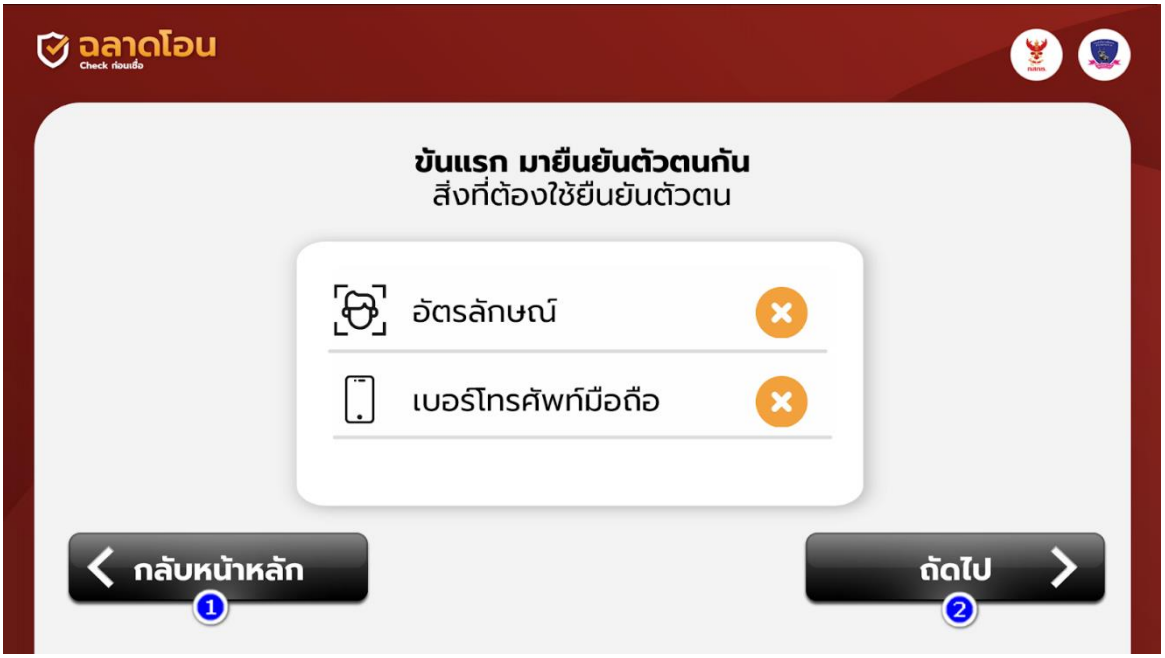
ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	ปุ่มกลับสู่หน้าหลัก	Yes		กลับสู่หน้าจอเมนูของตู้คีออส
2	ปุ่มถัดไป	Yes		เข้าสู่หน้าจอการยืนยันตัวตนด้วยอัตลักษณ์



รูปที่ 7-70 หน้าจอแสดงผลการอ่านบัตรประจำตัวประชาชน

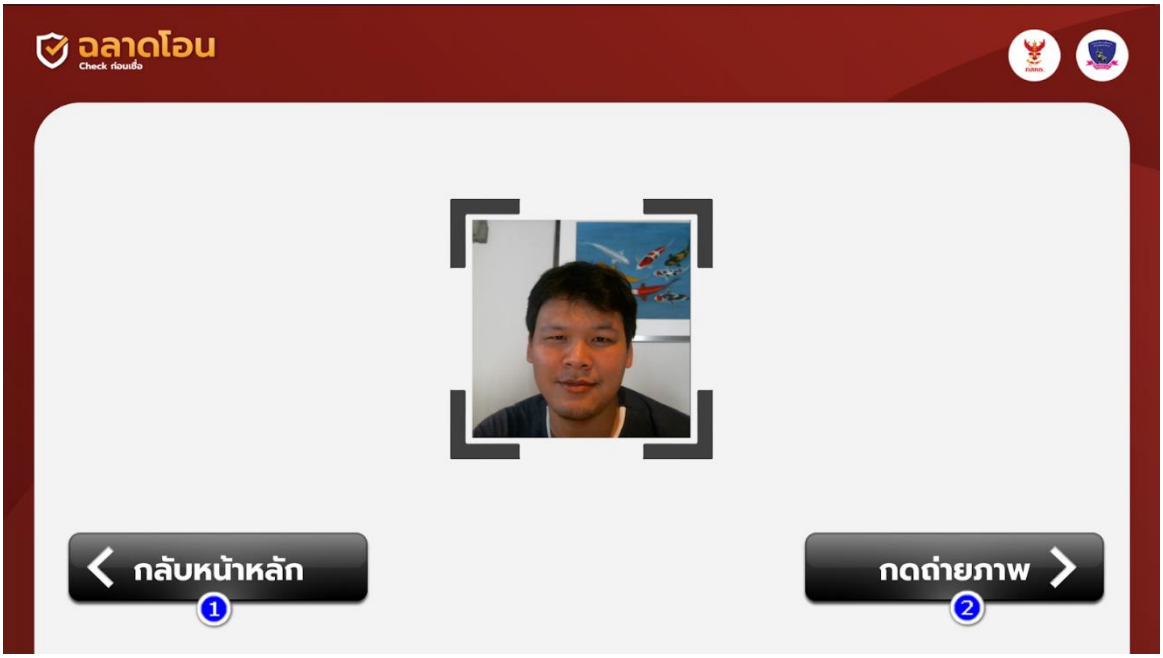
ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	ปุ่มปิดเพื่อทำรายการอีกครั้ง	Yes		กดเพื่อทำการสอดบัตรประจำตัวประชาชนอีกครั้ง

เมื่อระบบตรวจสอบบัตรประจำตัวประชาชนเป็นที่เรียบร้อย ระบบจะแสดงสถานะการยืนยันตัวตนของผู้ใช้งาน แสดงดังรูปที่ 7-71 จากนั้น ให้ผู้ใช้งานทำการยืนยันตัวตนด้วยการพิสูจน์อัตลักษณ์โดยกดถ่ายรูปใบหน้าจากหน้าตู้คีออส แสดงดังรูปที่ 7-72



รูปที่ 7-71 หน้าจอแสดงหลักฐานที่ต้องใช้เพื่อยืนยันตัวตน

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	ปุ่มย้อนกลับ	Yes		ย้อนกลับสู่หน้าจอเมนูของตู้คีออส
2	ปุ่มถัดไป	Yes		ระบบจะเข้าสู่ขั้นตอนการยืนยันตัวตนด้วยอัตลักษณ์



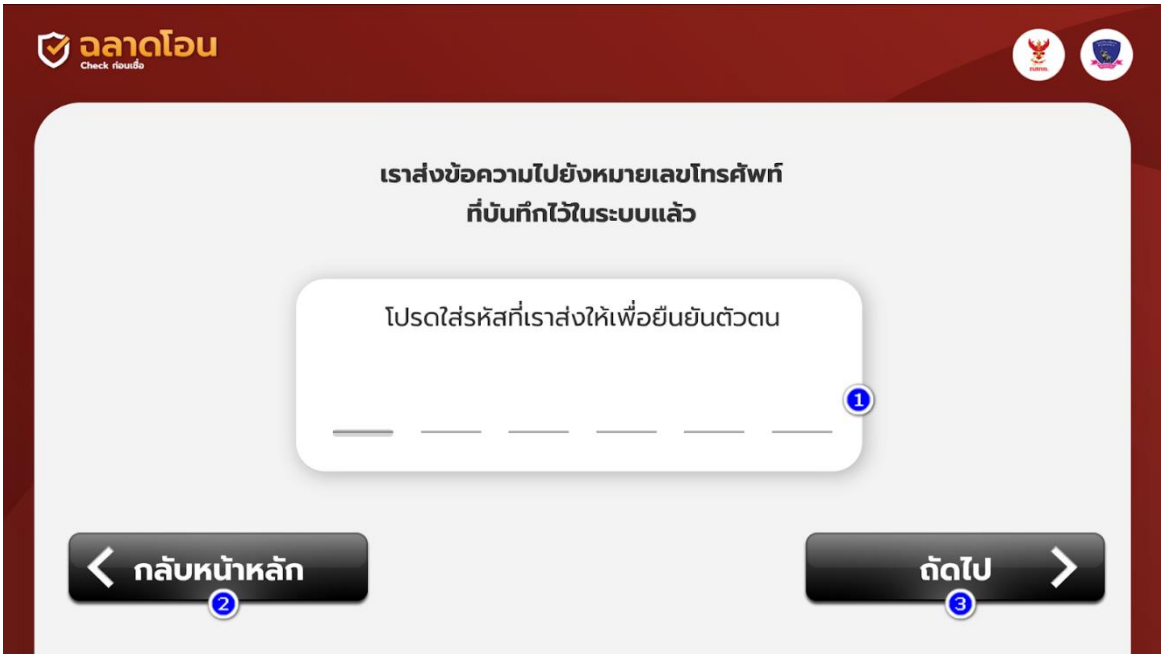
รูปที่ 7-72 หน้าจอการถ่ายภาพเพื่อยืนยันตัวตน

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	ปุ่มย้อนกลับ	Yes		ย้อนกลับสู่หน้าจอเมนูของตู้คีออส
2	ปุ่มกดถ่ายภาพ	Yes		กดถ่ายภาพเพื่อยืนยันตัวตนและเข้าสู่หน้าจอยืนยันตัวตนด้วยเลขหมายโทรศัพท์

เมื่อตรวจสอบยืนยันตัวตนด้วยอัตลักษณ์ผ่านเรียบร้อยแล้ว ขั้นต่อมาให้ผู้ใช้งานกรอกเลขหมายโทรศัพท์สำหรับการลงทะเบียนยืนยันตัวตน แสดงดังรูปที่ 7-73 และกรอกหมายเลข OTP ที่ได้รับสู่ระบบ แสดงดังรูปที่ 7-74 จากนั้นจะได้รับ QR Code เพื่อทำรายการต่อบนโทรศัพท์มือถือ แสดงดังรูปที่ 7-75

รูปที่ 7-73 หน้าจอแสดงผล กรอกเลขหมายโทรศัพท์มือถือ

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	ช่องสำหรับกรอกเลขหมายโทรศัพท์มือถือ	Yes		กรอกเลขหมายโทรศัพท์ให้ครบ 10 หลัก
2	ปุ่มย้อนกลับ	Yes		กลับสู่หน้าจอยืนยันตัวตนด้วยเลขหมายโทรศัพท์
3	ปุ่มส่งรหัส OTP	Yes		เข้าสู่หน้าจอสำหรับกรอกรหัส OTP ตามที่ได้แจ้งเลขหมายโทรศัพท์ไว้



รูปที่ 7-74 หน้าจอแสดงผล สำหรับกรอกรหัส OTP ตามที่ได้แจ้งเลขหมายโทรศัพท์ไว้

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	ช่องสำหรับกรอกรหัส OTP	Yes		กรอกรหัส OTP ตามที่ได้แจ้งเลขหมายโทรศัพท์ให้ถูกต้อง
2	ปุ่มย้อนกลับ	Yes		กลับสู่หน้าจอกรอกเลขหมายโทรศัพท์มือถือ
3	ปุ่มยืนยัน	Yes		เข้าสู่หน้าจอแสดง QR Code

รูปที่ 7-75 หน้าจอแสดงผล QR Code เพื่อทำรายการต่อบนโทรศัพท์มือถือ

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	ปุ่มกลับหน้าหลัก	Yes		สำหรับการกลับสู่หน้าหลัก

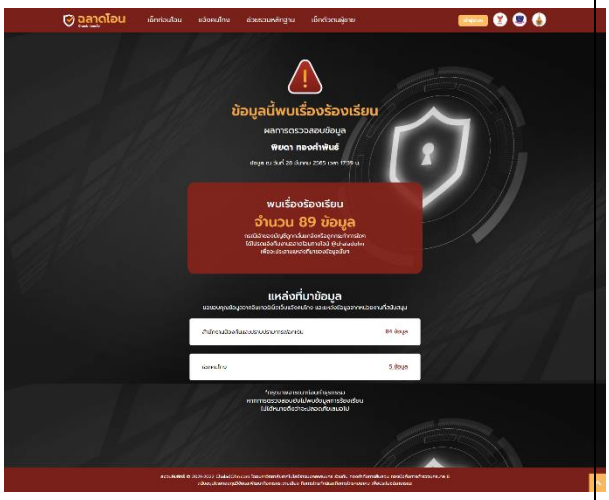
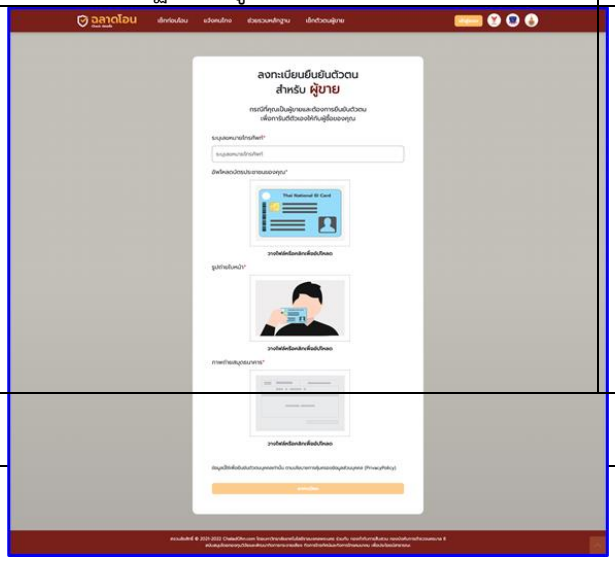
7.6.4 การส่งมอบตู้คีออสให้กับเจ้าหน้าที่ตำรวจ

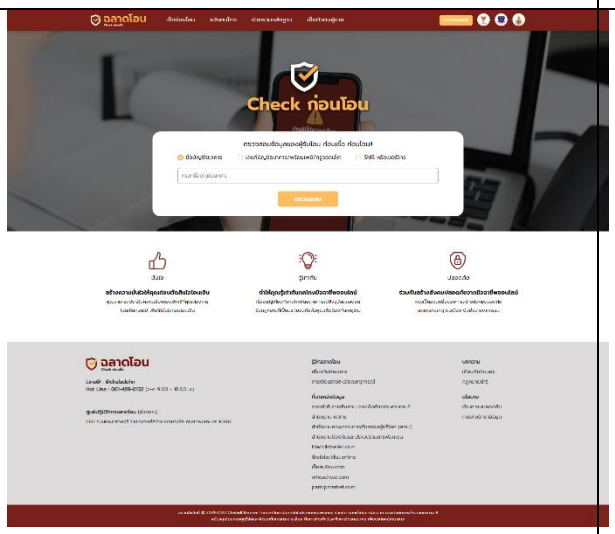
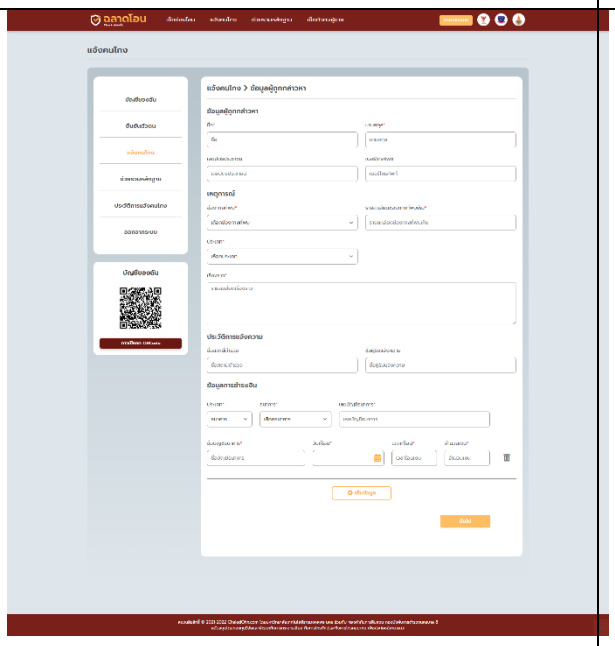
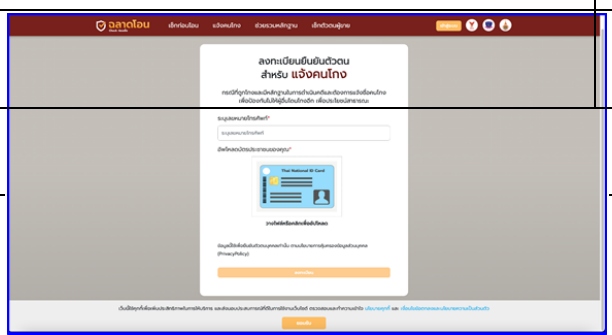
เมื่อวันพฤหัสบดีที่ 25 พฤศจิกายน 2564 ดร.เทอดพงษ์ แดงสี มหาวิทยาลัยเทคโนโลนีราชมงคลพระนคร หัวหน้าโครงการ ได้ส่งมอบตู้คีออส ในโครงการพัฒนาระบบต้นแบบเพื่อสนับสนุนงานป้องกันและปราบปรามมิจฉาชีพออนไลน์ที่ไม่ระบุตัวตนฯ เพื่อใช้สำหรับประชาสัมพันธ์โครงการ รวมถึงการลงทะเบียนและยืนยันตัวตนเบื้องต้น โดยมีเจ้าหน้าที่ตำรวจจากกองบังคับการตำรวจนครบาล 8 มารับมอบไว้เป็นที่เรียบร้อยแล้ว ณ มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร แสดงดังรูปที่ 7-76

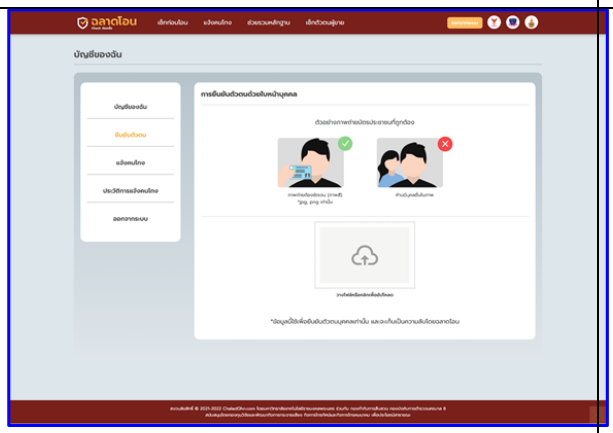
รูปที่ 7-76 รูปการส่งมอบตู้คีออส จำนวน 3 ตู้

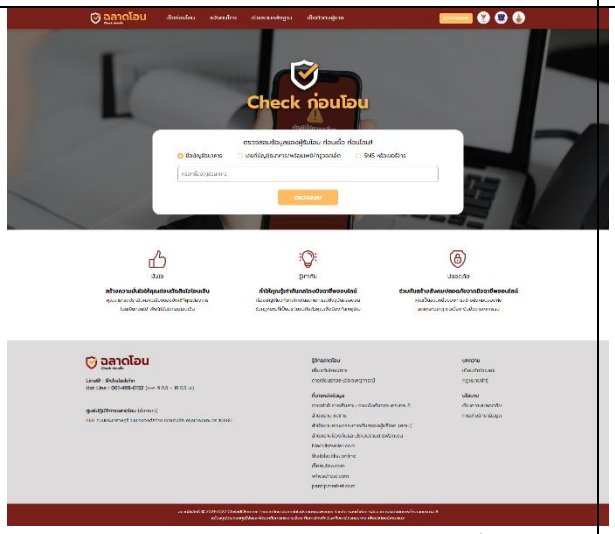
7.7 รายงานการทดสอบระบบ (User Acceptance Testing)

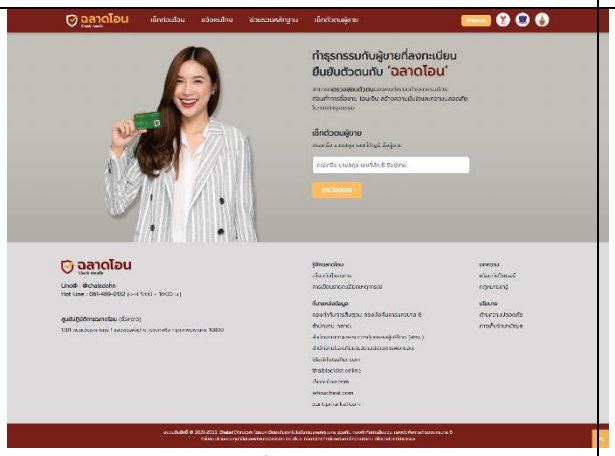
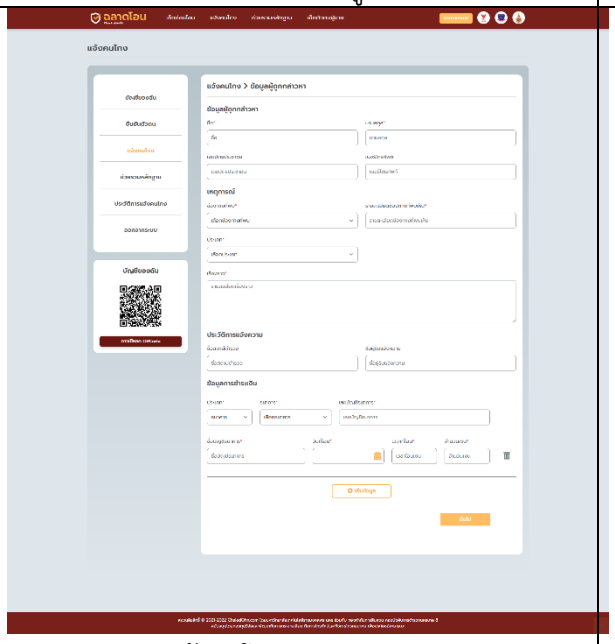
รายการทดสอบระบบต้นแบบเพื่อสนับสนุนงานป้องกันและปราบปรามมิจฉาชีพออนไลน์ที่ไม่ระบุตัวตน

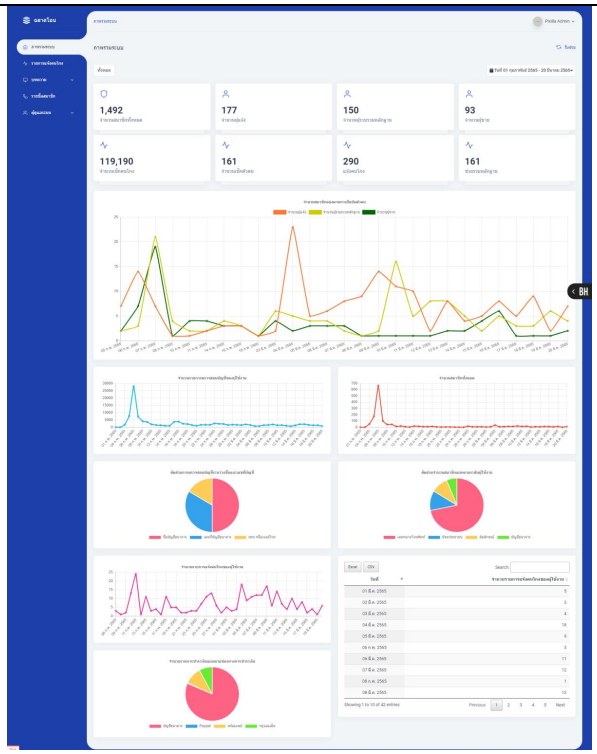
TOR ข้อที่	รายละเอียดตามขอบเขตงาน	ผลการพัฒนาระบบ	ผลการทดสอบ
4.7	งานออกแบบ และพัฒนาระบบแลกเปลี่ยนข้อมูลและระบบฐานข้อมูลมิจฉาชีพแบบออนไลน์เพื่อใช้ติดตามคดี และเป็นข้อมูลประวัติผู้กระทำความผิด ในเขตพื้นที่ศึกษา อาทิ เช่น เว็บเซอร์วิสทะเบียนราษฎร์ในการตรวจสอบชื่อที่อยู่ของผู้ถูกกล่าวหา เว็บเซอร์วิสของโอเปอร์เรเตอร์เพื่อตรวจสอบเลขหมายต่างๆ กับเลขบัตรประชาชน เป็นต้น	 ระบบแลกเปลี่ยนข้อมูล (กรมการปกครอง)  ระบบฐานข้อมูลมิจฉาชีพแบบออนไลน์	☑ ผ่าน ☐ ไม่ผ่าน
4.8	งานศึกษา วิเคราะห์และออกแบบระบบป้องกันและปราบปรามมิจฉาชีพแบบออนไลน์ เพื่อรองรับการทำงานของพนักงานสอบสวนและผู้เสียหาย โดยมี		☑ ผ่าน ☐ ไม่ผ่าน

TOR ข้อที่	รายละเอียดตามขอบเขตงาน	ผลการพัฒนาระบบ	ผลการทดสอบ
	ระบบงานหลัก ดังนี้	ระบบยืนยันตัวตนก่อนทำธุรกรรมออนไลน์	
4.8.1	ระบบยืนยันตัวตนระหว่างผู้ซื้อและผู้ขายก่อนทำธุรกรรมออนไลน์		
4.8.2	ระบบตรวจสอบและสืบค้นหลักฐานข้อมูลผู้กระทำความผิด ดำเนินคดี และผู้ถูกกล่าวหา	 ระบบตรวจสอบและสืบค้นหลักฐานข้อมูลผู้กระทำความผิด	☑ ผ่าน ☐ ไม่ผ่าน
4.8.3	ระบบแจ้งความดำเนินคดีออนไลน์ธุรกรรมออนไลน์ที่ไม่สามารถระบุตัวตนผู้ถูกกล่าวหา	 ระบบแจ้งความดำเนินคดีออนไลน์	☑ ผ่าน ☐ ไม่ผ่าน
4.9	งานพัฒนาระบบยืนยันตัวตนของผู้ขาย		☑ ผ่าน

TOR ข้อที่	รายละเอียดตามขอบเขตงาน	ผลการพัฒนาระบบ	ผลการทดสอบ
	ที่ต้องการจะรับโอนเงินก่อนส่งสินค้าหรือบริการเพื่อเป็นต้นแบบแนวทางปฏิบัติของผู้ขายที่ประกอบอาชีพสุจริต โดยต้องมีแนวทางการตรวจสอบอย่างน้อยดังนี้	การยืนยันตัวตนด้วยเลขหมายโทรศัพท์และเลขบัตรประจำตัวประชาชน	☐ ไม่ผ่าน
4.9.1	ระบบยืนยันตัวตนด้วยเลขหมายโทรศัพท์ และเลขบัตรประชาชนที่ใช้ลงทะเบียนซื้อซิมกับผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่		
4.9.2	ระบบยืนยันตัวตนด้วยการตรวจสอบอัตลักษณ์บัตรประชาชนและรูปใบหน้าอัตโนมัติ	 การยืนยันตัวตนด้วยการตรวจสอบอัตลักษณ์บัตรประชาชน	☑ ผ่าน ☐ ไม่ผ่าน

TOR ข้อที่	รายละเอียดตามขอบเขตงาน	ผลการพัฒนาระบบ	ผลการทดสอบ
4.9.3	ระบบเชื่อมโยงข้อมูลการยืนยันตัวตนกับระบบงานอื่นตามที่สำนักงาน กสทช. กำหนด	 ปัจจุบันระบบฉลาดโอนสามารถเชื่อมโยงข้อมูลการยืนยันตัวตนกับกรมการปกครอง กระทรวงมหาดไทยได้	☑ ผ่าน ☐ ไม่ผ่าน
4.10	งานพัฒนาระบบตรวจสอบ สืบค้นข้อมูลของผู้ขาย และผู้ซื้อ ผ่านเว็บไซต์ เพื่อให้ประชาชนสามารถตรวจสอบประวัติของผู้ที่จะดำเนินธุรกรรมด้วย เบื้องต้นก่อนการตัดสินใจ สำหรับประชาชนในเขตพื้นที่ศึกษา โดยจะแสดงข้อมูลเฉพาะส่วนที่สามารถเปิดเผยได้ และไม่เปิดเผยข้อมูลชื่อหรือเลขหมายโทรศัพท์ของผู้กระทำความผิดต่อสาธารณะ และต้องเป็นไปตามกฎหมายเท่านั้น	 ระบบตรวจสอบ สืบค้นข้อมูลผู้ขายผ่านเว็บไซต์	☑ ผ่าน ☐ ไม่ผ่าน

TOR ข้อที่	รายละเอียดตามขอบเขตงาน	ผลการพัฒนาระบบ	ผลการทดสอบ
		 ระบบเช็กตัวตนผู้ขาย	
4.11	งานพัฒนาระบบแจ้งความคดีธุรกรรมออนไลน์ที่ไม่สามารถระบุตัวตนผู้ถูกกล่าวหาได้ชัดเจน สำหรับประชาชนสามารถบันทึกข้อมูลหลักฐานทางอิเล็กทรอนิกส์ต่างๆ ประกอบสำนวนการดำเนินคดี เพื่อให้เจ้าหน้าที่ที่เกี่ยวข้องสามารถข้ามาตรวจสอบพยานหลักฐานของผู้แจ้งความในเบื้องต้นก่อนตัดสินใจรับแจ้งความ และสามารถตรวจสอบประวัติผู้ถูกกล่าวหาเพื่อพิจารณาแนวทางในการดำเนินคดีต่อไป	 ระบบแจ้งคนโกง / ช่วยรวมหลักฐาน	☑ ผ่าน ☐ ไม่ผ่าน

TOR ข้อที่	รายละเอียดตามขอบเขตงาน	ผลการพัฒนาระบบ	ผลการทดสอบ
4.12	งานพัฒนาระบบแสดงผลรายงานสถิติต่างๆ สำหรับผู้บริหารและพนักงานที่เกี่ยวข้องพร้อมทั้งแจ้งเตือนผลความก้าวหน้าของคดีที่ต้องการติดตามเป็นพิเศษ	 ระบบแสดงผลรายงานสถิติการลงทะเบียนและการเข้าใช้งานเว็บไซต์ฉลาดโอน	☑ ผ่าน ☐ ไม่ผ่าน

*ดำเนินการทดสอบระบบฯ โดยคณะผู้วิจัย

บทที่ 8
การดำเนินการประชาสัมพันธ์

บทที่ 8 นี้ จัดทำขึ้นเพื่อสรุปการดำเนินการประชาสัมพันธ์ของเว็บไซต์ฉลาดโอน โดยแบ่งข้อมูลออกเป็น 3 ส่วน ได้แก่ ส่วนของสื่อวิดีทัศน์ ส่วนของสื่อสิ่งพิมพ์ออนไลน์ และบทความบนเว็บไซต์ฉลาดโอน

8.1 สื่อวิดีทัศน์

คณะผู้วิจัย ได้จัดจ้างให้ทำสื่อวิดีทัศน์ เพื่อใช้สำหรับการประชาสัมพันธ์เว็บไซต์ฉลาดโอน โดยให้ Influencer กลุ่มคนที่มีอิทธิพลต่อความคิดและการตัดสินใจของกลุ่มเป้าหมาย และมีชื่อเสียงในด้านความรู้ ความเชี่ยวชาญเฉพาะด้าน และเผยแพร่เรื่องราวต่างๆบนโซเชียลมีเดีย เข้ามารีวิวเว็บไซต์ฉลาดโอนและนำเสนอแง่มุมการใช้งาน รวมถึงเผยแพร่เรื่องราวที่จะเป็นประโยชน์กับผู้ใช้งานคนอื่น ๆ โดยมีการเผยแพร่ทางช่องยูทูบ เมื่อวันที่ 15 กุมภาพันธ์ 2565 ผ่านลิงก์ (https://www.youtube.com/watch?v=cK0Q1jDr1-g) แสดงตัวอย่างดังรูปที่ 8-1

รูปที่ 8-1 สื่อวิดีทัศน์จากช่อง DOM

จากนั้น คณะผู้จัดทำได้ผลิตสื่อวิดีทัศน์อีก 1 ชิ้น เพื่อแนะนำเว็บไซต์ฉลาดโอนให้กับผู้ใช้งานทั่วไป โดยมีเนื้อหาครอบคลุมที่มาของฉลาดโอน ฟังก์ชันของระบบฉลาดโอน โดยมีการเผยแพร่ทางช่องยูทูบเมื่อวันที่ 2 มีนาคม 2565 ผ่านลิงก์ (https://www.youtube.com/watch?v=Gx-BhcKiQEw) แสดงตัวอย่างดังรูปที่ 8-2

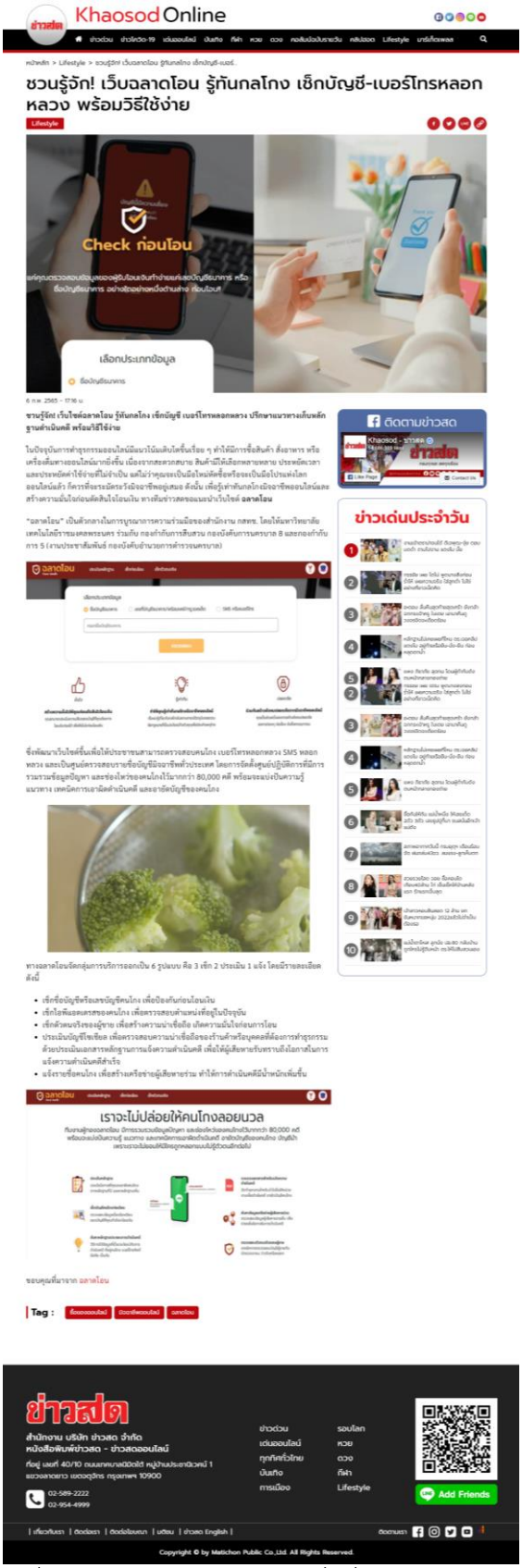
รูปที่ 8-2 สื่อวิดีทัศน์จากช่องฉลาดโอน

8.2 สื่อสิ่งพิมพ์ออนไลน์

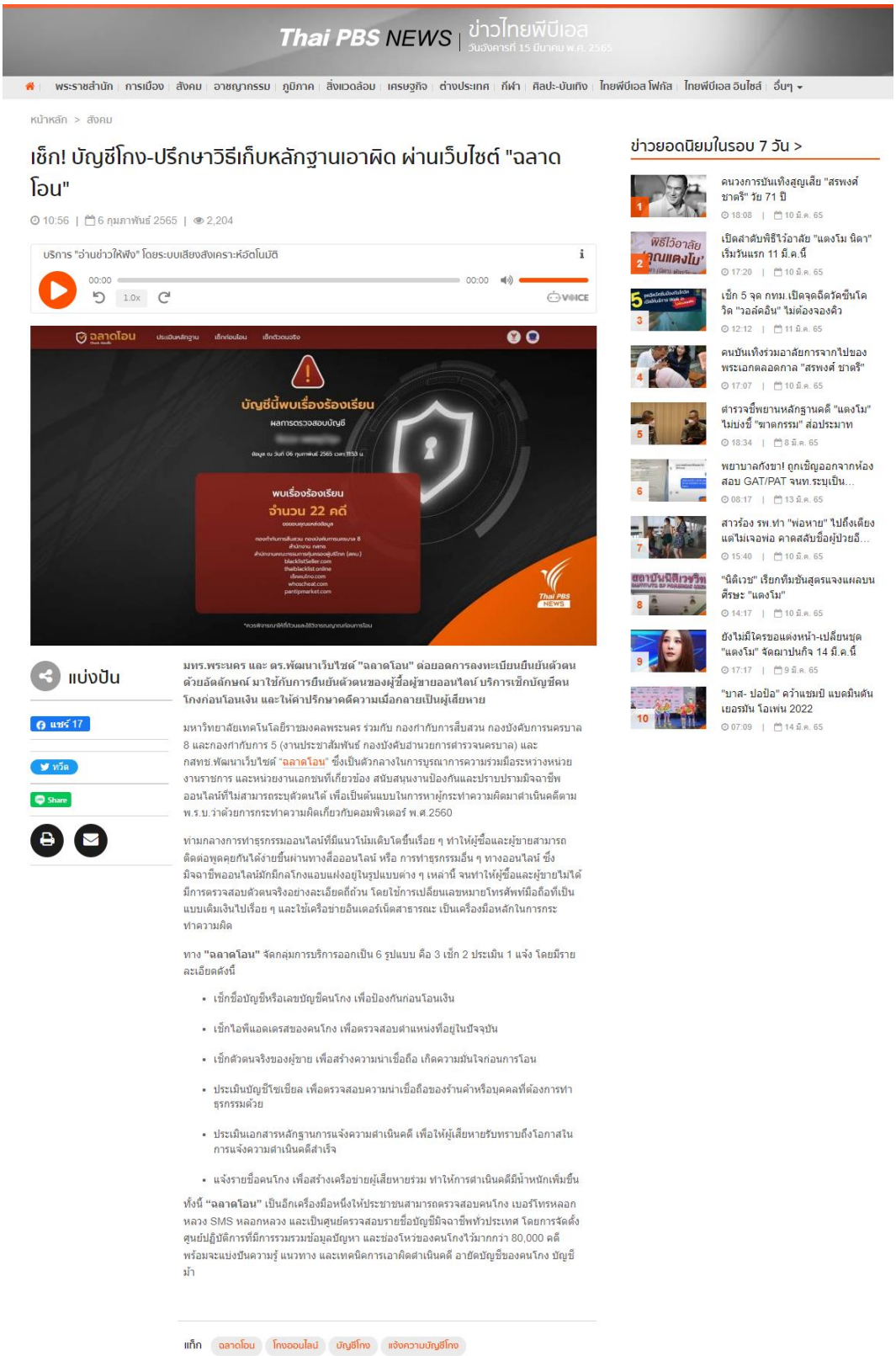
เว็บไซต์ฉลาดโอน มีการเปิดตัวเมื่อวันที่ 4 กุมภาพันธ์ 2565 เป็นครั้งแรก โดยเปิดให้ประชาชนทั่วไปเข้าใช้บริการในด้านต่าง ๆ โดยจัดกลุ่มการบริการออกเป็น 6 รูปแบบ คือ 3 เช็ก 2 ประเมิน 1 แจ้ง ดังนี้

- เช็กชื่อบัญชีหรือเลขบัญชีคนโกง เพื่อป้องกันก่อนโอนเงิน
- เช็กไอพีแอดเดรสของคนโกง เพื่อตรวจสอบตำแหน่งที่อยู่ในปัจจุบัน
- เช็กตัวตนจริงของผู้ขาย เพื่อสร้างความน่าเชื่อถือ เกิดความมั่นใจก่อนการโอน
- ประเมินบัญชีโซเชียล เพื่อตรวจสอบความน่าเชื่อถือของร้านค้าหรือบุคคลที่ต้องการทำธุรกรรมด้วยประเมินเอกสารหลักฐานการแจ้งความดำเนินคดี เพื่อให้ผู้เสียหายรับทราบถึงโอกาสในการแจ้งความดำเนินคดีสำเร็จ
- แจ้งรายชื่อคนโกง เพื่อสร้างเครือข่ายผู้เสียหายร่วม ทำให้การดำเนินคดีมีน้ำหนักเพิ่มขึ้น

หลังจากที่ได้เปิดตัวระบบฉลาดโอน ก็ได้รับผลตอบรับที่ดี มีผู้เข้ามาใช้เช็กบัญชีคนโกง เฉลี่ยวันละ 1,000 ครั้งเป็นอย่างน้อย มีสื่อหนังสือพิมพ์ออนไลน์นำเสนอข่าวเกี่ยวกับฉลาดโอนอย่างแพร่หลาย ในหลายสำนักข่าวไม่ว่าจะเป็นข่าวสดออนไลน์ คมชัดลึกออนไลน์ ไทยพีบีเอส เป็นต้น รวมถึงถูกกล่าวถึงบนแพลตฟอร์มโซเชียลมีเดีย เช่น ทวิตเตอร์ เฟสบุ๊ค เป็นต้น แสดงตัวอย่างดังรูปที่ 8-3 ถึง 8-8



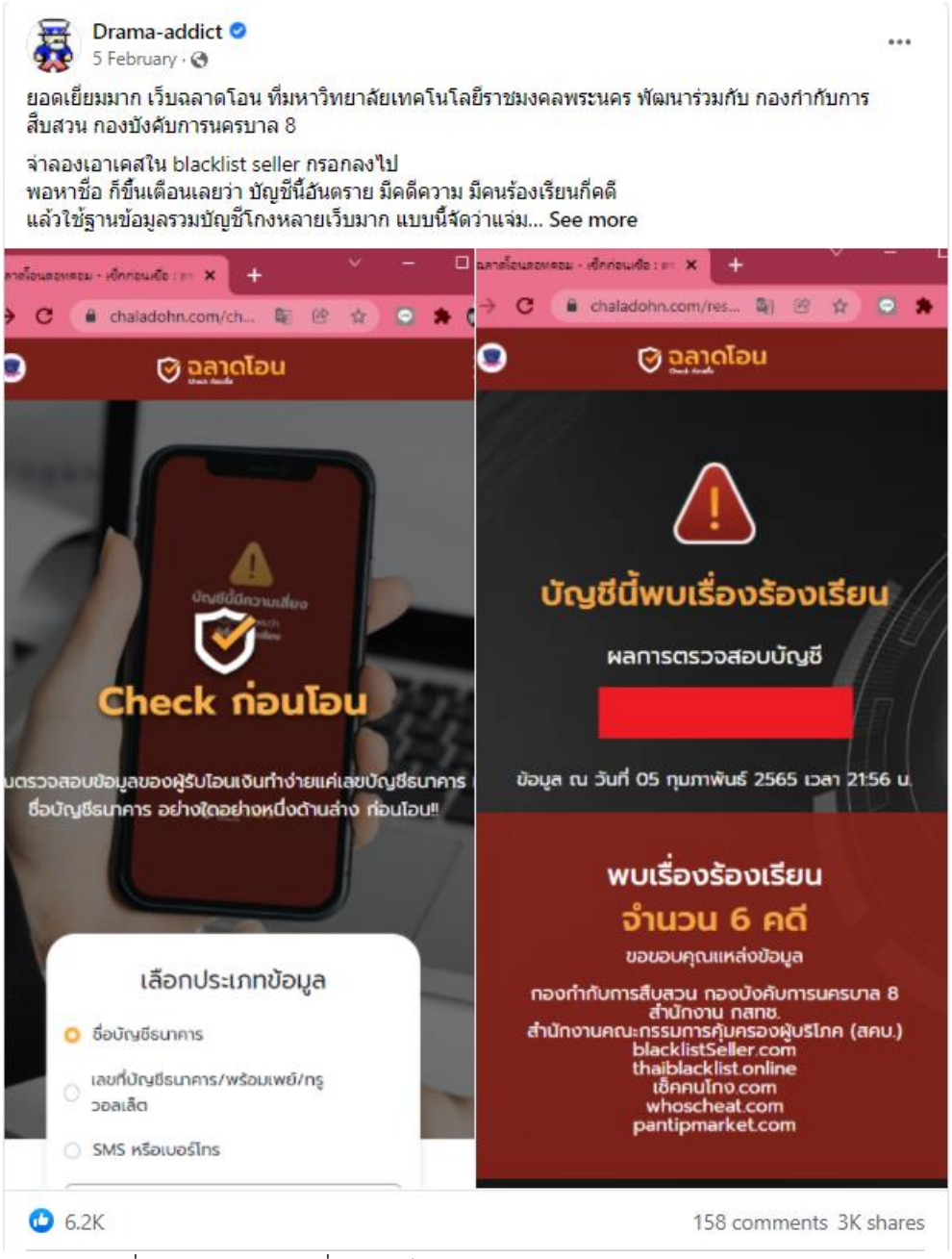
รูปที่ 8-3 การลงข่าวเกี่ยวกับเว็บไซต์ฉลาดโอนบนสื่อสิ่งพิมพ์ออนไลน์ของข่าวสดออนไลน์



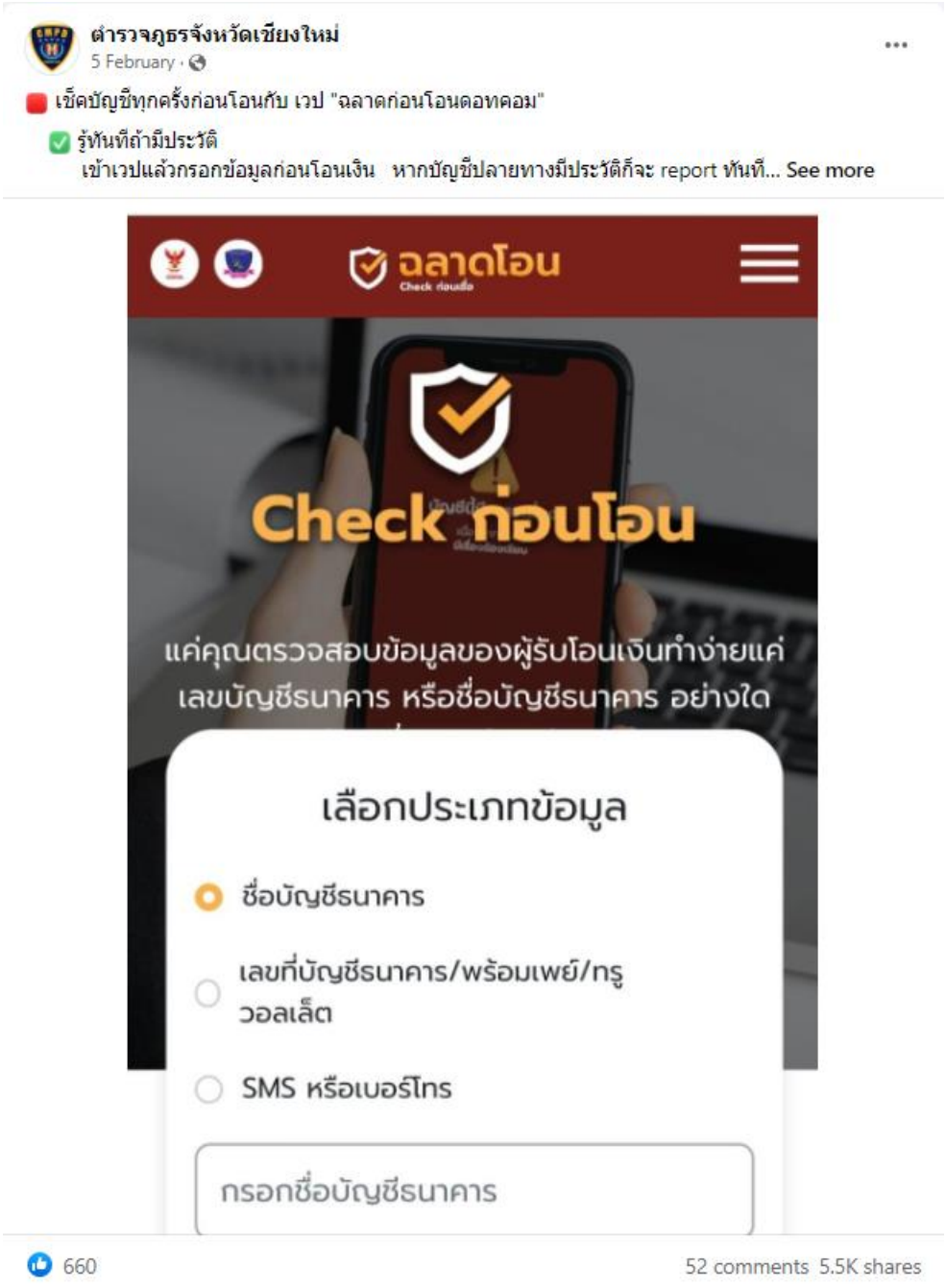
รูปที่ 8-4 การลงข่าวเกี่ยวกับเว็บไซต์ฉลาดโอนบนสื่อสิ่งพิมพ์ออนไลน์ของไทยพีบีเอส

รูปที่ 8-5 การลงข่าวเกี่ยวกับเว็บไซต์ฉลาดโอนบนแพลตฟอร์มทวิตเตอร์ของบัญชีผู้ใช้งานชื่อ “Sunshine Redio”

รูปที่ 8-6 การลงข่าวเกี่ยวกับเว็บไซต์ฉลาดโอนบนแพลตฟอร์มทวิตเตอร์ของบัญชีผู้ใช้งานชื่อ “Sale Here”



รูปที่ 8-7 การลงข่าวเกี่ยวกับเว็บไซต์ฉลาดโอนบนแพลตฟอร์มเฟสบุ๊กของบัญชีผู้ใช้งานชื่อ “Drama-addict”



รูปที่ 8-8 การลงข่าวเกี่ยวกับเว็บไซต์ฉลาดโอนบนแพลตฟอร์มเฟสบุ๊กของ
บัญชีผู้ใช้งานชื่อ “ตำรวจภูธรจังหวัดเชียงใหม่”

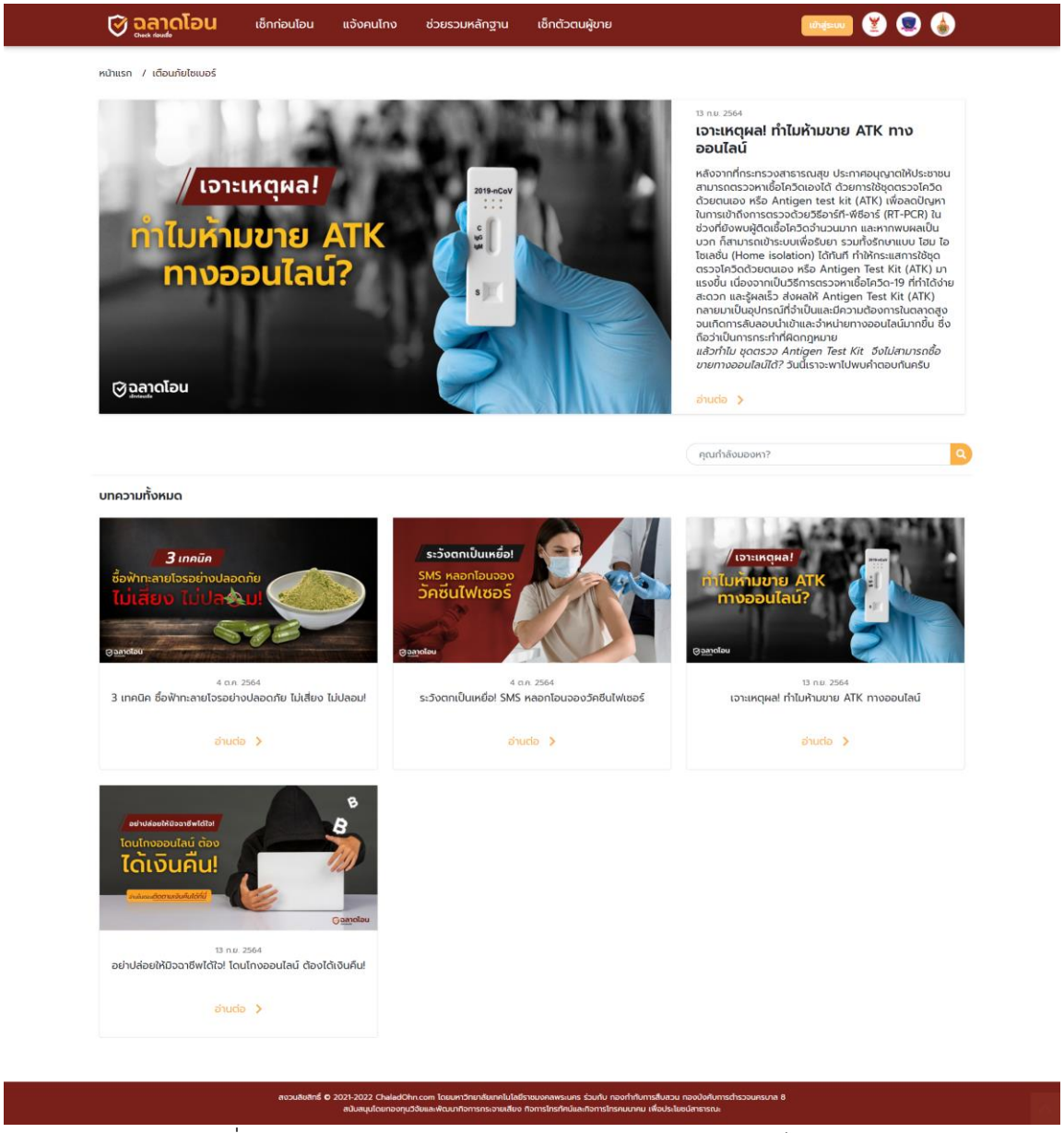
8.3 บทความบนเว็บไซต์ฉลาดโอน

การนำเสนอระบบฉลาดโอน หรือระบบต้นแบบฯ เพื่อสนับสนุนแนวทางการป้องกันและปราบปรามมิจฉาชีพออนไลน์ อันมีวัตถุประสงค์เพื่อมุ่งเน้นให้ผู้ใช้งานระบบต้นแบบฯ หรือผู้บริโภคสินค้าออนไลน์ตระหนักถึงความสำคัญของการศึกษาและตรวจสอบข้อมูลที่ระบุถึงตัวตน รวมทั้งประวัติการกระทำความผิดของบุคคลที่ตนต้องการทำธุรกรรมโอนเงินเสียก่อน คณะผู้วิจัยจึงได้นำเสนอเนื้อหาให้เป็นไปตามแนวทางการป้องกันและปราบปรามมิจฉาชีพออนไลน์ ผ่านการถ่ายทอดที่มุ่งเน้นให้ผู้ใช้งานระบบต้นแบบฯ เล็งเห็นถึงความสำคัญของการตระหนักรู้ถึงความสำคัญของการตรวจสอบข้อมูลบุคคลที่ตนต้องการจะทำธุรกรรมโอนเงิน หรือทราบถึงประวัติการกระทำความผิดของบุคคลนั้น ตลอดจนชื่อบัญชีธนาคาร หรือเลขที่บัญชีธนาคารก่อนการทำธุรกรรมโอนเงินออนไลน์ รวมทั้งออกแบบส่วนการเสริมสร้างองค์ความรู้เกี่ยวกับการทำธุรกรรมออนไลน์ เพื่อให้ผู้ใช้งานระบบต้นแบบฯ ทราบถึงแนวทางการป้องกันและปราบปรามมิจฉาชีพออนไลน์ผ่านบทความที่จะให้เสริมสร้างความรู้และความเข้าใจเกี่ยวกับกฎหมายและกรณีตัวอย่างที่มีความเกี่ยวข้องกับการทำธุรกรรมออนไลน์อีกด้วย นอกจากนี้ยังมีการประชาสัมพันธ์คดีที่เจ้าหน้าที่ตำรวจสามารถจับกุมตัวผู้กระทำผิดมาดำเนินคดีได้เป็นที่เรียบร้อยแล้วอีกด้วย

เว็บไซต์ฉลาดโอน ได้มีการลงบทความ เพื่อใช้สำหรับการประชาสัมพันธ์โครงการ โดยแบ่งหมวดหมู่ของบทความออกเป็น 4 หัวข้อ ดังนี้

(1) เตือนภัยไซเบอร์

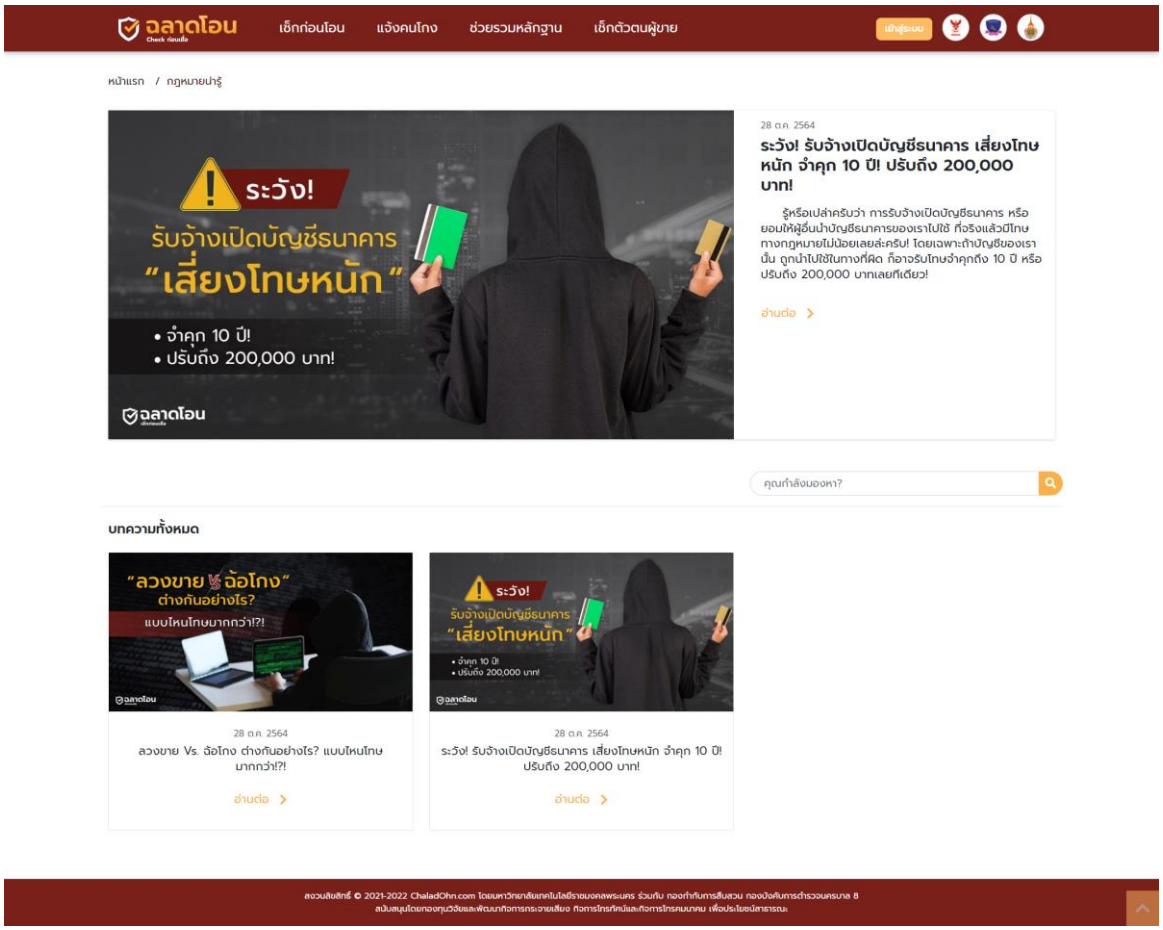
ในหัวข้อเตือนภัยไซเบอร์จะนำเสนอในแง่มุมของการนำเสนอผ่านเหตุการณ์ข่าวสารในปัจจุบันที่มีความเกี่ยวข้องกับการทำธุรกรรมออนไลน์ โดยมีเนื้อหาถึงเหตุการณ์ที่เกิดขึ้น ข้อสรุปของเหตุการณ์ และข้อกฎหมายที่มีความเกี่ยวข้องกับเหตุการณ์ ให้มีความเข้าใจง่าย ประชาชนทั่วไปสามารถเข้าถึงสาระสำคัญของข้อกฎหมายนั้น และสามารถนำความรู้ที่เกี่ยวข้องกับข้อกฎหมายนั้นไปประยุกต์ใช้ได้ในการดำเนินชีวิต เพื่อเป็นแนวทางการป้องกันและปราบปรามมิจฉาชีพออนไลน์



รูปที่ 8-9 หน้าจอแสดงการลงบทความหมวดหมู่ “เตือนภัยไซเบอร์”

(2) กฎหมายน่ารู้

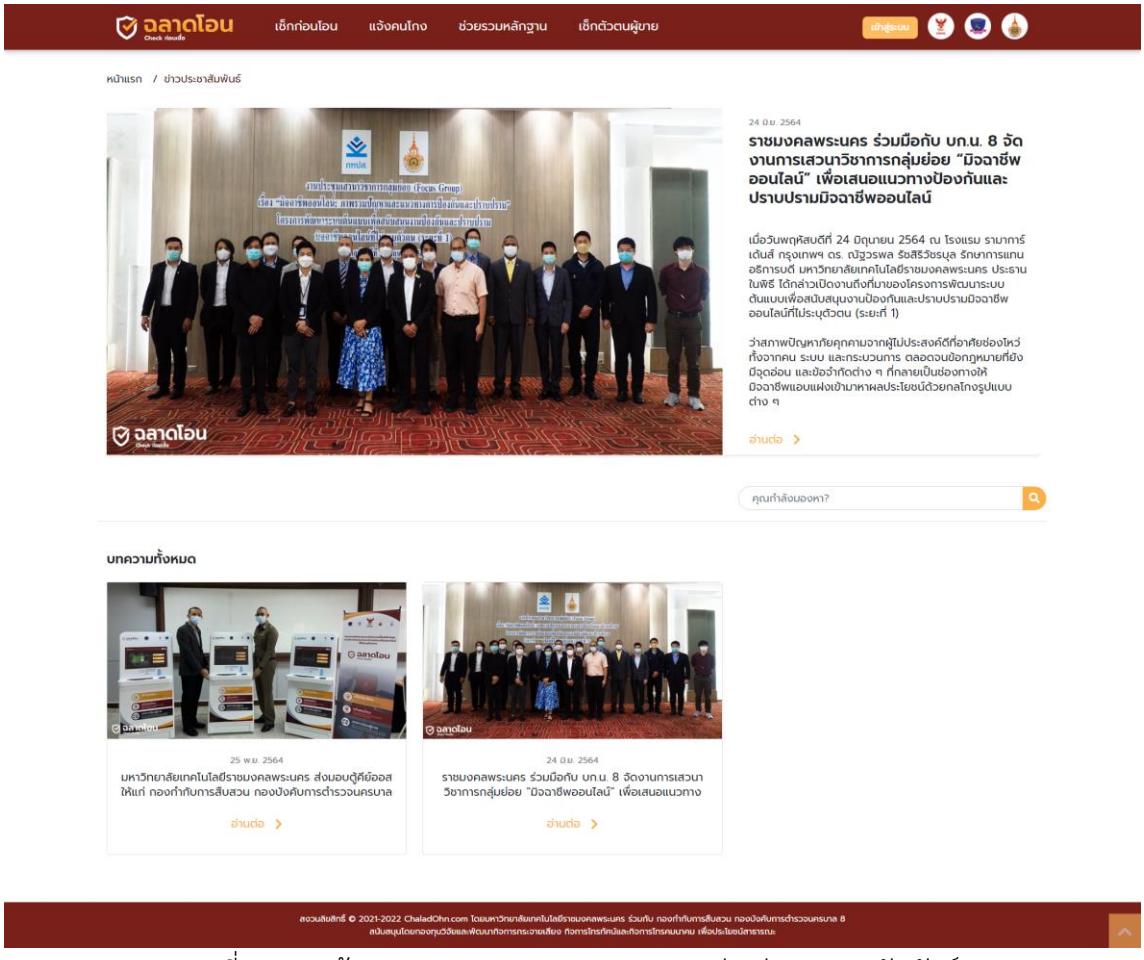
ในหัวข้อกฎหมายน่ารู้ ทางผู้วิจัยได้นำเสนอบทความในมุมมองของการนำข้อกฎหมายที่มีความเกี่ยวข้องกับการทำธุรกรรมออนไลน์มานำเสนอในแง่มุมที่เข้าใจง่าย เป็นประโยชน์ต่อประชาชนทั่วไปที่มีพฤติกรรมในการซื้อ-ขายสินค้าออนไลน์ หรือให้ความสนใจต่อขั้นตอนการค้นหาบัญชีผู้กระทำความผิด เพื่อเสริมสร้างองค์ความรู้ และเสริมสร้างความมั่นใจก่อนการทำธุรกรรมโอนเงินออนไลน์



รูปที่ 8-10 หน้าจอแสดงการลงบทความหมวดหมู่ “เตือนภัยไซเบอร์”

(3) ข่าวประชาสัมพันธ์

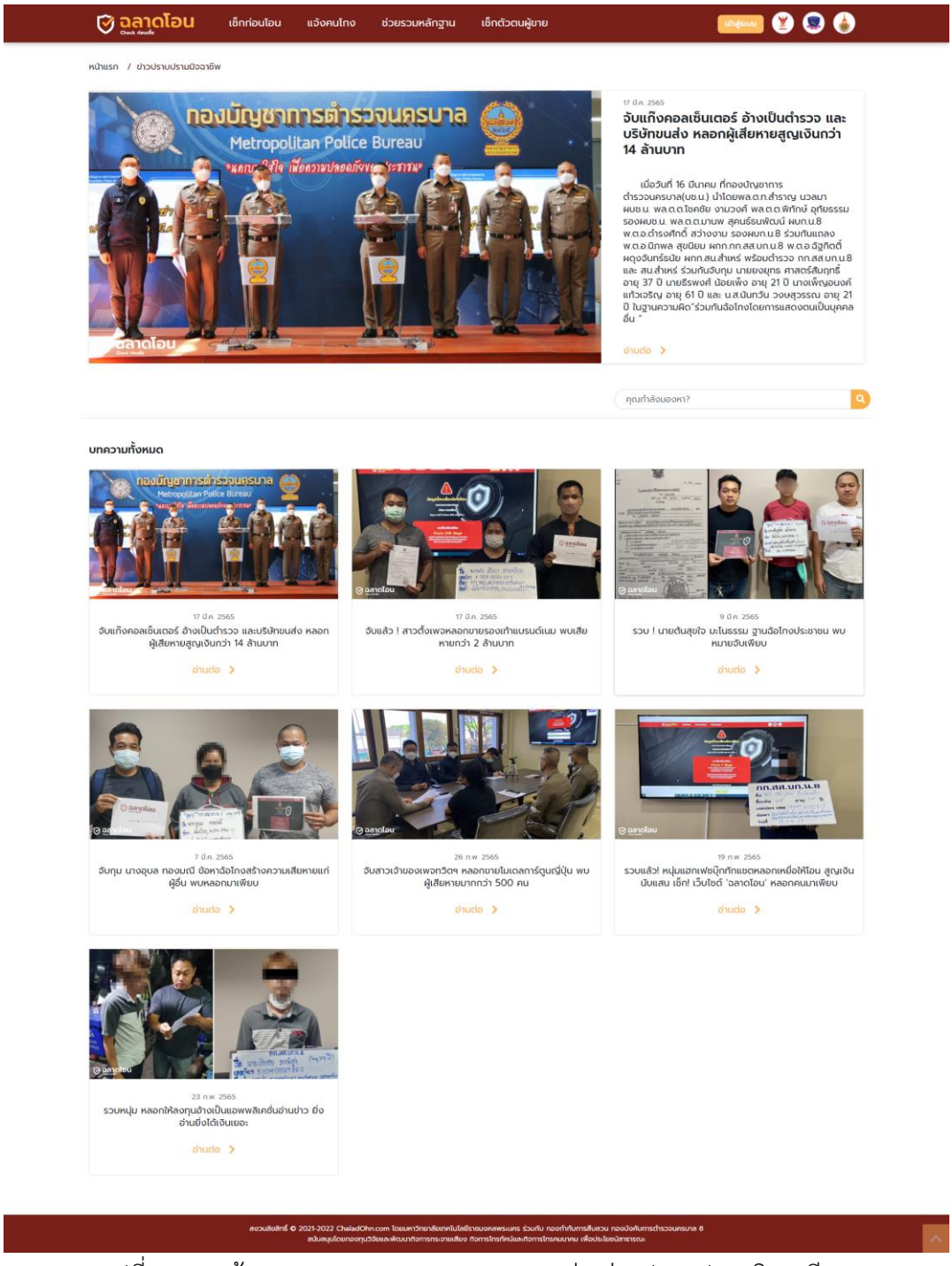
หัวข้อข่าวประชาสัมพันธ์ ผู้วิจัยใช้สำหรับรวบรวมเหตุการณ์ที่เกิดขึ้นระหว่างการดำเนินโครงการ เช่น การจัดงานเสวนาการประชุมกลุ่มย่อย เพื่อเสนอแนวทางป้องกันและปราบปรามมิจฉาชีพออนไลน์ หรือการส่งมอบตู้คีออสให้แก่ กองกำกับการสืบสวน กองบังคับการตำรวจนครบาล 8



รูปที่ 8-11 หน้าจอแสดงการลงบทความหมวดหมู่ “ข่าวประชาสัมพันธ์”

(4) ข่าวปราบปรามมิจฉาชีพ

หัวข้อข่าวปรามปรามมิจฉาชีพ ใช้สำหรับการประชาสัมพันธ์ การเข้าจับกุมผู้ต้องหาของคดีที่เกี่ยวข้องกับการซื้อขายออนไลน์ ที่มีการใช้ข้อมูลจากฉลาดโอนในการสืบสวนร่วมด้วย เพื่อให้ผู้เสียหายได้รับทราบ และเข้ามาแจ้งความเพื่อเป็นผู้เสียหายร่วมของผู้ต้องหาแต่ละราย นอกจากนี้ยังใช้เพื่อเตือนภัยประชาชน ให้เห็นถึงรูปแบบวิธีการโกงผ่านช่องทางออนไลน์รูปแบบต่าง ๆ และรู้เท่าทันมิจฉาชีพออนไลน์อีกช่องทางหนึ่ง



รูปที่ 8-12 หน้าจอแสดงการลงบทความหมวดหมู่ “ข่าวปราบปรามมิจฉาชีพ”

บทที่ 9
รายงานการเข้าใช้งานระบบฯ

บทที่ 9 นี้ จัดทำขึ้นเพื่อสรุปรายงานสถิติการเข้าใช้งานของระบบต้นแบบเพื่อสนับสนุนงานป้องกันและปราบปรามมิจฉาชีพออนไลน์ที่ไม่ระบุตัวตน ตั้งแต่ช่วงวันที่ 1 กุมภาพันธ์ 2565 ถึง 20 มีนาคม 2565 รวมระยะเวลา 48 วัน โดยแบ่งข้อมูลออกเป็น 2 ส่วน ได้แก่ สถิติการเข้าใช้งานผ่านเว็บไซต์ฉลาดโอน และสถิติการเข้าใช้งานผ่านช่องทาง LINE Official Account ฉลาดโอน.com

สำหรับดัชนีชี้วัดความสำเร็จระดับผลลัพธ์ของโครงการฯ มีดังนี้

ตัวชี้วัด	เป้าหมาย	ผลลัพธ์	หมายเหตุ
พนักงานสอบสวนในเขตพื้นที่ศึกษา สามารถรวบรวมหลักฐานเพื่อดำเนินคดีกับผู้ถูกกล่าวหาในชั้นศาล	เพิ่มขึ้น 50%	ข้อมูลตำรวจ เดือน ม.ค. 65 – 29 เคส ข้อมูลตำรวจ เดือน ก.พ. 65 – 13 เคส ข้อมูลฉลาดโอน เดือน ก.พ. 65 – 3 เคส	
จำนวนคดีมิจฉาชีพธุรกรรมออนไลน์ที่ไม่สามารถระบุตัวตนผู้ถูกกล่าวหาได้ในเขตพื้นที่ศึกษา	ลดลง 50%	ข้อมูลตำรวจ เดือน ม.ค. 65 – 3 เคส ข้อมูลตำรวจ เดือน ก.พ. 65 – 1 เคส ข้อมูลฉลาดโอน เดือน ก.พ. 65 – 0 เคส	
การใช้งานของผู้ซื้อสินค้าออนไลน์			
ลงทะเบียนยืนยันตัวตน	5,000 คน	5,392 คน	
ใช้งานเว็บไซต์	20,000 ครั้ง	119,725 ครั้ง	

(ข้อมูล ณ วันที่ 20 มีนาคม 2565)

9.1 สถิติการเข้าใช้งานผ่านเว็บไซต์

คณะผู้วิจัยได้สรุปรายงานสถิติการเข้าใช้งานผ่านเว็บไซต์ฉลาดโอน (www.chaladohn.com) แยกออกเป็นประเภทต่าง ๆ ได้แก่ จำนวนสมาชิกทั้งหมด จำนวนผู้แจ้ง จำนวนผู้รวบรวมหลักฐาน จำนวนผู้ขาย จำนวนการเช็กคนโกง จำนวนการเช็กตันตน จำนวนการแจ้งคนโกง และจำนวนช่วยรวมหลักฐาน นอกจากนี้ ยังแสดงรายงานจำนวนรายการตรวจสอบบัญชีของผู้ใช้งาน รายงานจำนวนผู้ใช้งานที่ลงทะเบียนยืนยันตัวตน และรายงานจำนวนรายการแจ้งคนโกงของผู้ใช้งาน แสดงดังรูปที่ 9-1

รูปที่ 9-1 แสดงรายงานสถิติการเข้าใช้งานเว็บไซต์ฉลาดโอน

9.1.1 สถิติการลงทะเบียนยืนยันตัวตนบนเว็บไซต์ฉลาดโอน

สถิติการลงทะเบียนยืนยันตัวตนผ่านเว็บไซต์ฉลาดโอนในระดับต่าง ๆ ช่วงวันที่ 1 กุมภาพันธ์ 2565 – 20 มีนาคม 2565 มีดังนี้

รายการ	จำนวน (คน)
เลขหมายโทรศัพท์	1,073
เลขหมายโทรศัพท์ + บัตรประจำตัวประชาชน	177
เลขหมายโทรศัพท์ + บัตรประจำตัวประชาชน + ภาพถ่ายใบหน้าของผู้ลงทะเบียน (อัตลักษณ์)	149
เลขหมายโทรศัพท์ + บัตรประจำตัวประชาชน + ภาพถ่ายใบหน้าของผู้ลงทะเบียน (อัตลักษณ์) +บัญชีธนาคาร	93
รวม	1,492

9.1.2 สถิติการเข้าใช้งานเว็บไซต์ฉลาดโอน

สถิติการเข้าใช้งานเว็บไซต์ฉลาดโอนในฟังก์ชันต่าง ๆ ช่วงวันที่ 1 กุมภาพันธ์ 2565 – 20 มีนาคม 2565 มีดังนี้

รายการ	จำนวน (ครั้ง)
การเช็กคนโกง	119,190
การเช็กตัวตน	161
การแจ้งคนโกง	290
การช่วยรวมหลักฐาน	161
รวม	119,802

9.1.3 สถิติการเช็กคนโกง

สถิติการเช็กคนโกงผ่านเว็บไซต์ฉลาดโอนสามารถแบ่งการตรวจสอบออกเป็น 3 ประเภท ได้แก่ การตรวจสอบผ่านชื่อบัญชีธนาคาร การตรวจสอบผ่านเลขที่บัญชีธนาคาร และการตรวจสอบผ่านหมายเลขโทรศัพท์หรือระบบการส่งข้อความระยะสั้น (Short Message Service, SMS) ช่วงวันที่ 1 กุมภาพันธ์ 2565 – 20 มีนาคม 2565 มีรายละเอียดดังนี้

รายการตรวจสอบ	จำนวน (คน)	ร้อยละ (%)
ชื่อบัญชีธนาคาร	59,583	50
เลขที่บัญชีธนาคาร	39,949	34
หมายเลขโทรศัพท์หรือ SMS	19,658	16
รวม	119,190	100

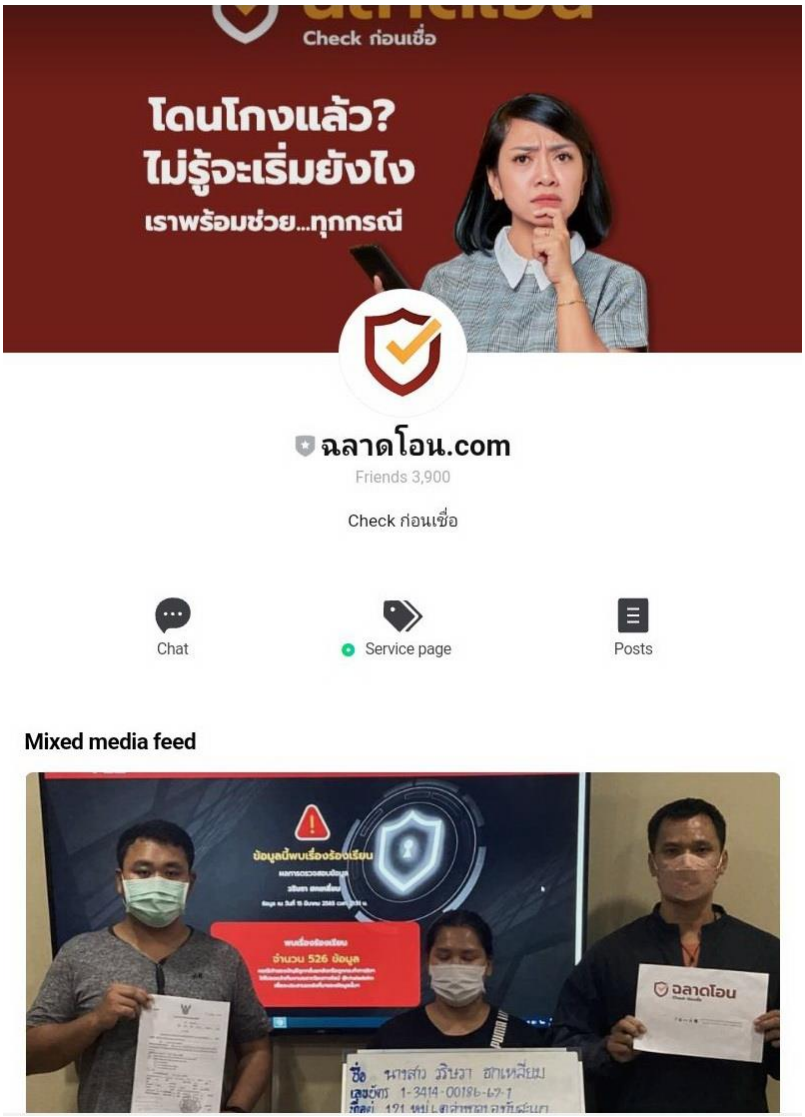
9.1.4 สถิติการแจ้งคนโกง

สถิติการแจ้งคนโกงผ่านเว็บไซต์ฉลาดโอนสามารถแบ่งตามช่องทางการชำระเงินออกเป็น 4 ประเภท ได้แก่บัญชีธนาคาร พร้อมเพย์ ทรูวอลเล็ต และ PayPal ช่วงวันที่ 1 กุมภาพันธ์ 2565 – 20 มีนาคม 2565 มีรายละเอียดดังนี้

รายการตรวจสอบ	จำนวน (คน)	ร้อยละ (%)
บัญชีธนาคาร	456	81
พร้อมเพย์	57	10
ทรูวอลเล็ต	44	8
PayPal	3	1
รวม	560	100

9.2 สถิติการเข้าใช้งานผ่านช่องทาง LINE Official Account ฉลาดโอน.com

จากการรวบรวมสถิติของผู้เสียหายที่เข้าใช้งานผ่านช่องทาง LINE Official Account ฉลาดโอน.com ของฉลาดโอน ตั้งแต่วันที่ 1 กุมภาพันธ์ 2565 – 20 มีนาคม 2565 พบว่ามีผู้ลงทะเบียนผ่าน LINE Official Account เป็นจำนวน 3,900 คน (อัปเดท 20 มี.ค. 65) แสดงดังรูปที่ 9-2 และมีผู้ติดต่อเพื่อสอบถามการเข้าใช้งานระบบฉลาดโอนกับเจ้าหน้าที่เป็นจำนวน 1,657 คน (อัปเดท 20 มี.ค. 65) โดยทางคณะผู้วิจัยแบ่งประเภทการใช้บริการออกเป็น 3 ประเภท ได้แก่ การให้บริการ การติดต่อเจ้าหน้าที่ และอื่น ๆ แสดงดังรูปที่ 9-3



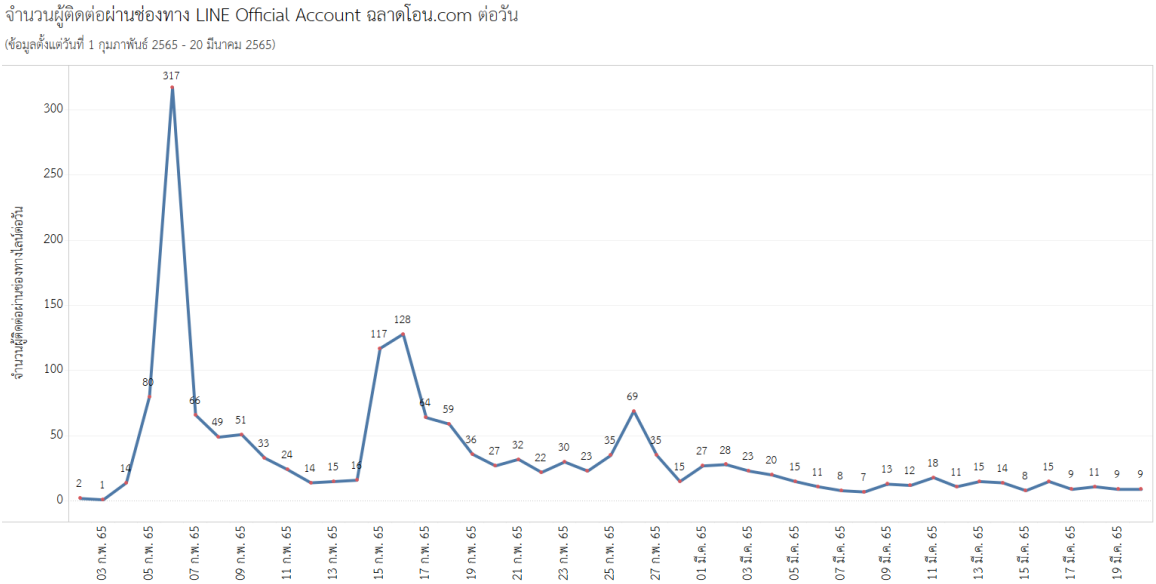
รูปที่ 9-2 รูปภาพแสดงจำนวนผู้ติดตามบนช่องทาง Line Official ฉลาดโอน.com

วันที่	ผู้ใช้งาน	การให้บริการ						ติดต่อเจ้าหน้าที่			อื่น ๆ
		เช็กคนโกง	เช็กหลักฐาน	เช็กตัวตน	ประเมินบัญชีโซเชียล	ช่วยรวมหลักฐาน	แจ้งคนโกง	สอบถาม	แจ้งปัญหาการใช้งาน	ข้อเสนอแนะ	
1 ก.พ. 65	2						1				
2 ก.พ. 65	-										
3 ก.พ. 65	1						1				
4 ก.พ. 65	14	2				2	9	1			2
5 ก.พ. 65	80	17	5	1	1	9	22	4			23
6 ก.พ. 65	317	67	1	3	6	45	58	33	4	1	102
7 ก.พ. 65	66	4			1	11	19	8	4		19
8 ก.พ. 65	49	7	1	1		10	16	3	1		12
9 ก.พ. 65	51	4		1		14	21	7	1		4
10 ก.พ. 65	33	9		2		4	15	4			1
11 ก.พ. 65	24	3		2		2	10	2			5
12 ก.พ. 65	14	3		1		1	5				4
13 ก.พ. 65	15					3	11	1			1
14 ก.พ. 65	16	2		2		5	4	3			1
15 ก.พ. 65	117	33	1	5	6	18	26	25			10
16 ก.พ. 65	128	22		6	10	27	28	27			12
17 ก.พ. 65	64	18		4	3	16	8	9			10
18 ก.พ. 65	59	13		2	1	5	20	17			6
19 ก.พ. 65	36	7		3	3	5	10	10			1
20 ก.พ. 65	27	5	1	2	2	2	11	2			2
21 ก.พ. 65	32	6	1		1	9	11	5			2
22 ก.พ. 65	22	2		1	4	3	4	4			3
23 ก.พ. 65	30	8		1	2	4	5	7			2
24 ก.พ. 65	23	8		2	1	3	6	5			2
25 ก.พ. 65	35	6		5	2	5	9	6			3
26 ก.พ. 65	69	3	1	3	3	10	33	9			8
27 ก.พ. 65	35	6			2	4	14	5			4
28 ก.พ. 65	15	3			1		5				3
1 มี.ค. 65	27	3	1			3	15	8			2
2 มี.ค. 65	28	12				2	11	7			1
3 มี.ค. 65	23	3	1	1		2	15	4			
4 มี.ค. 65	20	3		1		2	4	10			1
5 มี.ค. 65	15	1				3	8	3			2
6 มี.ค. 65	11	2			1	2	2	7			1
7 มี.ค. 65	8	3			2	4	1	2			
8 มี.ค. 65	7	1				2	1	5			
9 มี.ค. 65	13	2			1	2	3	4			5
10 มี.ค. 65	12	1				2	7	5			1
11 มี.ค. 65	18			1	1	7	4	5	1		
12 มี.ค. 65	11	1		1	2	3	1	2			1
13 มี.ค. 65	15	3			1	7	2	3			1
14 มี.ค. 65	14	3		2	1	4	3	4			1
15 มี.ค. 65	8			1		1	1	3			
16 มี.ค. 65	15	1		2		3	5	3			2
17 มี.ค. 65	9	1		2		1	2	4			1
18 มี.ค. 65	11	3				1	3	4			
19 มี.ค. 65	9	1			1	1	2	4			
20 มี.ค. 65	9	1					1	6			1
รวม	1657	303	13	58	58	269	473	290	11	1	261

รูปที่ 9-3 แสดงภาพรวมสถิติการเข้าใช้งานผ่านช่องทาง LINE Official Account ฉลาดโอน.com

9.2.1 สถิติของจำนวนผู้ติดต่อผ่านช่องทาง LINE Official Account ฉลาดโอน.com

จำนวนผู้ติดต่อผ่านช่องทาง LINE Official Account ฉลาดโอน.com ช่วงวันที่ 1 กุมภาพันธ์ 2565 – 20 มีนาคม 2565 มีจำนวนรวมทั้งสิ้น 1,657 คน โดยวันที่มีติดต่อเข้ามามากที่สุด คือวันที่ 6 กุมภาพันธ์ 2565 มีผู้ติดต่อเข้ามาเป็นจำนวน 317 รายและวันที่มีติดต่อเข้ามน้อยที่สุด คือวันที่ 3 กุมภาพันธ์ 2565 มีผู้ติดต่อเข้ามาเป็นจำนวน 1 ราย แสดงรายละเอียดดังรูปที่ 9-4



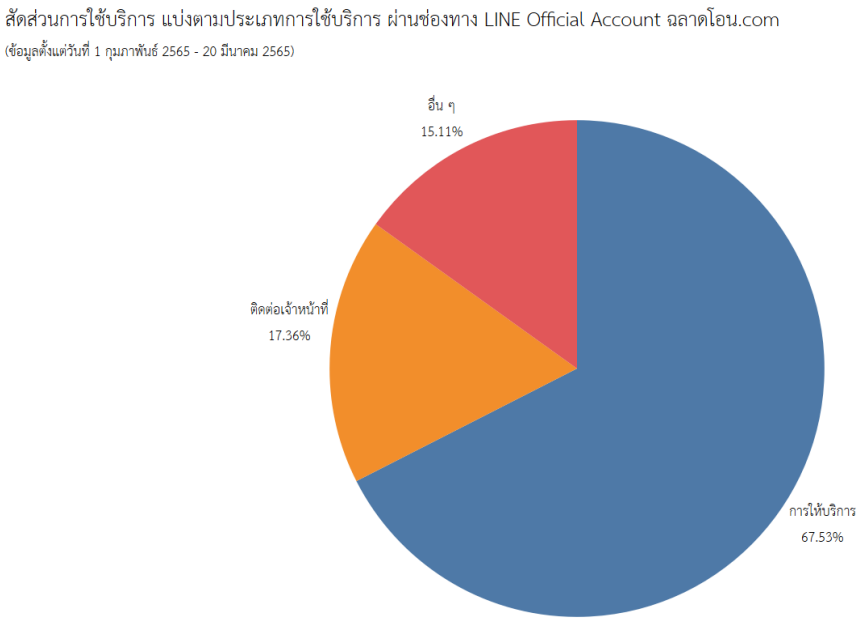
รูปที่ 9-4 แสดงจำนวนผู้ติดต่อผ่านช่องทาง LINE Official Account ฉลาดโอน.com ในแต่ละวัน

9.2.2 สถิติการใช้บริการ แบ่งตามประเภทการใช้บริการผ่านช่องทาง LINE Official Account ฉลาดโอน.com

สถิติการใช้งานของผู้ที่ติดต่อเข้ามา แบ่งออกได้เป็น 3 ประเภท คือ

1. ต้องการให้เจ้าหน้าที่ฉลาดโอนให้ความช่วยเหลือในด้านต่าง ๆ (3 เช็ก 2 ประเมิน 1 แจ้ง)
2. ติดต่อสอบถาม หรือแจ้งปัญหาการใช้งานกับเจ้าหน้าที่ฉลาดโอน
3. อื่น ๆ เช่น การส่งข้อความให้กำลังใจ กดติดตามเผื่อไว้ใช้ในวันหลัง

โดยแบ่งจำนวนการติดต่อเข้ามาของผู้ใช้งานดังนี้ สัดส่วนการขอความช่วยเหลือจากเจ้าหน้าที่ฉลาดโอนมีจำนวนมากที่สุด จำนวน 1,175 ราย คิดเป็น 67.53% รองลงมาคือการติดต่อสอบถาม หรือแจ้งปัญหาการใช้งานกับเจ้าหน้าที่ฉลาดโอน จำนวน 302 ราย คิดเป็น 17.36% และลำดับสุดท้ายคืออื่น ๆ มีจำนวน 263 ราย คิดเป็น 15.11% แสดงดังรูปที่ 9-5



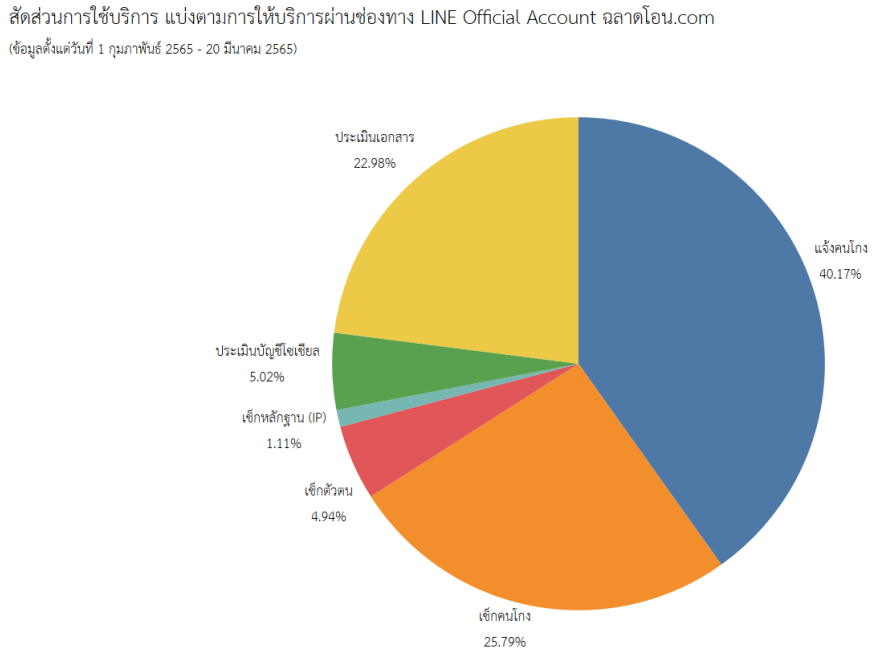
รูปที่ 9-5 แสดงสถิติการใช้บริการแบ่งตามประเภทการใช้บริการผ่านช่องทาง LINE Official Account ฉลาดโอน.com

9.2.3 สถิติการใช้บริการ แบ่งตามการให้บริการผ่านช่องทาง LINE Official Account ฉลาดโอน.com

การให้บริการของเจ้าหน้าที่ฉลาดโอน แบ่งออกเป็น 6 ประเภท ดังนี้

1) เช็กคนโกง
2) เช็กหลักฐาน
3) เช็กตัวตน
4) ประเมินบัญชีโซเชียล
5) ประเมินเอกสาร (ช่วยรวมหลักฐาน)
6) แจ้งคนโกง

การให้บริการของผู้ที่ติดต่อผ่านช่องทาง LINE Official Account ฉลาดโอน.com ช่วงวันที่ 1 กุมภาพันธ์ 2565 – 20 มีนาคม 2565 มีจำนวนรวมทั้งสิ้น 1,657 คน แบ่งจำนวนตามประเภทต่าง ๆ ได้ดังนี้ การให้บริการที่มีผู้ใช้งานมากที่สุดคือการแจ้งคนโกง มีจำนวน 472 ราย คิดเป็น 40.17% รองลงมาคือการเช็กคนโกง มีจำนวน 303 ราย คิดเป็น 25.79% การประเมินหลักฐาน มีจำนวน 270 ราย คิดเป็น 22.98% ส่วนการให้บริการที่มีผู้ใช้งานน้อยที่สุดคือการเช็กหลักฐาน มีจำนวน 13 ราย คิดเป็น 1.11% แสดงดังรูปที่ 9-6



รูปที่ 9-6 แสดงสถิติการให้บริการผ่านช่องทาง LINE Official Account ฉลาดโอน.com

คู่มือผู้ใช้งานทั่วไป

สารบัญ

1. ขั้นตอนเข้าสู่ระบบ

เข้าสู่เว็บไซต์ https://chaladohn.com จะแสดงหน้าจอเว็บไซต์หลักของฉลาดโอน โดยการเข้าสู่ระบบจะแบ่งเป็น 2 กรณีคือ กรณีที่ 1 ลงทะเบียนสำหรับผู้ใช้งานใหม่ และกรณีที่ 2 เข้าสู่ระบบสำหรับผู้ที่มีบัญชีอยู่แล้ว

1.1 ลงทะเบียนสำหรับผู้ใช้งานใหม่

ผู้ใช้งานที่ยังไม่เคยลงทะเบียนกับฉลาดโอน สามารถลงทะเบียนผ่านเว็บไซต์ฉลาดโอน ได้ 3 ช่องทาง ดังนี้

1.1.1 ลงทะเบียนเพื่อแจ้งคนคนโกง

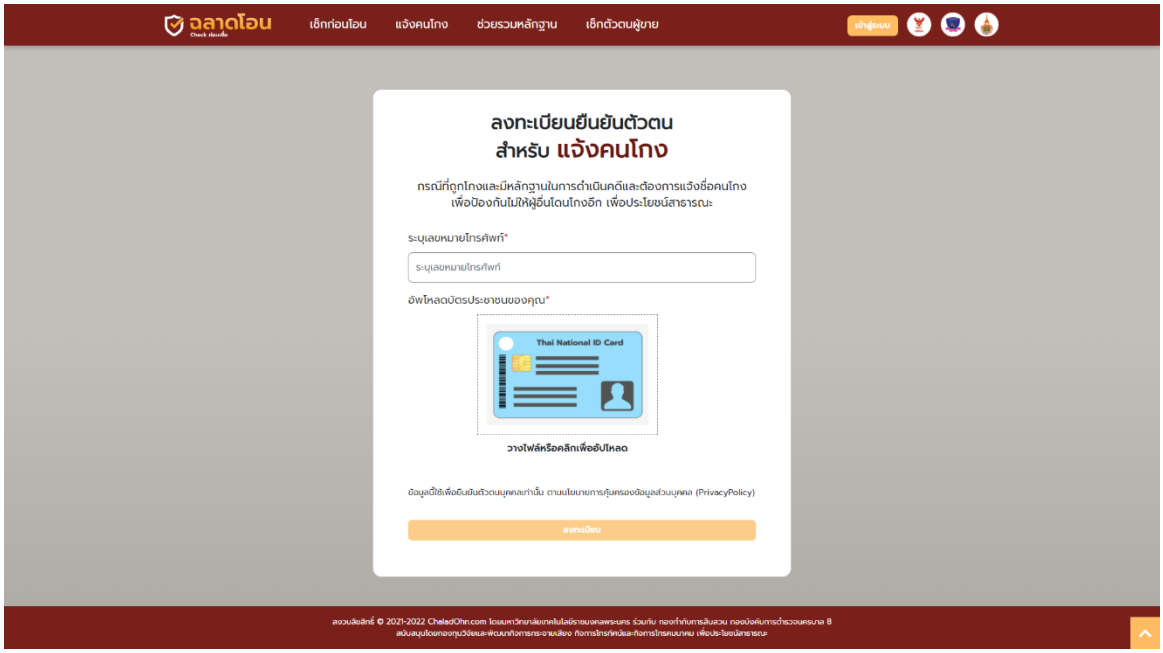
ให้ผู้ใช้งานคลิกเลือกเมนู “แจ้งคนโกง” หรือ “เข้าสู่ระบบ” แสดงดังรูปที่ 1 เพื่อทำการลงทะเบียน

รูปที่ 1 ขั้นตอนการเข้าเมนูแจ้งคนโกงบนหน้าจอเว็บไซต์หน้าหลัก

จากนั้น กดปุ่มลงทะเบียน เพื่อเข้าสู่ขั้นตอนการยืนยันตัวตน แสดงดังรูปที่ 2

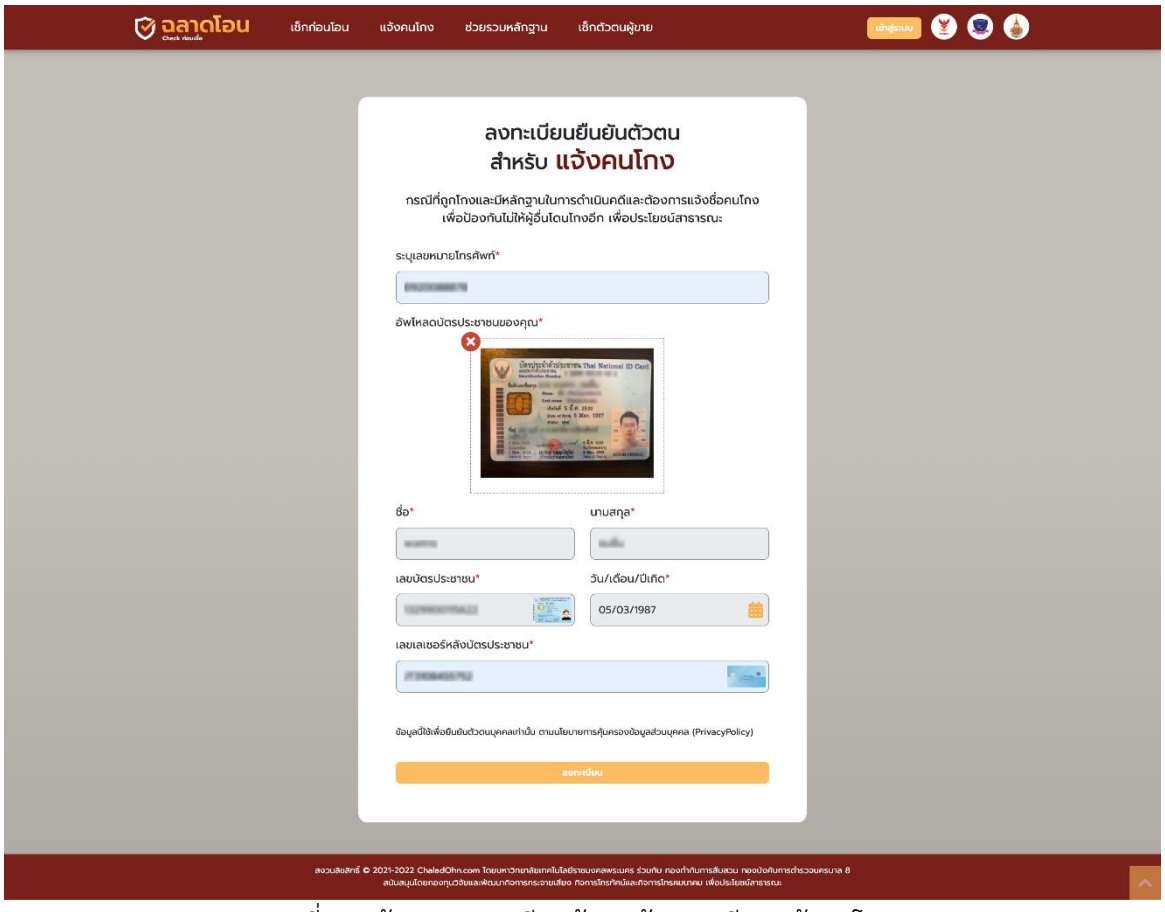
รูปที่ 2 หน้าจอแสดงขั้นตอนการลงทะเบียนแจ้งคนโกง

จะพบหน้าจอลงทะเบียนยืนยันตัวตน แสดงดังรูปที่ 3



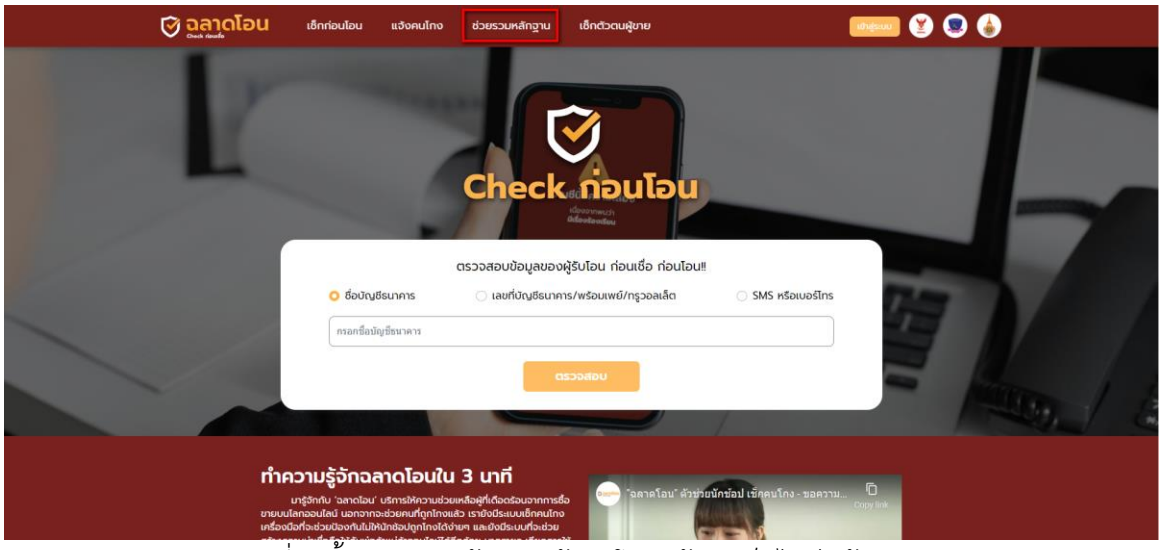
รูปที่ 3 หน้าจอลงทะเบียนยืนยันตัวตนสำหรับแจ้งคนโกง

ให้ผู้ใช้งาน กรอกเลขหมายโทรศัพท์และอัปโหลดบัตรประจำตัวประชาชนลงในระบบ จากนั้น ตรวจสอบข้อมูลและกดปุ่มลงทะเบียน แสดงดังรูปที่ 4



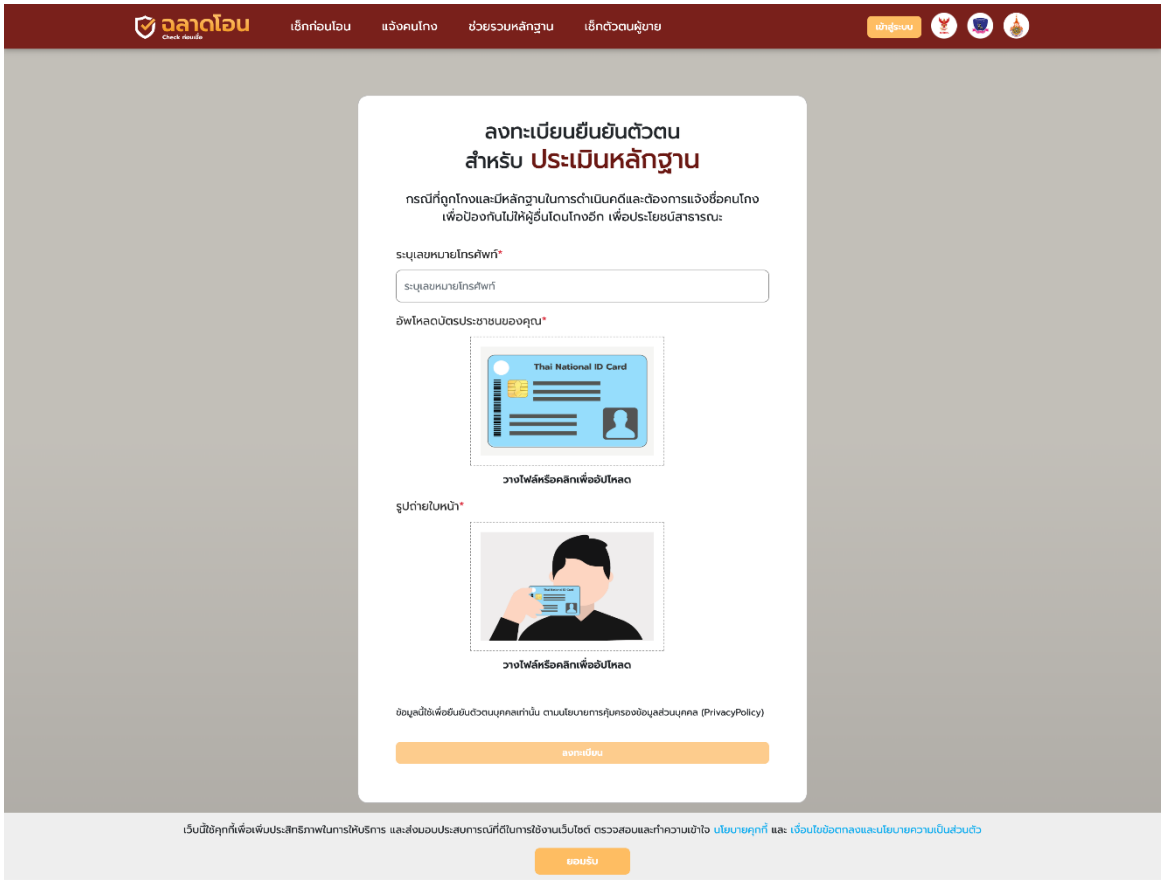
รูปที่ 4 หน้าจอรายละเอียดข้อมูลผู้ลงทะเบียนแจ้งคนโกง

1.1.2 ลงทะเบียนเพื่อช่วยรวมหลักฐาน
ให้ผู้ใช้งานคลิกที่เมนู “ช่วยรวมหลักฐาน” แสดงดังรูปที่ 5



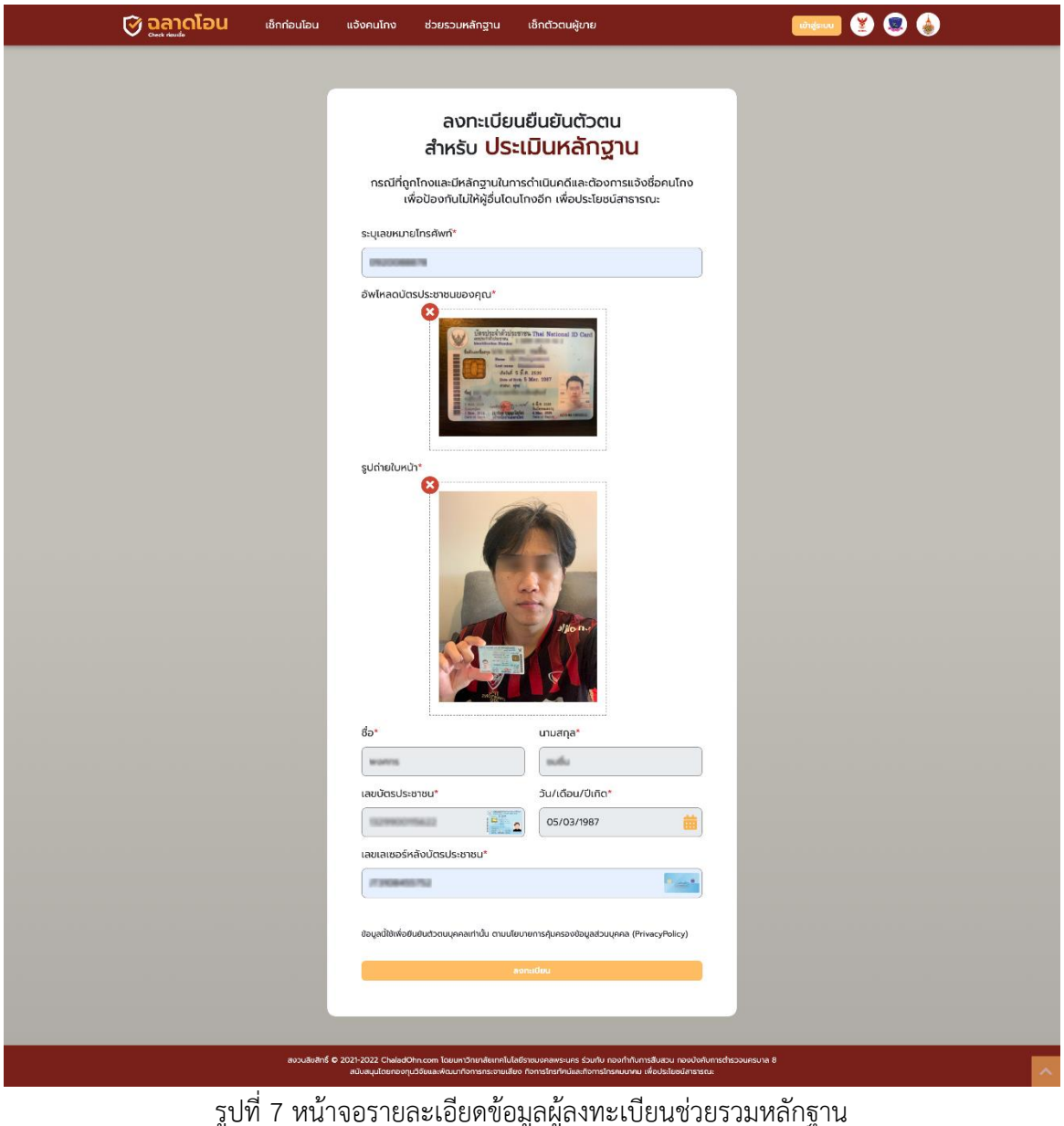
รูปที่ 5 ขั้นตอนการเข้าเมนูแจ้งคนโกงหน้าจอเว็บไซต์หน้าหลัก

จากนั้น คลิกที่ปุ่ม “ลงทะเบียน” เพื่อลงทะเบียนยืนยันตัวตน



รูปที่ 6 หน้าจอลงทะเบียนยืนยันตัวตนสำหรับช่วยรวมหลักฐาน

ให้ผู้ใช้งาน กรอกเลขหมายโทรศัพท์ อัปโหลดบัตรประจำตัวประชาชน และรูปถ่ายใบหน้าลงในระบบ แสดงดัง จากนั้นตรวจสอบความถูกต้องของข้อมูลและกดปุ่ม “ลงทะเบียน” แสดงดังรูปที่ 7

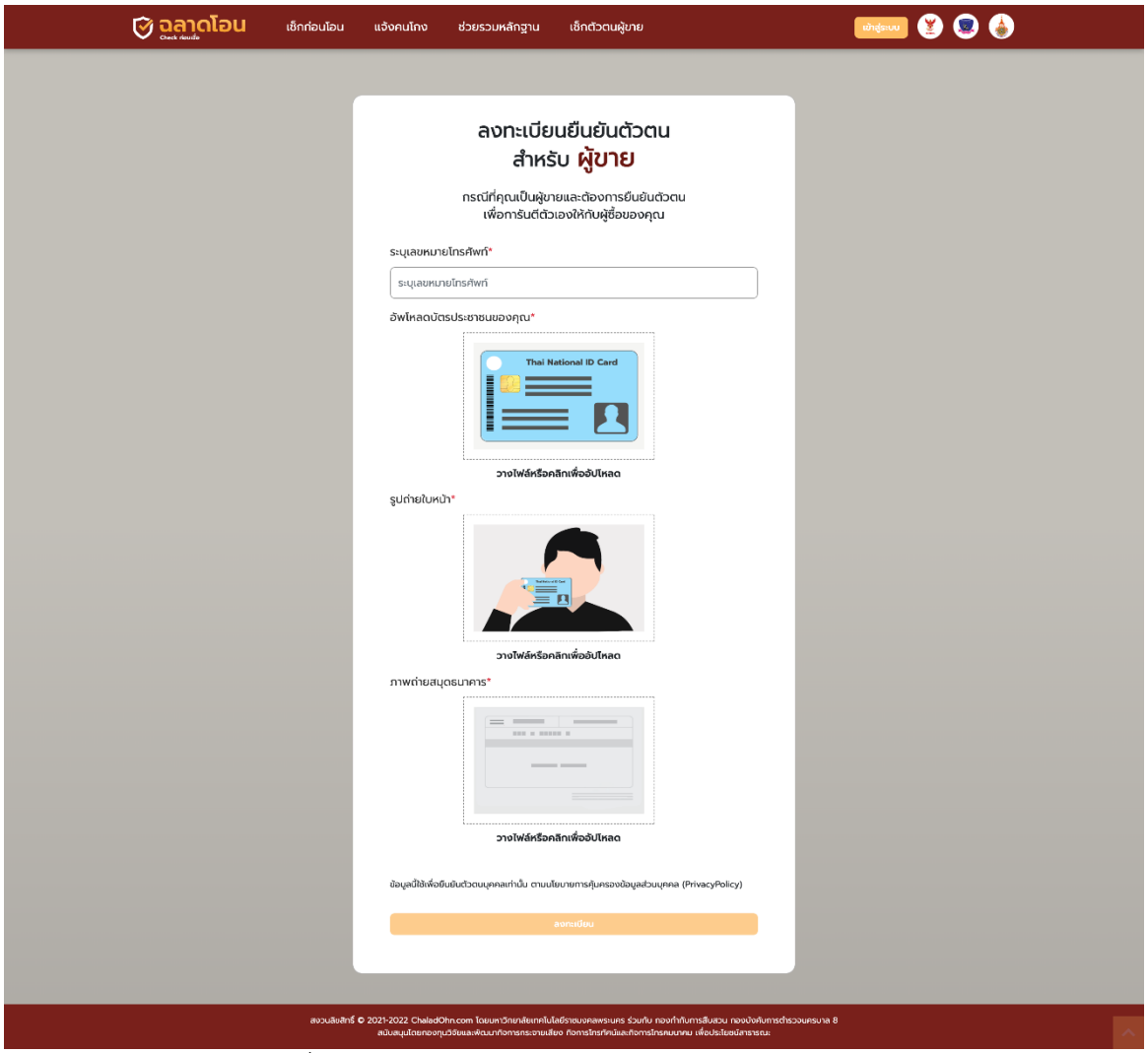


รูปที่ 7 หน้าจอรายละเอียดข้อมูลผู้ลงทะเบียนช่วยรวมหลักฐาน

1.1.3 ลงทะเบียนเพื่อสมัครเป็นผู้ขาย

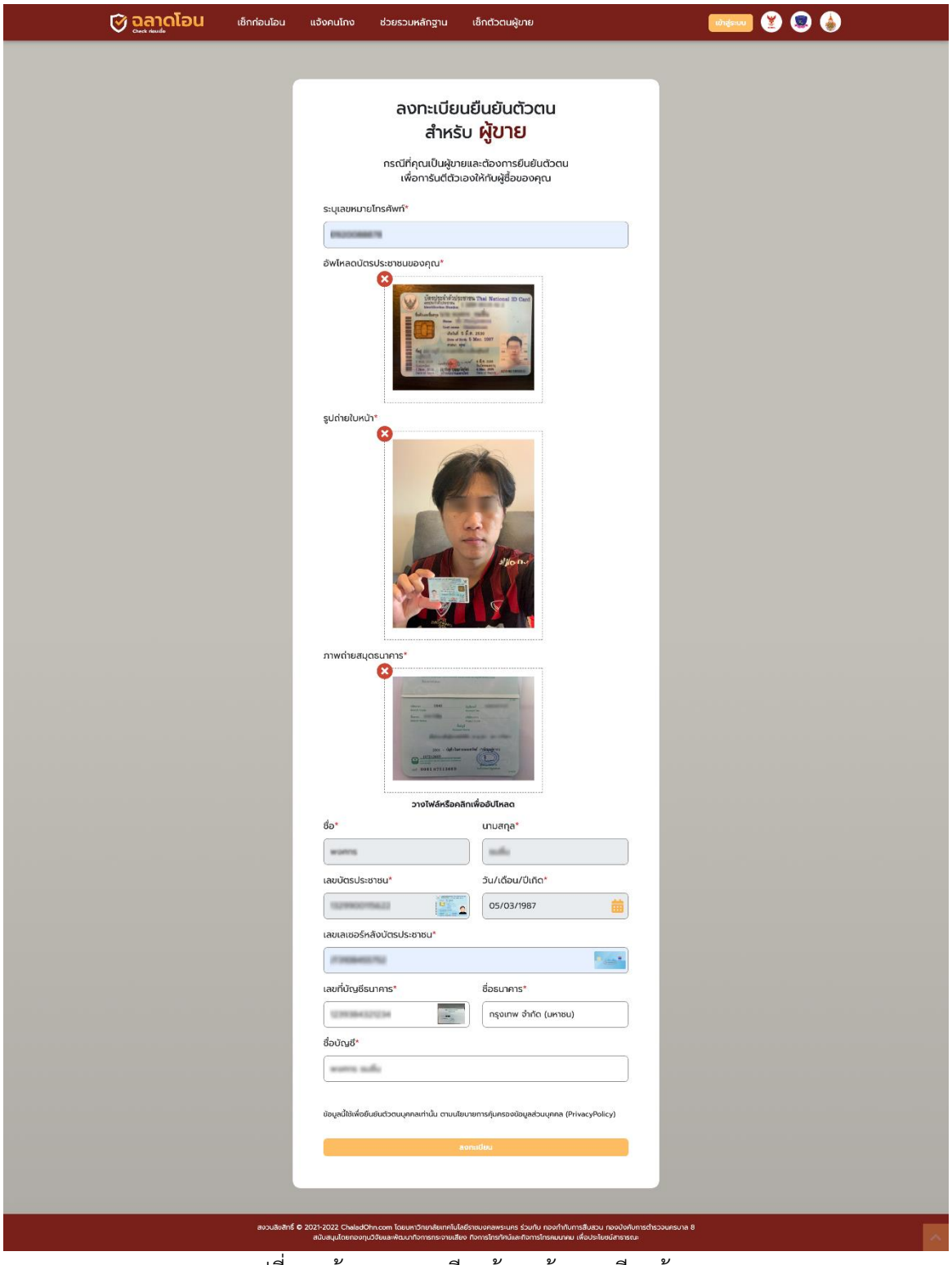
การลงทะเบียนเพื่อสมัครเป็นผู้ขาย สามารถกระทำได้ 2 วิธี ดังนี้

(1) ขอลิงก์ลงทะเบียนจากเจ้าหน้าที่ฉลาดโอน ผ่านช่องทาง LINE Official Account ฉลาดโอน.com แสดงดังรูปที่ 8



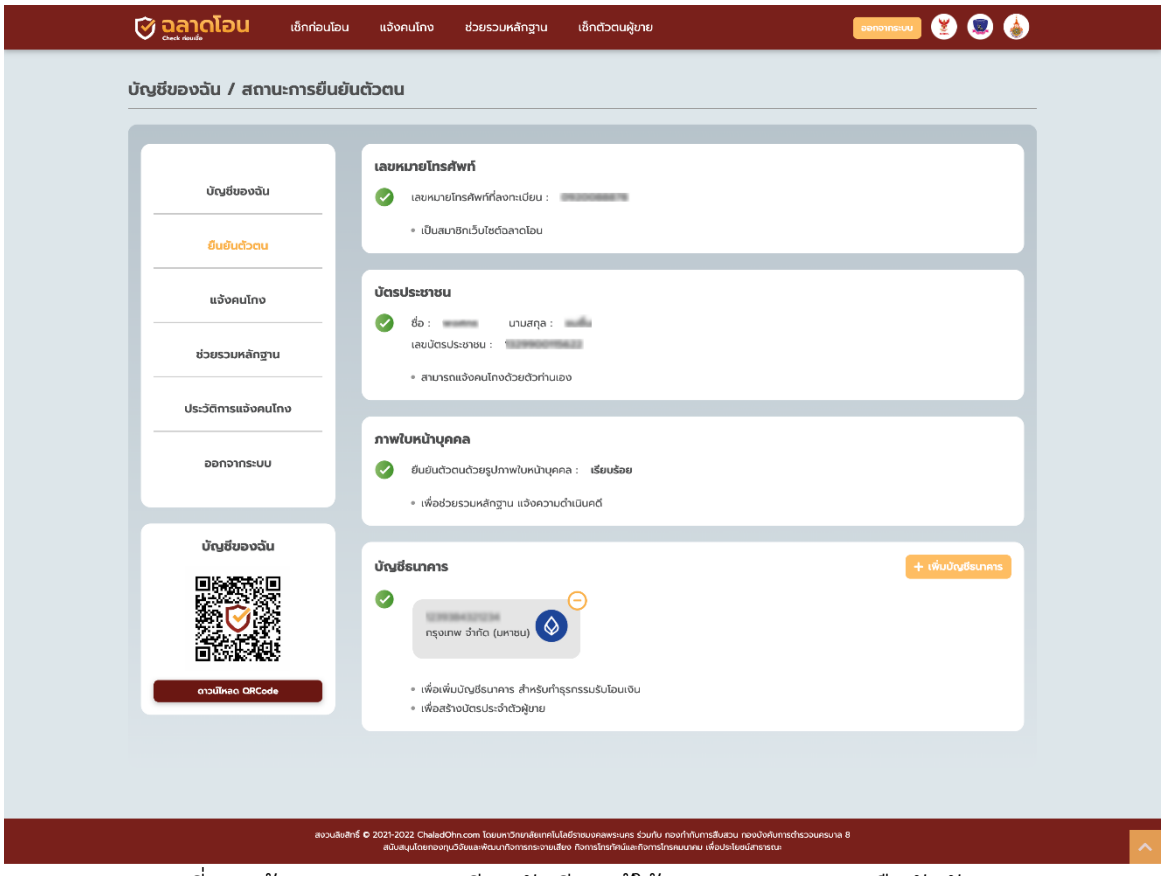
รูปที่ 8 หน้าจอลงทะเบียนยืนยันตัวตนสำหรับสมัครผู้ขาย

จากนั้นให้ผู้ใช้งาน กรอกเลขหมายโทรศัพท์ อัปโหลดบัตรประจำตัวประชาชน รูปถ่ายใบหน้า และภาพถ่ายสมุดบัญชีธนาคารลงในระบบ แสดงดังรูปที่ 9



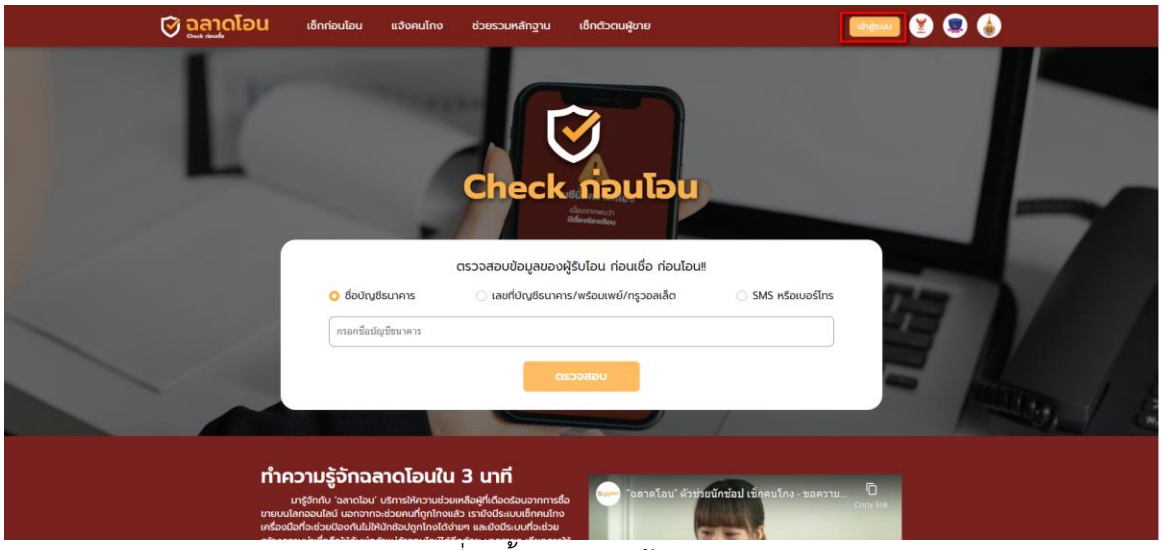
รูปที่ 7 หน้าจอรายละเอียดข้อมูลผู้ลงทะเบียนผู้ขาย

(2) สามารถลงทะเบียนแจ้งคนโกง หรือช่วยรวมหลักฐาน แล้วหน้าบัญชีของฉัน จากนั้นกดเข้าเมนู “ยืนยันตัวตน” และอัปโหลดสมุดบัญชีเพิ่มเติม แสดงดังรูปที่ 8



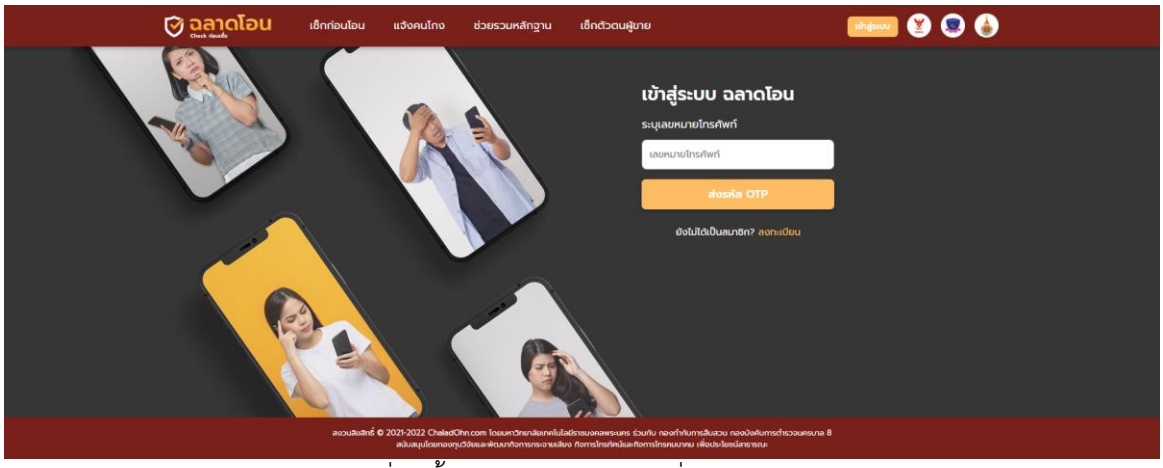
รูปที่ 8 หน้าจอแสดงรายละเอียดบัญชีของผู้ใช้งานและสถานะการยืนยันตัวตน

1.2 การเข้าสู่ระบบสำหรับผู้ที่มีบัญชีอยู่แล้ว
สำหรับผู้ใช้งานที่มีบัญชีอยู่แล้วสามารถคลิกเลือกเมนู “เข้าสู่ระบบ” แสดงดังรูปที่ 9



รูปที่ 9 ขั้นตอนการเข้าสู่ระบบ

ให้ผู้ใช้งานกรอกเลขหมายโทรศัพท์ จากนั้นกดปุ่ม “ส่งรหัส OTP” แสดงดังรูปที่ 10

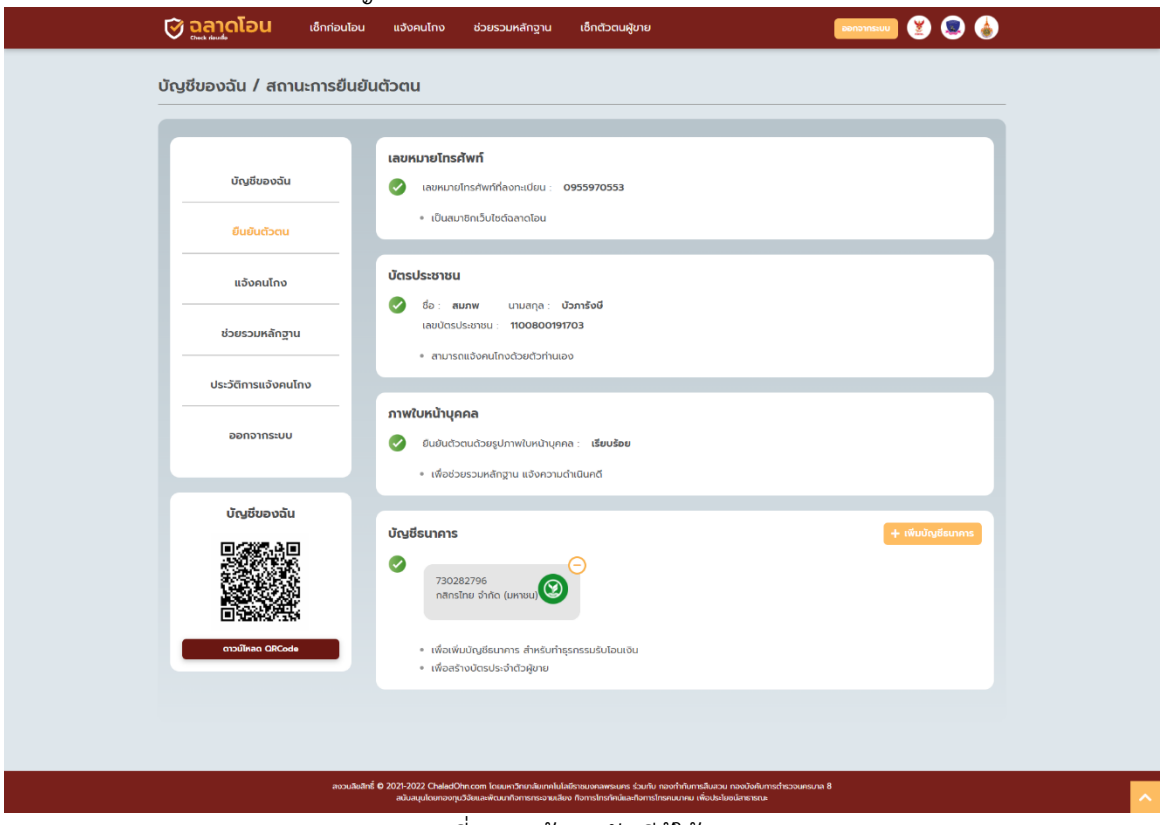


รูปที่ 9 ขั้นตอนการส่ง OTP เพื่อเข้าสู่ระบบ

กรอกเลข OTP ที่ได้รับผ่านเลขหมายโทรศัพท์ที่กรอกไว้ ลงในหน้าจอ จากนั้นกดปุ่ม “เข้าสู่ระบบ”

รูปที่ 10 ขั้นตอนการกรอก OTP เพื่อเข้าสู่ระบบ

จากนั้นจะพบกับหน้าบัญชีของฉัน



รูปที่ 10 หน้าจอบัญชีผู้ใช้งาน

1.3 บัญชีของฉัน

หน้าบัญชีของฉัน ประกอบด้วย หน้าหลัก “บัญชีของฉัน” ประกอบไปด้วยข้อมูลการยืนยันตัวตน เมนูการแจ้งคนโกง เมนูช่วยรวมหลักฐาน เมนูประวัติการแจ้งคนโกง เมนูออกจากระบบ และการดาวน์โหลดคิวอาร์โค้ดของบัญชีผู้ใช้งาน สามารถแสดงรายลเอียดแต่ละเมนูได้ดังนี้

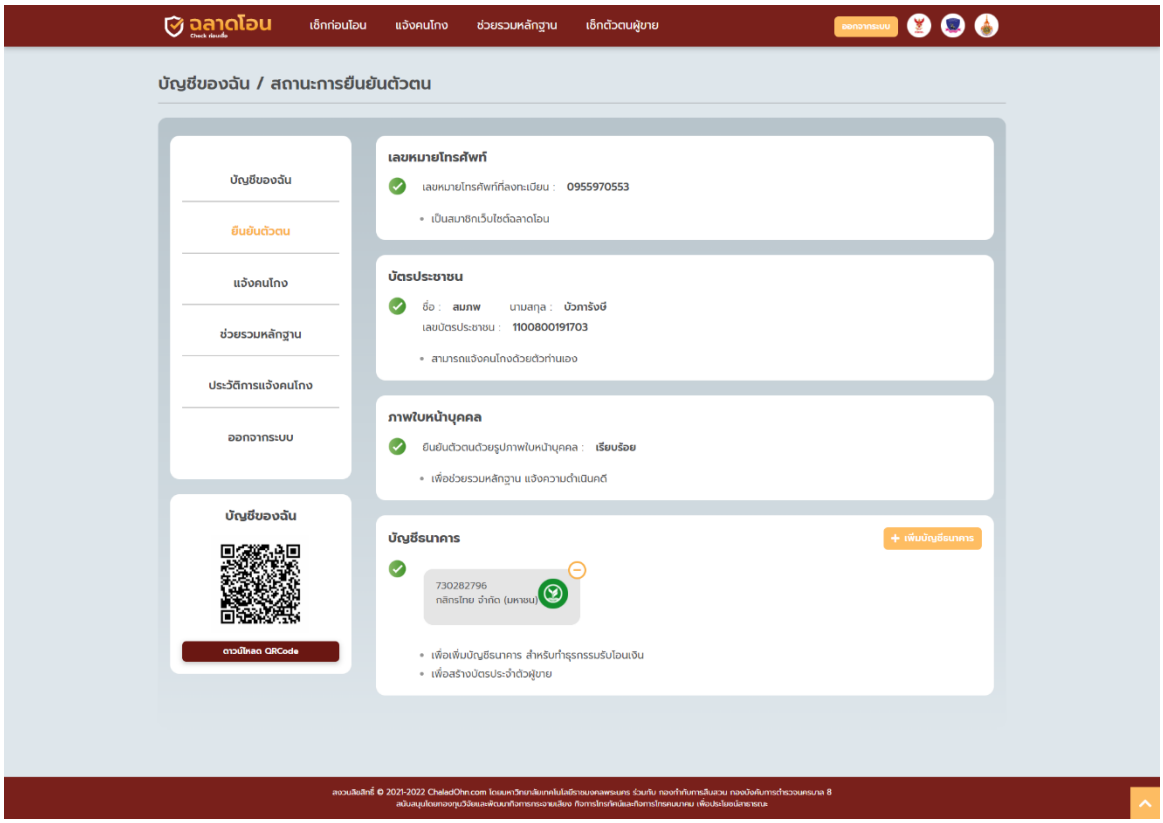
(1) เมนูบัญชีของฉัน

เมนูนี้จะแสดงบัตรประจำตัวอิเล็กทรอนิกส์ของผู้ใช้งาน ประกอบด้วย ชื่อ-นามสกุล ของผู้ใช้งาน รหัสไอดีของผู้ใช้งาน ช่วงเวลาที่เริ่มเป็นสมาชิกกับฉลาดโอน และคิวอาร์โค้ดสำหรับส่งต่อให้ผู้ซื้อ แสดงดังรูปที่ 11

รูปที่ 11 ตัวอย่างบัตรประจำตัวอิเล็กทรอนิกส์ของผู้ใช้งาน

(2) เมนูยืนยันตัวตน

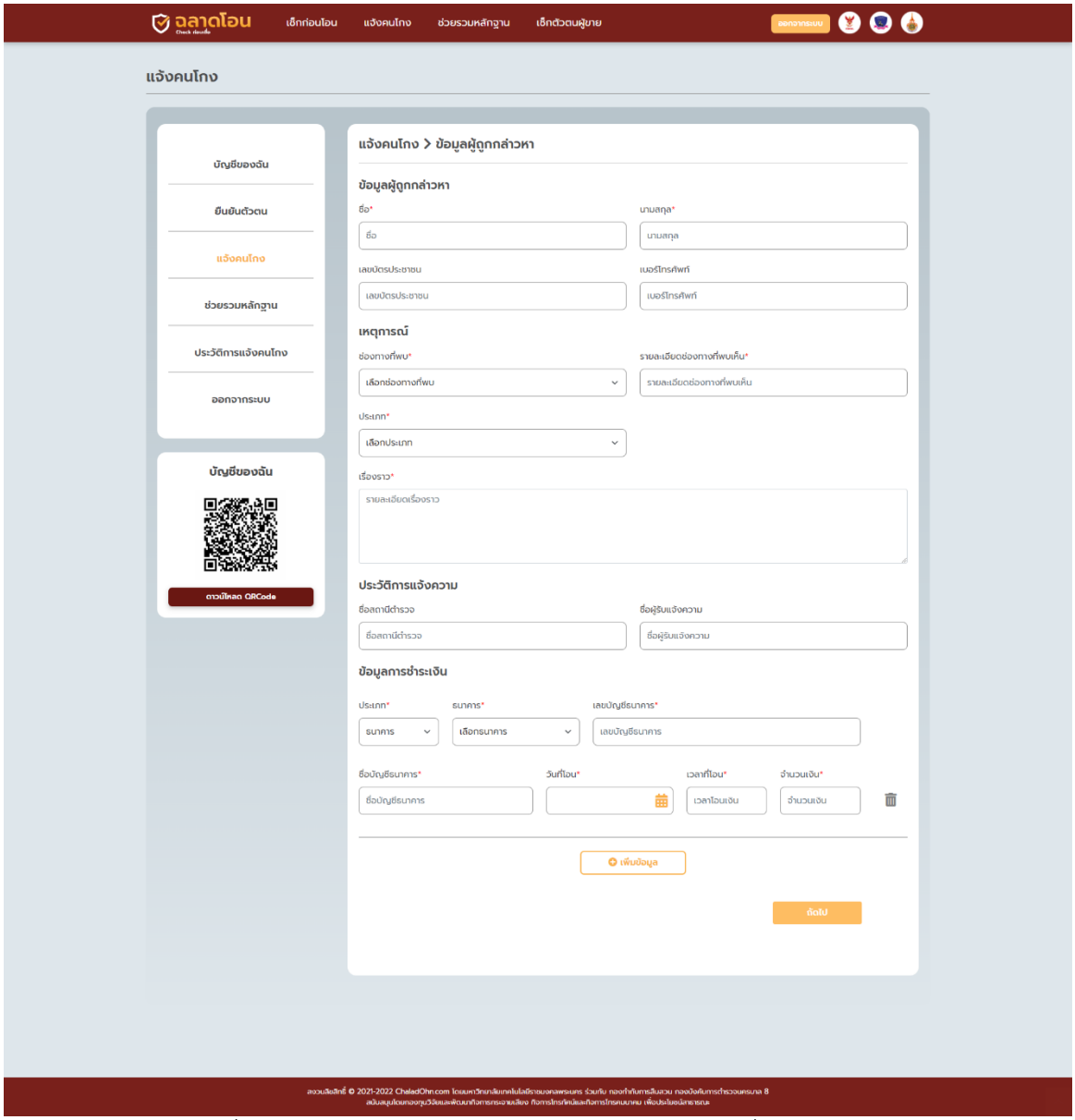
เมนูนี้จะแสดงสถานะการยืนยันตัวตนของผู้ใช้งาน และสิทธิ์ในการเข้าใช้งานระบบฉลาดโอน แสดงดังรูปที่ 12



รูปที่ 12 หน้าจอแสดงสถานะการยืนยันตัวตน

(3) เมนูแจ้งคนโกง

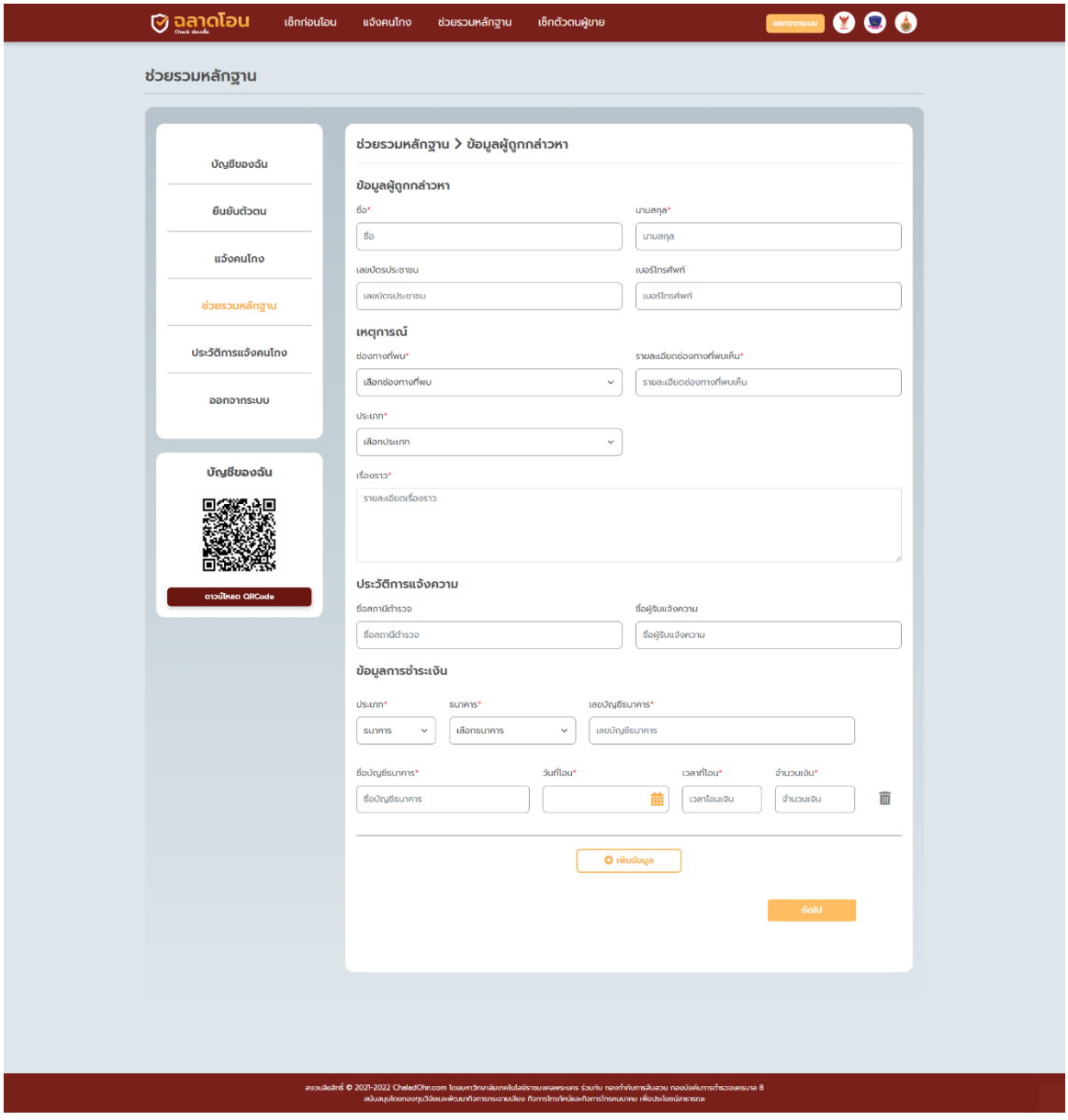
เมนูนี้มีไว้เพื่อแจ้งรายชื่อคนโกงให้กับระบบฉลาดโอน โดยผู้ใช้งานจะต้องกรอกชื่อ-นามสกุลของผู้ถูกกล่าวหา ช่องทางที่พบเห็น รายละเอียดช่องทางที่พบเห็น ประเภทการถูกโกง ลำดับเหตุการณ์ที่เกิดขึ้น รวมถึงข้อมูลการชำระเงิน รูปภาพสลิปการโอนเงิน รวมถึงแชทการสนทนาระหว่างผู้เสียหายกับผู้ถูกกล่าวหา แสดงดังรูปที่ 13



รูปที่ 13 หน้าจอแสดงรายละเอียดสำหรับกรอกข้อมูลเพื่อแจ้งคนโกง

(4) เมนูช่วยรวมหลักฐาน

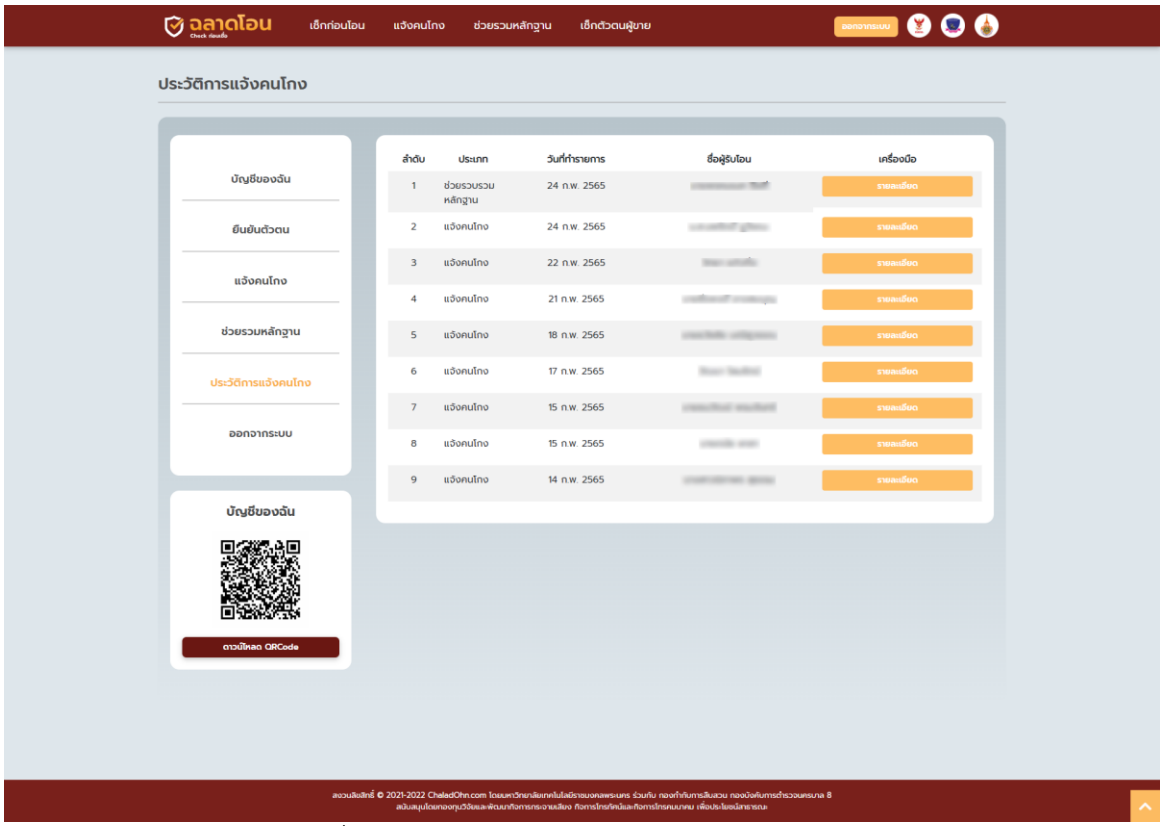
เมนูนี้มีไว้สำหรับให้ฉลาดโอนช่วยรวมหลักฐาน เพื่อใช้ประกอบการแจ้งความกับเจ้าหน้าที่ตำรวจที่สถานีตำรวจ เพื่อดำเนินคดี โดยผู้ใช้งานจะต้องกรอกรายละเอียดเช่นเดียวกันกับส่วนของการแจ้งคนโกง แต่ในส่วนของเมนูนี้ ผู้ใช้สามารถสั่งพิมพ์เอกสารเพื่อใช้เป็นหลักฐานประกอบการแจ้งความเพื่อดำเนินได้



รูปที่ 14 หน้าจอแสดงรายละเอียดสำหรับกรอกข้อมูลช่วยรวมหลักฐาน

(5) เมนูประวัติการแจ้งคนโกง

เมนูนี้จะแสดงรายชื่อที่ผู้ใช้งานมีการแจ้งไว้กับเว็บฉลาดโอนทั้งหมด แสดงตามวันที่ทำรายการ โดยสามารถกดเข้าดูรายละเอียดของแต่ละเคสได้



รูปที่ 15 หน้าจอแสดงรายการประวัติการแจ้งคนโกง

(6) เมนูออกจากระบบ

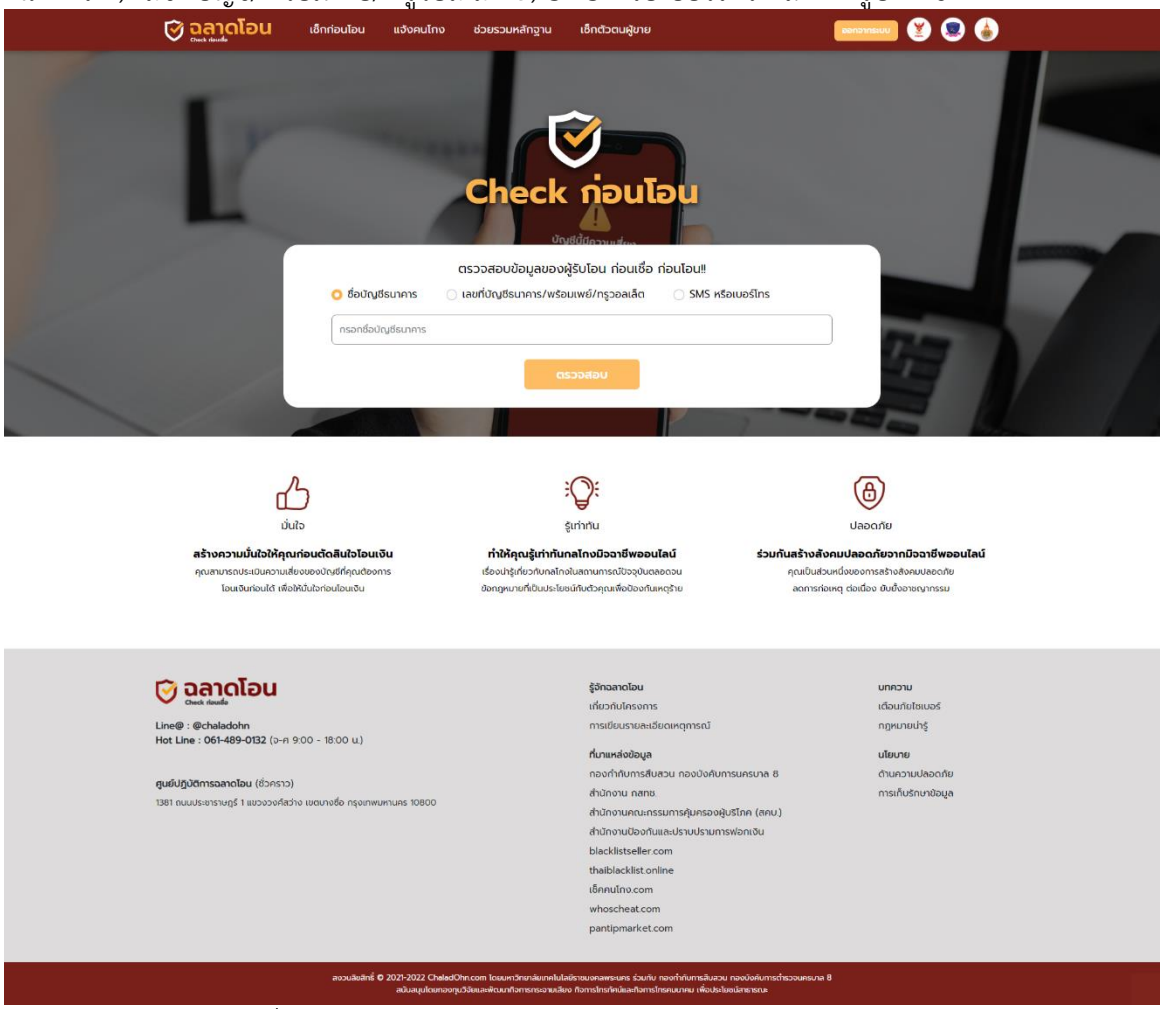
ผู้ใช้งานสามารถกดปุ่มเพื่อออกจากระบบได้

(7) ดาวน์โหลด QR Code

ผู้ใช้งานสามารถกดปุ่มสำหรับดาวน์โหลด QR Code ได้ เพื่อนำไปส่งต่อให้กับผู้อื่น กรณีที่ผู้ใช้งานสมัครเป็นผู้ขายเรียบร้อยแล้ว

2. เช็กก่อนโอน

ขั้นตอนสำหรับการตรวจสอบรายชื่อคนโกงสามารถคลิกที่เมนู “เช็กก่อนโอน” จากนั้นจะแสดงหน้าจอ Check ก่อนโอน โดยผู้ใช้งานสามารถตรวจสอบรายชื่อได้จาก 3 ช่องทางได้แก่ 1) ชื่อบัญชีธนาคาร 2) เลขที่บัญชี/พร้อมเพย์/ทรูวอลเล็ต 3) SMS หรือเบอร์โทร แสดงดังรูปที่ 16

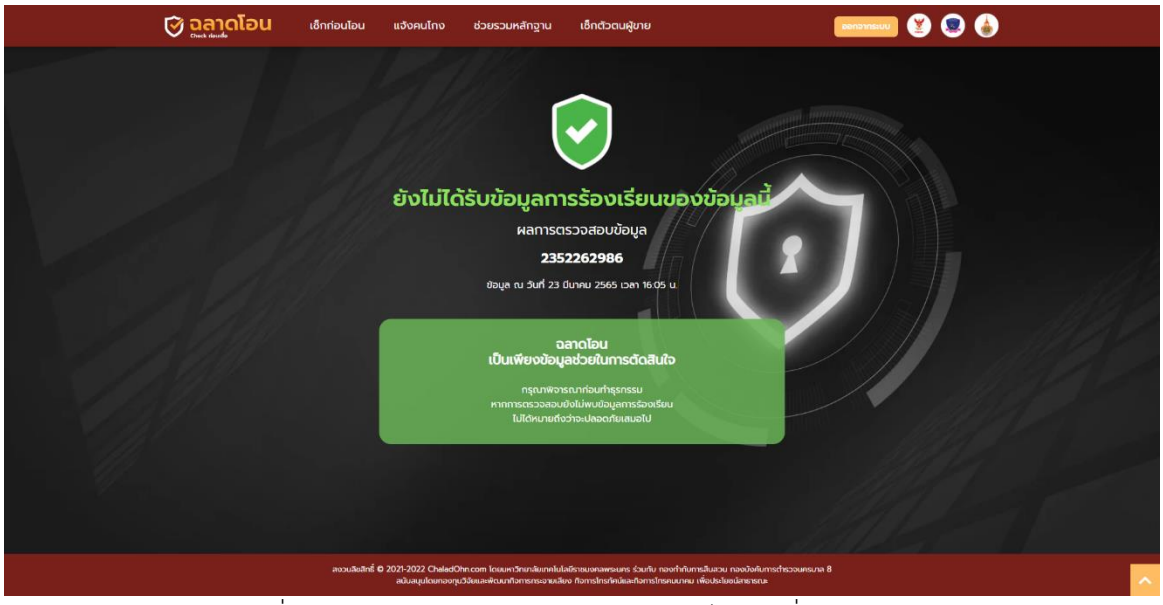


รูปที่ 16 หน้าจอเว็บไซต์หน้าหลักสำหรับเมนูในส่วนเช็กก่อนโอน

ในส่วนของการแสดงผลการตรวจสอบ แบ่งออกเป็น 2 รูปแบบ ดังนี้

(1) ไม่พบเรื่องร้องเรียน

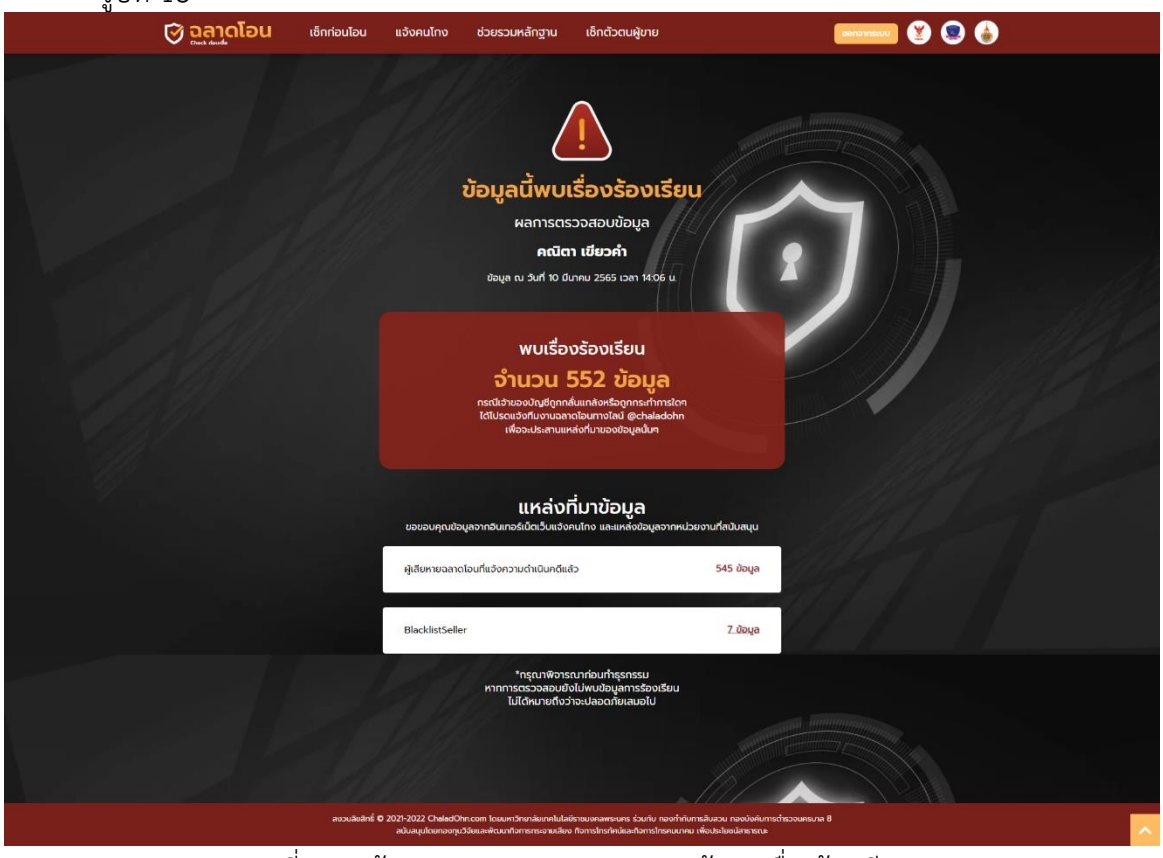
กรณีที่ผู้ใช้ตรวจสอบรายชื่อของคนโกงกับเว็บฉลาดโอนแล้วไม่พบ ระบบจะแสดงหน้าจอ แสดงดังรูปที่ 17



รูปที่ 17 หน้าจอแสดงผลการตรวจสอบแล้วไม่พบเรื่องร้องเรียน

(2) พบเรื่องร้องเรียน

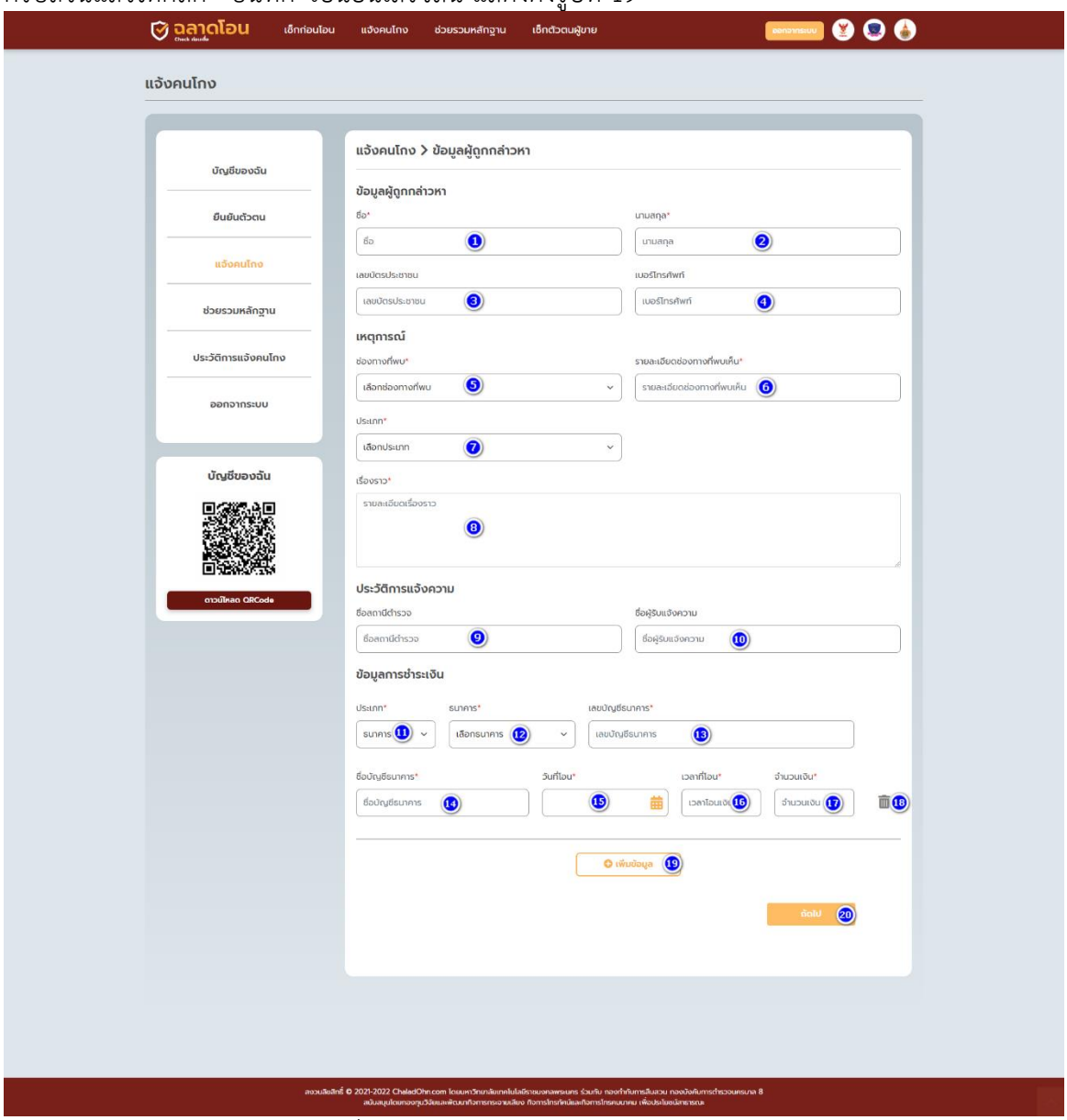
กรณีที่ผู้ใช้ตรวจสอบรายชื่อของคนโกงกับเว็บฉลาดโอนแล้วพบ ระบบจะแสดงหน้าจอ แสดงดังรูปที่ 18



รูปที่ 18 หน้าจอแสดงผลการตรวจสอบแล้วพบเรื่องร้องเรียน

3. แจ้งคนโกง

ขั้นตอนสำหรับการแจ้งคนโกงสามารถคลิกที่เมนู “แจ้งคนโกง” จากนั้นจะเข้าสู่หน้าจอการแจ้งข้อมูลผู้ถูกกล่าวหา ในการกรอกข้อมูลรายละเอียดต่างๆ ข้อมูลที่แสดงสัญลักษณ์ (*) จำเป็นจะต้องใส่ข้อมูลให้ครบถ้วนและถูกต้องและหากต้องการเพิ่มผู้ถูกกล่าวหาให้คลิกปุ่ม “เพิ่มข้อมูล” หากกรอกข้อมูลครบถ้วนแล้วให้คลิก “บันทึก”เป็นอันเสร็จสิ้น แสดงดังรูปที่ 19

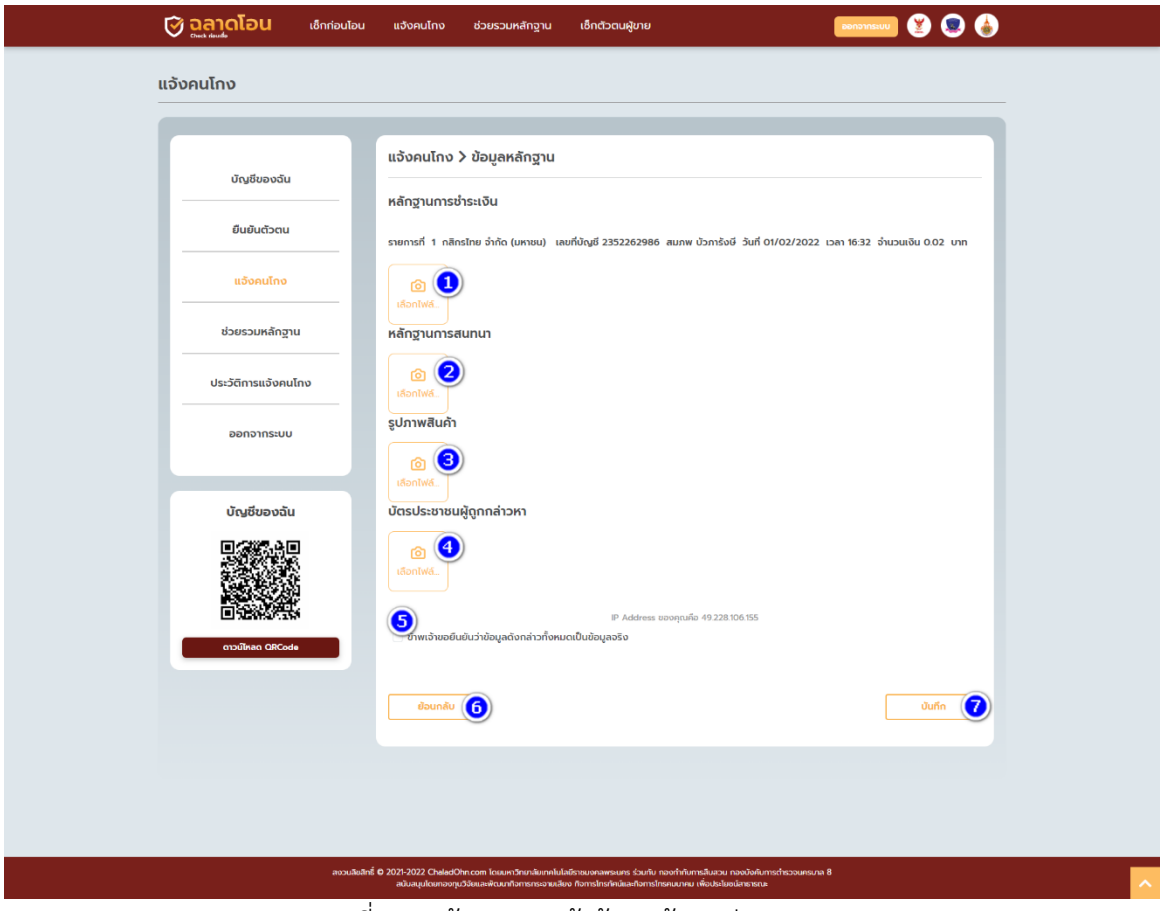


รูปที่ 19 หน้าจอการแจ้งข้อมูลผู้ถูกกล่าวหา

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	สำหรับระบุชื่อของผู้ถูกกล่าวหา	Yes	Text	
2	สำหรับระบุนามสกุลผู้ถูกกล่าวหา	Yes	Text	
3	หมายเลขบัตรประจำตัวประชาชนของผู้ถูกกล่าวหา		Numeric	
4	หมายเลขเบอร์โทรศัพท์ของผู้ถูกกล่าวหา		Numeric	
5	เลือกช่องทางที่พบเจอผู้ถูกกล่าวหา	Yes	Select	
6	กรอกรายละเอียดของช่องทางที่พบเจอผู้ถูกกล่าวหา	Yes	Text	
7	เลือกรูปแบบของการถูกโกง	Yes	Select	
8	กรอกเรื่องราวระหว่างตัวเองกับผู้ถูกกล่าวหา	Yes	Textarea	
9	กรอกชื่อสถานีตำรวจ	No	Text	
10	กรอกชื่อผู้รับแจ้งความ	No	Text	
11	เลือกประเภทของข้อมูลการชำระเงินของผู้ถูกกล่าวหา	Yes	Select	
12	เลือกธนาคารของผู้ถูกกล่าวหา	Yes	Select	
13	กรอกหมายเลขบัญชีธนาคารของผู้ถูกกล่าวหา	Yes	Numeric	
14	กรอกชื่อบัญชีธนาคารของผู้ถูกกล่าวหา	Yes	Text	
15	เลือกวันที่ ที่ทำ	Yes	Date	

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
	รายการโอน			
16	เลือกเวลา ที่ทำรายการโอน	Yes	Time	
17	กรอกจำนวนเงินที่ทำให้การโอนให้กับผู้ถูกกล่าวหา	Yes	Numeric	
18	กดเพื่อทำการลบข้อมูลเกี่ยวกับการชำระเงิน		Button	
19	กดเพื่อเพิ่มข้อมูลเกี่ยวกับการชำระเงิน		Button	
20	กดเพื่อไปยังหน้าเพิ่มข้อมูลหลักฐาน	Yes	Button	กดปุ่มเพื่อเข้าสู่ขั้นตอนต่อไป

จากนั้นจะเป็นส่วนของการแนบเอกสารที่เกี่ยวข้อง ประกอบไปด้วยหลักฐานการชำระเงิน หลักฐานการสนทนา รูปภาพสินค้า บัตรประชาชนผู้ถูกกล่าวหา โดยให้ผู้ใช้งานอัปโหลดเอกสารให้ได้มากที่สุด เพื่อให้เป็นข้อมูลที่เป็นประโยชน์ สำหรับการสืบสวนของเจ้าหน้าที่ตำรวจ แสดงดังรูปที่ 20



รูปที่ 20 หน้าจอการแจ้งข้อมูลผู้ถูกกล่าวหา (2)

ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
1	กดเพื่อทำการเพิ่มหลักฐานเกี่ยวกับการชำระเงิน		Image	
2	กดเพื่อทำการเพิ่มหลักฐานเกี่ยวกับการสนทนา		Image	
3	กดเพื่อทำการเพิ่มหลักฐานเกี่ยวกับรูปสินค้า		Image	
4	กดเพื่อทำการเพิ่มหลักฐานเกี่ยวกับบัตรประจำตัวประชาชนของผู้ถูกกล่าวหา		Image	
5	ลงชื่อยอมรับเงื่อนไข	Yes	Text	

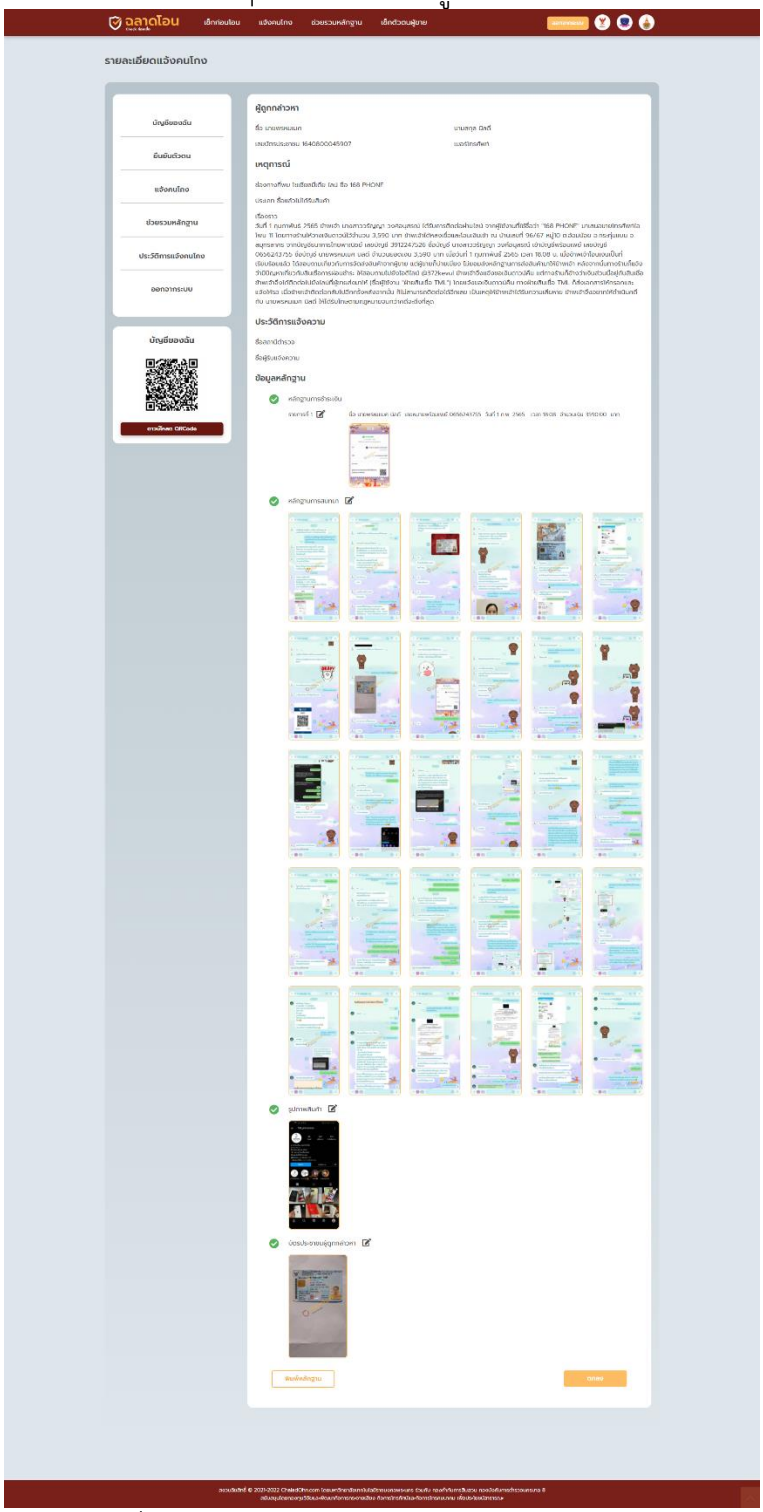
ลำดับ	รายละเอียด	บังคับ	ประเภท	ข้อกำหนด / กระบวนการทำงาน
	และข้อตกลงเพื่อทำการแจ้งคนโกง			
6	กดเพื่อย้อนกลับไปแก้ไขข้อมูลในหน้าแรก		Button	ย้อนกลับไปหน้าแรกเพื่อทำการดูหรือแก้ไขข้อมูลของผู้ถูกกล่าวหา
7	กดเพื่อทำการบันทึกข้อมูลการแจ้งคนโกง	Yes	Button	บันทึกข้อมูลการแจ้งคนโกงเสร็จสิ้น

เมื่อกดปุ่มบันทึก ระบบจะบันทึกข้อมูลทั้งหมด จากนั้นจะแสดงหน้าจอสรุปรายละเอียดทั้งหมดให้ผู้ใช้งานตรวจสอบอีกครั้ง สำหรับผู้ใช้งานที่ต้องการอัปโหลดหลักฐานเพิ่มเติม สามารถกดเพิ่มได้จากหน้าจอนี้ ในส่วนของเหตุการณ์ ผู้ใช้งานจะไม่สามารถแก้ไขได้เอง หากต้องการแก้ไข ให้ติดต่อเจ้าหน้าที่ฉลาดโอนผ่านช่องทาง ช่องทาง Line Official ฉลาดโอน.com เพื่อให้เจ้าหน้าที่ปรับแก้ให้ แสดงรายละเอียดหน้าจอ ดังรูปที่ 21

รูปที่ 20 หน้าจอสรุปข้อมูลการแจ้งคนโกง

4. ช่วยรวมหลักฐาน

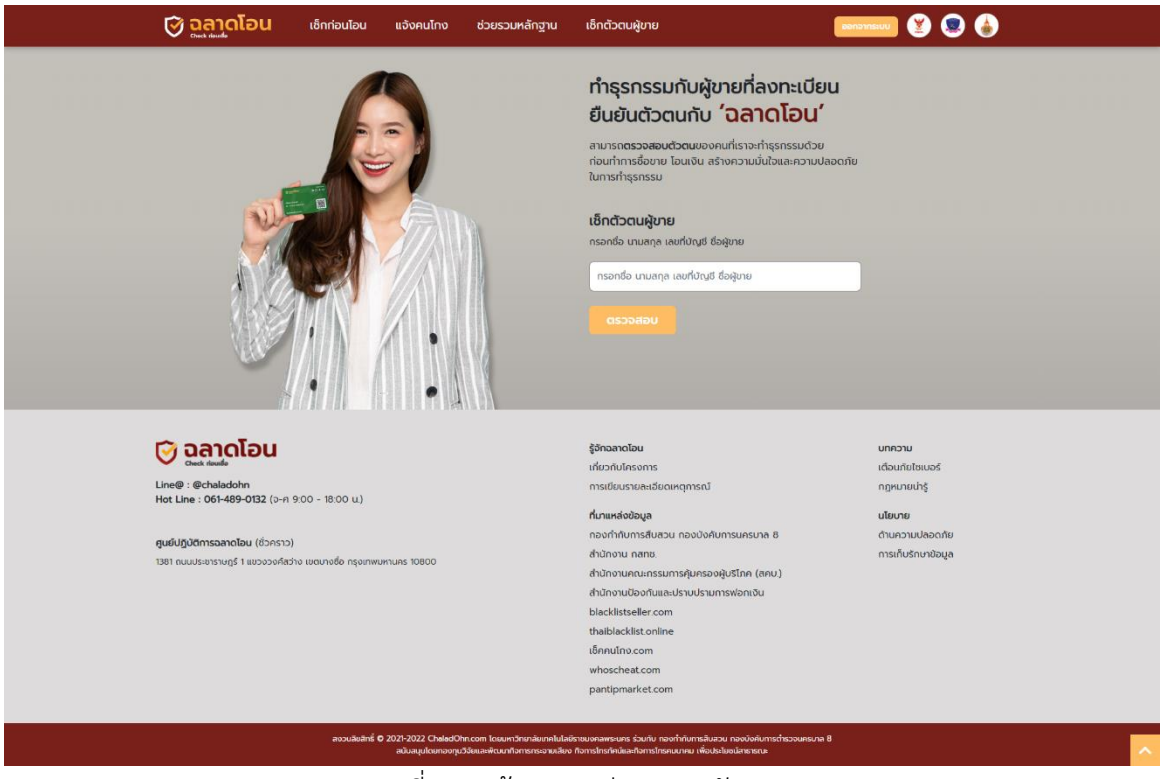
ในเมนูนี้ จะเป็นการให้ฉลาดโอนช่วยรวมหลักฐานให้ โดยให้ผู้ใช้งานกดเข้าเมนู “ช่วยรวมหลักฐาน” จากนั้นให้กรอกรายละเอียดเช่นเดียวกับการแจ้งคนโกง เมื่อกดบันทึกในขั้นตอนสุดท้าย จะปรากฏหน้าจอแสดงปุ่มพิมพ์หลักฐาน ซึ่งมีไว้สำหรับให้ผู้ใช้งานสั่งพิมพ์เอกสารเพื่อนำไปประกอบการแจ้งความเพื่อดำเนินคดีกับมิจฉาชีพรายนั้น ๆ แสดงหน้าจอดังรูปที่ 21



รูปที่ 20 หน้าจอสรุปข้อมูลการช่วยรวมหลักฐาน

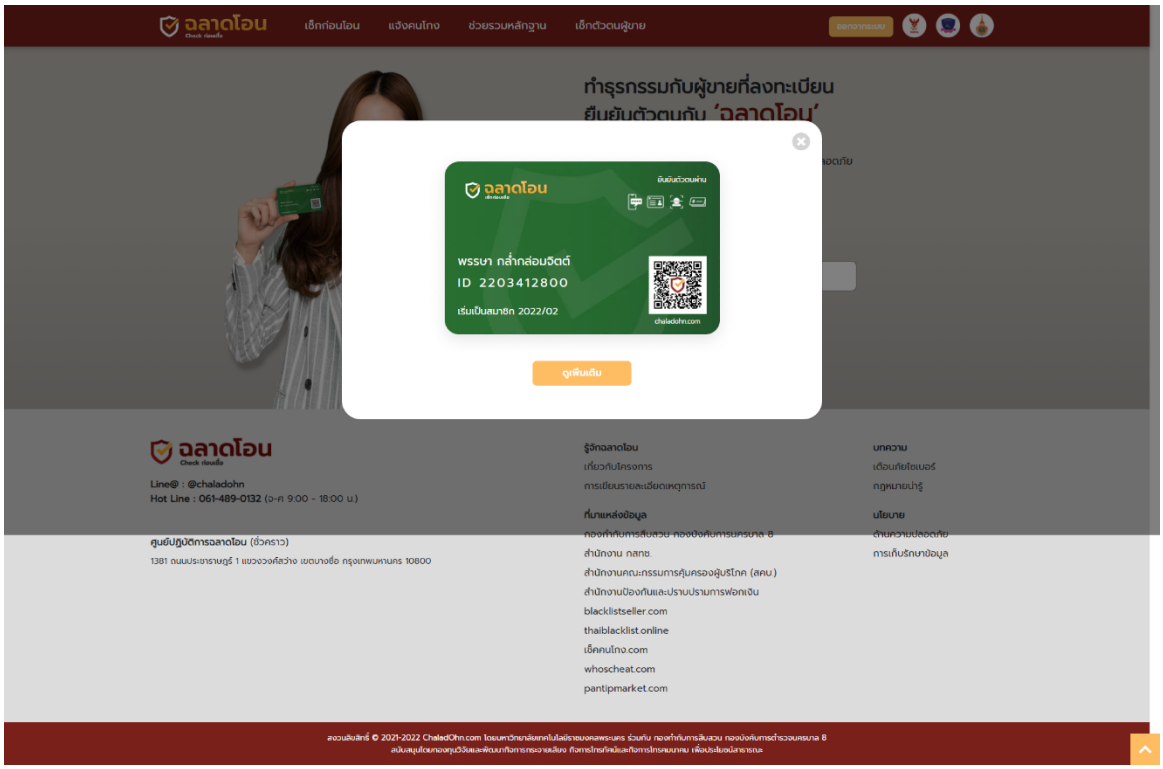
5. เช็กตัวตนผู้ขาย

เมนูนี้จะใช้สำหรับการเช็กตัวตนของผู้ขาย ว่าเคยมีการลงทะเบียนไว้กับเว็บฉลาดโอนแล้วหรือยัง โดยเมื่อผู้ใช้งานกดเข้ามาที่เมนู “เช็กตัวตนผู้ขาย” จะพบกับหน้าจอ แสดงดังรูปที่ 21



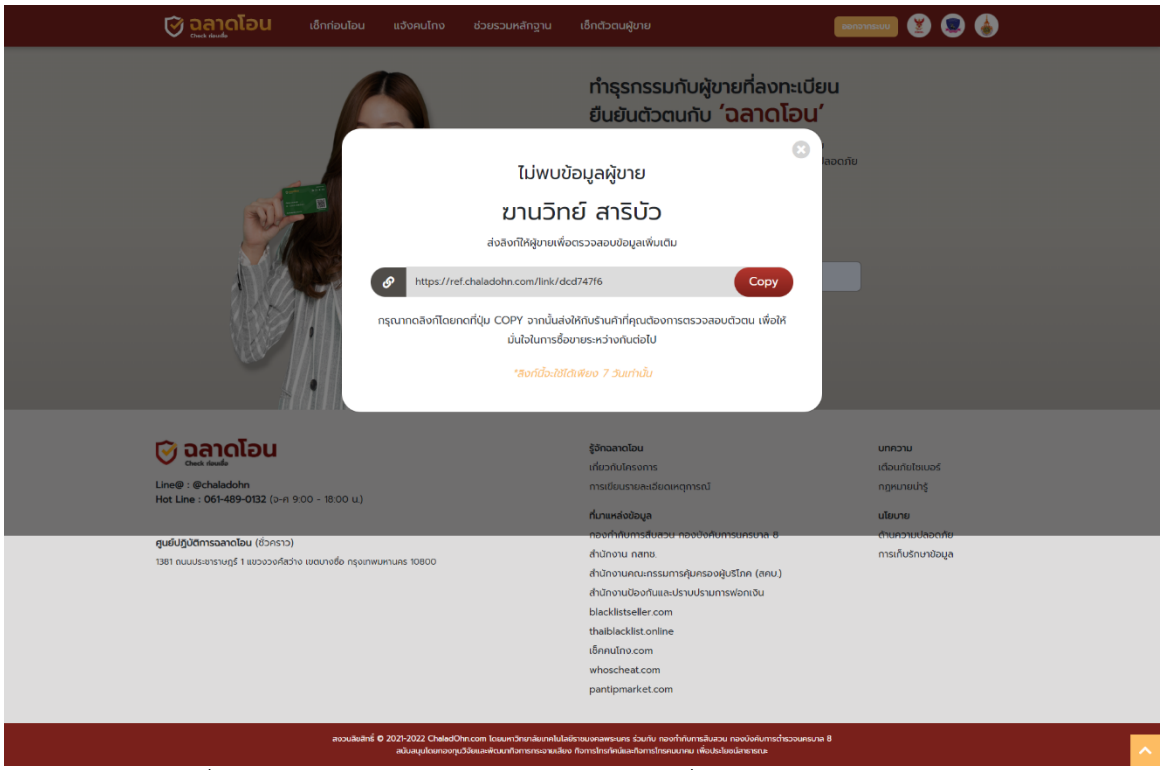
รูปที่ 20 หน้าจอเมนูช่วยรวมหลักฐาน

จากนั้นให้ผู้ใช้งานกรอกชื่อ นามสกุล ของผู้ขายที่เราต้องการตรวจสอบ หากผู้ขายที่เราตรวจสอบมีการลงทะเบียนกับเว็บไซต์ฉลาดโอนแล้ว ก็จะขึ้นรูปบัตรประจำตัวอิเล็กทรอนิกส์ แสดงดังรูปที่ 21



รูปที่ 21 หน้าจอแสดงบัตรประจำตัวอิเล็กทรอนิกส์

ในกรณีที่ไม่พบการลงทะเบียนของผู้ขายในระบบ ก็จะแสดงหน้าจอว่า “ไม่พบข้อมูลผู้ขาย” แสดงดังรูปที่ 22



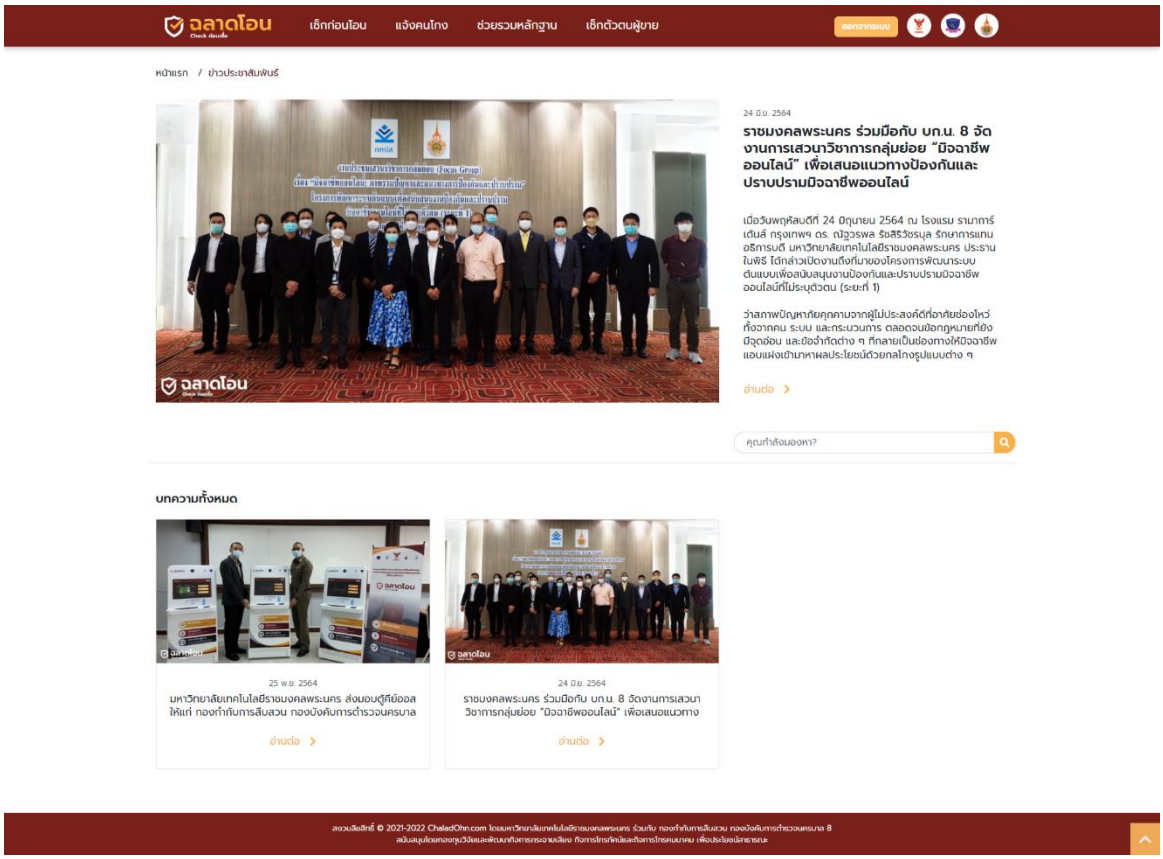
รูปที่ 21 หน้าจอแสดงข้อความ “ไม่พบผู้ขาย” ที่ลงทะเบียนกับเว็บฉลาดโอน

6. ลิงก์อื่น ๆ ของเว็บไซต์ฉลาดโอน

นอกจากเมนูหลักที่เป็นฟังก์ชันสำหรับผู้ใช้งานแล้ว บนหน้าเว็บไซต์ฉลาดโอน ยังมีลิงก์อื่น ๆ ที่เกี่ยวข้อง ที่เป็นประโยชน์กับผู้ใช้งาน เช่น ข่าวประชาสัมพันธ์ ข่าวปราบปรามมิจฉาชีพ เกี่ยวกับโครงการ เป็นต้น โดยแต่ละลิงก์มีรายละเอียดดังนี้

6.1 ข่าวประชาสัมพันธ์

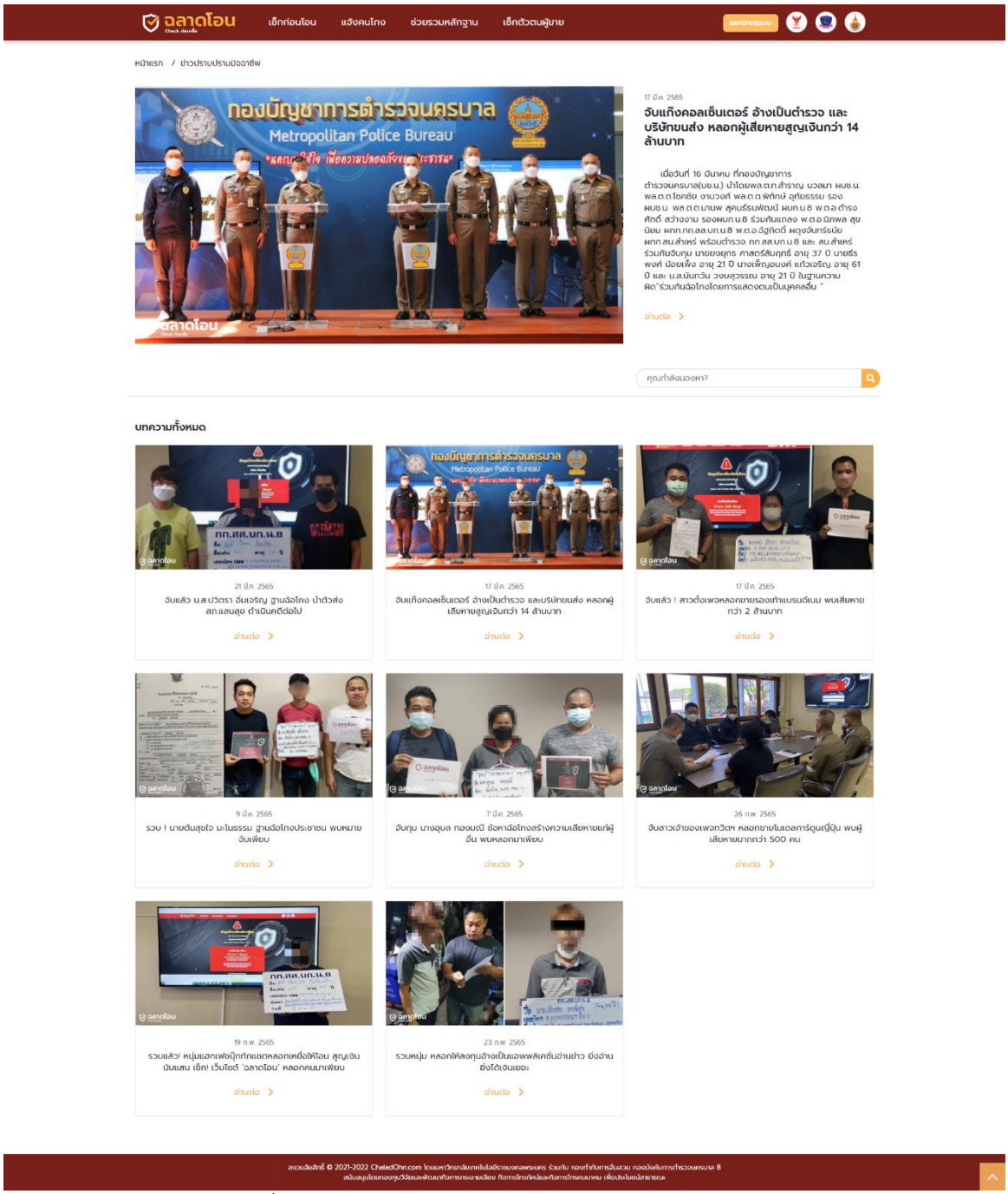
หน้าข่าวประชาสัมพันธ์ จะพูดถึงการประชุมของโครงการฉลาดโอนกับหน่วยงานอื่น ๆ ที่เกี่ยวข้อง รวมถึงกิจกรรมต่าง ๆ ที่เกิดขึ้นของโครงการ แสดงดังรูปที่ 22



รูปที่ 22 หน้าจอแสดงข้อมูลหน้าข่าวประชาสัมพันธ์

6.2 ข่าวปราบปรามมิจฉาชีพ

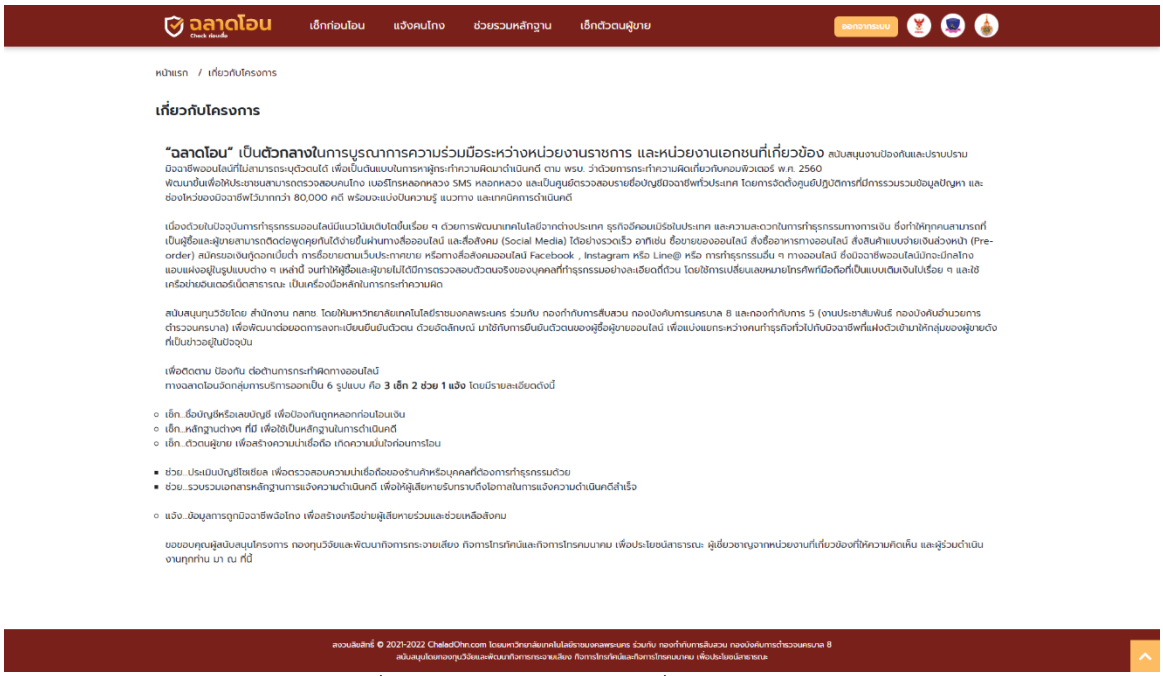
หน้าข่าวปราบปรามมิจฉาชีพ ใช้สำหรับแจ้งข้อมูลข่าวสารการเข้าจับกุมมิจฉาชีพที่มีการใช้ข้อมูลจากเว็บไซต์ฉลาดโอนประกอบการสืบสวน เพื่อเป็นสื่อกลางในการเผยแพร่ข้อมูล และมีเป้าประสงค์เพื่อให้บุคคลที่โดนหลอกแต่ละรายเข้าแจ้งความเพื่อเพิ่มผู้เสียหายร่วม แสดงดังรูปที่ 23



รูปที่ 23 หน้าจอแสดงข้อมูลหน้าข่าวปราบปรามมิจฉาชีพ

6.3 เกี่ยวกับโครงการ

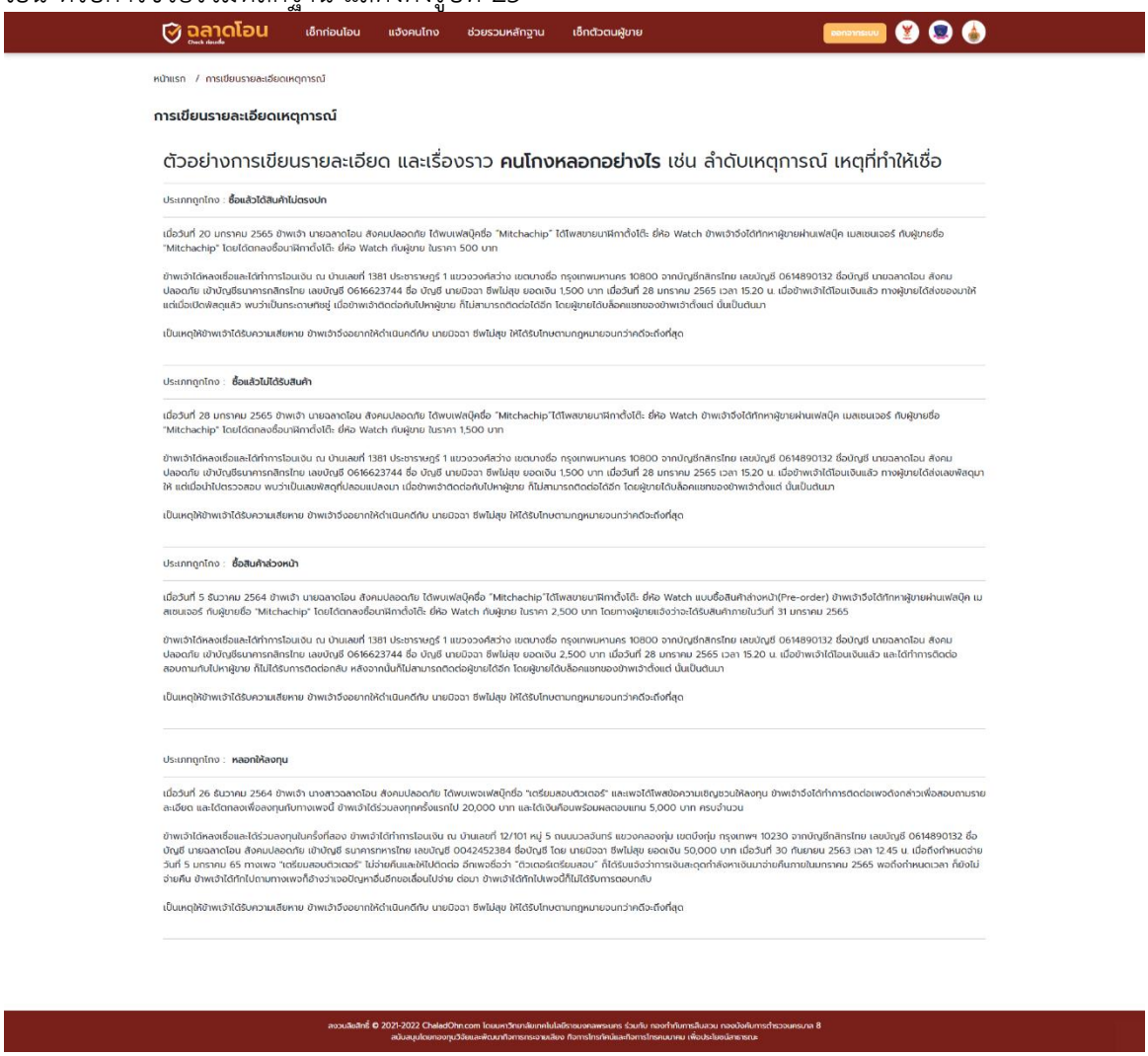
หน้าเกี่ยวกับโครงการ จะกล่าวถึงที่มาของโครงการ วัตถุประสงค์ของเว็บไซต์ การให้บริการของฉลาดโอน ความร่วมมือระหว่างหน่วยงานต่าง ๆ แสดงดังรูปที่ 24



รูปที่ 24 หน้าจอแสดงข้อมูลเกี่ยวกับโครงการ

6.4 การเขียนรายละเอียดเหตุการณ์

หน้าการเขียนรายละเอียดเหตุการณ์ จะแสดงตัวอย่างการเขียนเรื่องราวที่ผู้เสียหายโดยมิจฉาชีพหลอก เพื่อให้ผู้ใช้งานใช้เป็นแนวทางในการเขียนเรื่องราวประกอบสำนวนการแจ้งคนโกงผ่านระบบฉลาดโอน หรือการช่วยรวมหลักฐาน แสดงดังรูปที่ 25



รูปที่ 25 หน้าจอแสดงข้อมูลการเขียนรายละเอียดเหตุการณ์

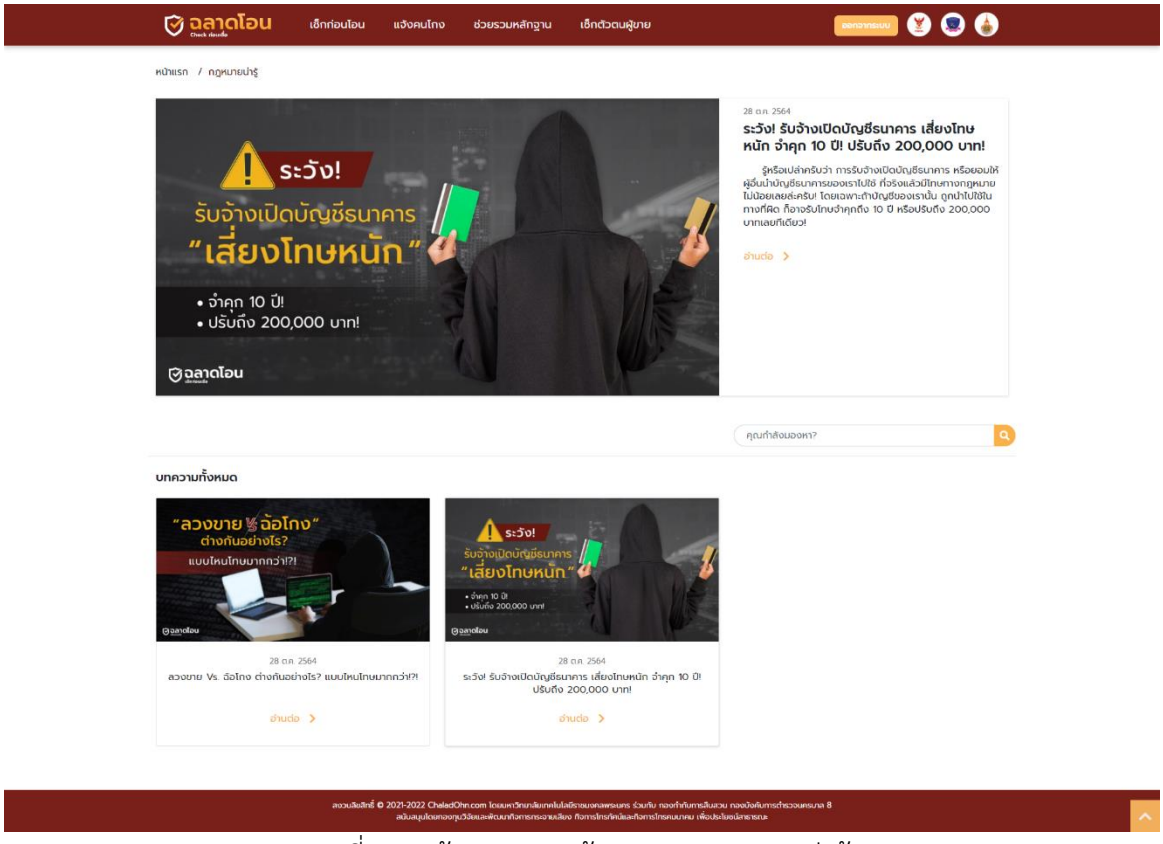
6.5 เตือนภัยไซเบอร์

หน้าบทความเตือนภัยไซเบอร์ จะนำเสนอในแง่มุมของการนำเสนอผ่านเหตุการณ์ข่าวสารในปัจจุบันที่มีความเกี่ยวข้องกับการทำธุรกรรมออนไลน์ โดยมีเนื้อหาถึงเหตุการณ์ที่เกิดขึ้น ข้อสรุปของเหตุการณ์ และข้อกฎหมายที่มีความเกี่ยวข้องกับเหตุการณ์ ให้มีความเข้าใจง่าย ประชาชนทั่วไปสามารถเข้าถึงสาระสำคัญของข้อกฎหมายนั้น และสามารถนำความรู้ที่เกี่ยวข้องกับข้อกฎหมายนั้นไปประยุกต์ใช้ได้ในการดำเนินชีวิต เพื่อเป็นแนวทางการป้องกันและปราบปรามมิจฉาชีพออนไลน์ แสดงดังรูปที่ 26

รูปที่ 26 หน้าจอแสดงหน้าบทความเตือนภัยไซเบอร์

6.6 กฎหมายน่ารู้

หน้าบทความกฎหมายน่ารู้ จะนำเสนอบทความในมุมมองของการนำข้อกฎหมายที่มีความเกี่ยวข้องกับการทำธุรกรรมออนไลน์มานำเสนอในแง่มุมที่เข้าใจง่าย เป็นประโยชน์ต่อประชาชนทั่วไปที่มีพฤติกรรมในการซื้อ-ขายสินค้าออนไลน์ หรือให้ความสนใจต่อขั้นตอนการค้นหาบัญชีผู้กระทำความผิด เพื่อเสริมสร้างองค์ความรู้ และเสริมสร้างความมั่นใจก่อนการทำธุรกรรมโอนเงินออนไลน์ แสดงดังรูปที่ 27



รูปที่ 27 หน้าจอแสดงหน้าบทความกฎหมายน่ารู้

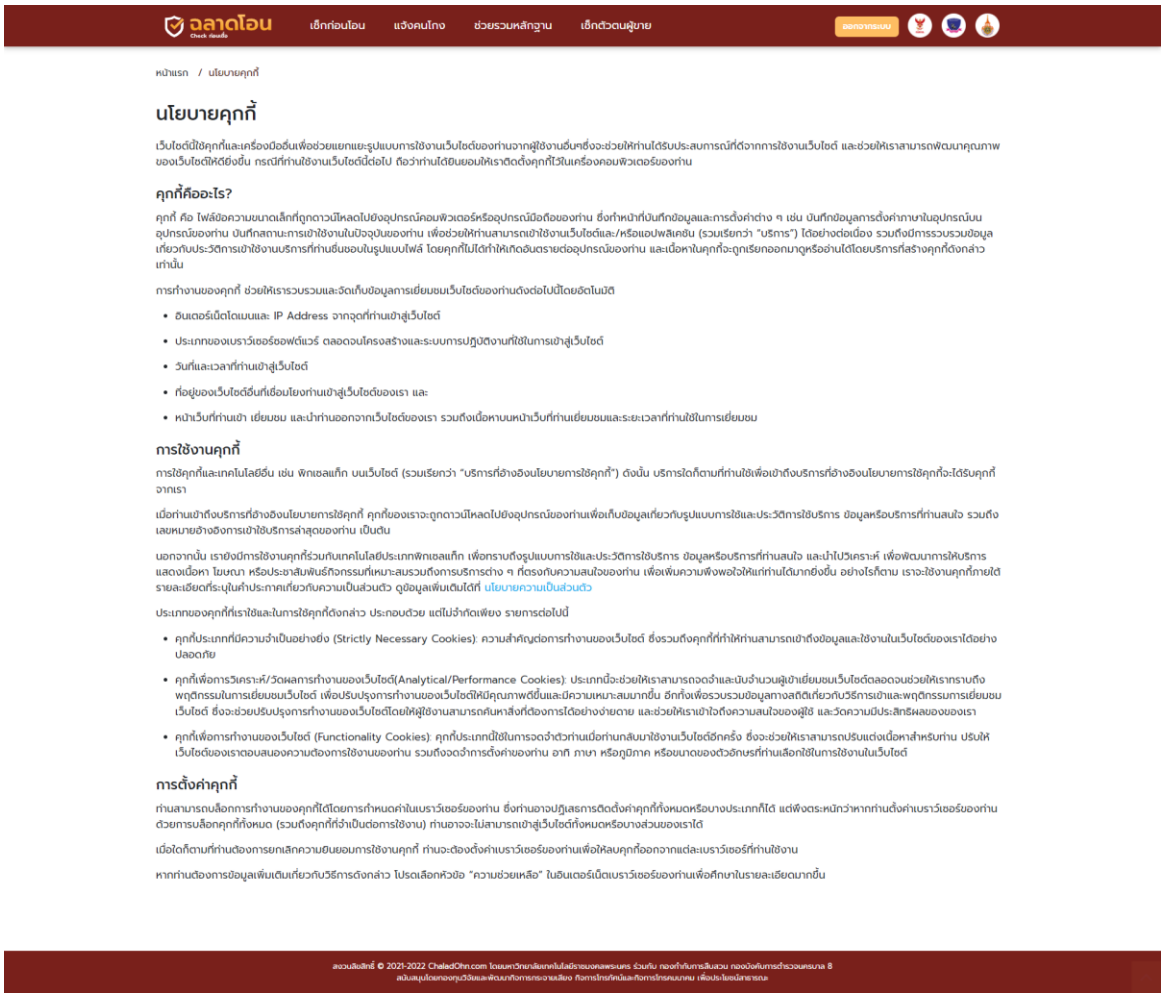
6.7 นโยบายด้านความปลอดภัย

หน้านโยบายด้านความปลอดภัย จะแสดงรายละเอียดหลักสัญญาระหว่างฉลาดโอนและผู้ใช้งาน โดยจะแจ้งรายละเอียดการจัดเก็บข้อมูลของผู้ใช้งาน รวมถึงนโยบายการคุ้มครองข้อมูลส่วนบุคคล แสดงดังรูปที่ 28

รูปที่ 28 หน้าจอแสดงนโยบาลด้านความปลอดภัย

6.8 นโยบายการเก็บรักษาข้อมูล

หน้านโยบายการเก็บรักษาข้อมูล จะแสดงข้อมูลที่ฉลาดโอนรวบรวมและจัดเก็บข้อมูลการเยี่ยมชมเว็บไซต์ของผู้ใช้งาน แสดงดังรูปที่ 29



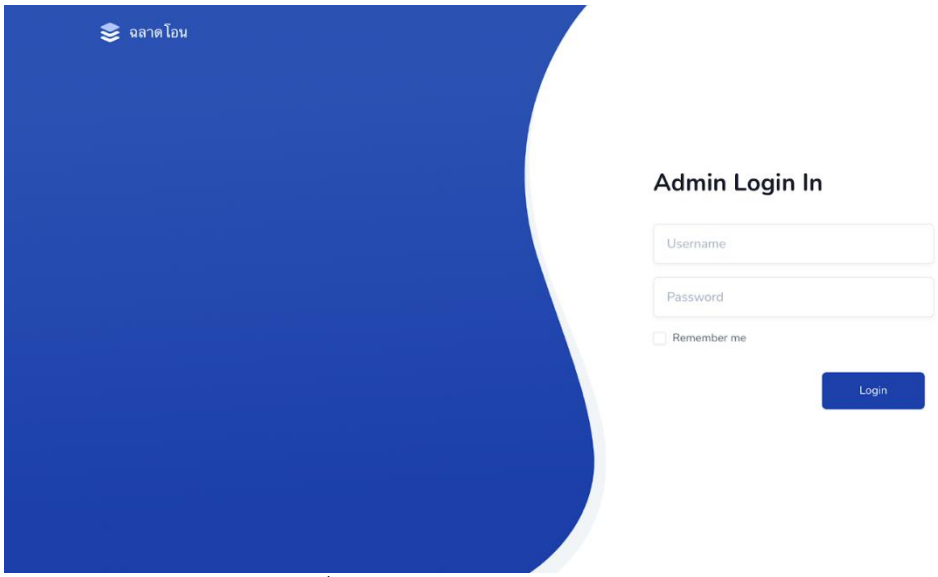
รูปที่ 29 หน้าจอแสดงนโยบายการเก็บรักษาข้อมูล

คู่มือผู้ดูแลระบบ

สารบัญ

1. การเข้าสู่ระบบ

เข้าสู่เว็บไซต์ https://chaladohn.com/report/adm2022 จะแสดงหน้าจอสำหรับการล็อกอินเข้าสู่ระบบ แสดงดังรูปที่ 1 โดยจะต้องกรอก Username และ Password ให้ถูกต้อง จากนั้นกดปุ่มล็อกอิน (Login) เพื่อเข้าสู่ระบบ



รูปที่ 1 หน้าจอสำหรับการล็อกอินเข้าสู่ระบบฉลาดโอน

2. หน้าบัญชีการใช้งาน

เมื่อผู้ใช้งานล็อกอินเข้ามาแล้วจะพบกับหน้าบัญชีการใช้งานซึ่งจะเป็นหน้าของภาพรวมระบบ ดังรูปที่ 2 ซึ่งจะประกอบไปด้วยทั้งหมด 5 ส่วน ได้แก่

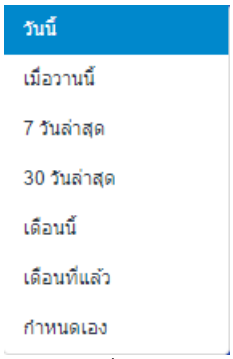
2.1 ภาพรวมระบบ
2.2 รายการแจ้งคนโกง
2.3 บทความ
2.4 รายชื่อสมาชิก
2.5 ผู้ดูแลระบบ

2.1) ภาพรวมระบบ

หน้าภาพรวมระบบจะแสดงข้อมูลสถิติต่าง ๆ ทั้งหมด เช่น จำนวนสมาชิกทั้งหมด จำนวนผู้แจ้ง จำนวนผู้รวบรวมหลักฐาน จำนวนผู้ขาย จำนวนเช็กคนโกง จำนวนเช็กตัวตน จำนวนแจ้งคนโกง จำนวนช่วยรวมหลักฐาน นอกจากนี้ ยังแสดงข้อมูลในรูปแบบกราฟเส้นและกราฟวงกลม แสดงดังรูปที่ 2

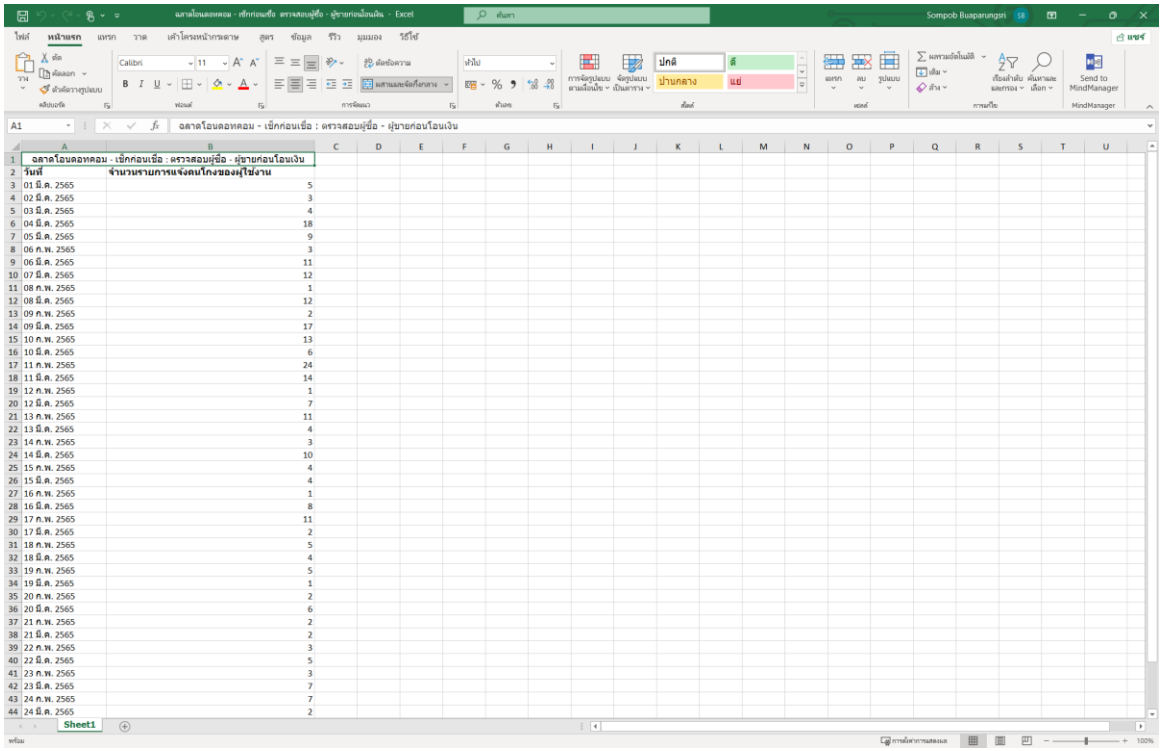
รูปที่ 2 หน้าจอภาพรวมระบบ

จากรูปที่ 2 ผู้ใช้งานสามารถกดเลือกวันที่ต้องการตรวจสอบข้อมูลได้ โดยกดที่ปุ่ม  จะปรากฏหน้าต่าง แสดงดังรูปที่ 3 จากนั้นระบบจะประมวลผล และแสดงข้อมูลตามที่ผู้ใช้งานเลือก



รูปที่ 3 หน้าต่างแสดงช่วงเวลาที่ผู้ใช้งานต้องการตรวจสอบข้อมูล

นอกจากนี้ ผู้ใช้งานยังสามารถนำออกข้อมูลจำนวนรายการแจ้งคนโกงในหน้ารายงาน ในรูปแบบไฟล์ Excel หรือ CSV โดยกดที่ปุ่ม  หรือ  โดยจะได้ข้อมูลออกมา แสดงดังรูปที่ 4



ฉลาดโอนดอทคอม - เช็กก่อนเชื่อ : ตรวจสอบผู้ซื้อ - ผู้ขายก่อนโอนเงิน	
วันที่	จำนวนรายการแจ้งคนโกงของผู้ใช้งาน
01 มี.ค. 2565	5
02 มี.ค. 2565	3
03 มี.ค. 2565	4
04 มี.ค. 2565	18
05 มี.ค. 2565	9
06 ก.พ. 2565	3
06 มี.ค. 2565	11
07 มี.ค. 2565	12
08 ก.พ. 2565	1
08 มี.ค. 2565	12
09 ก.พ. 2565	2
09 มี.ค. 2565	17
10 ก.พ. 2565	13
10 มี.ค. 2565	6
11 ก.พ. 2565	24
11 มี.ค. 2565	14
12 ก.พ. 2565	1
12 มี.ค. 2565	7
13 ก.พ. 2565	11
13 มี.ค. 2565	4
14 ก.พ. 2565	3
14 มี.ค. 2565	10
15 ก.พ. 2565	4
15 มี.ค. 2565	4
16 ก.พ. 2565	1
16 มี.ค. 2565	8
17 ก.พ. 2565	11
17 มี.ค. 2565	2
18 ก.พ. 2565	5
18 มี.ค. 2565	4
19 ก.พ. 2565	5
19 มี.ค. 2565	1
20 ก.พ. 2565	2
20 มี.ค. 2565	6
21 ก.พ. 2565	2
21 มี.ค. 2565	2
22 ก.พ. 2565	3
22 มี.ค. 2565	5
23 ก.พ. 2565	3
23 มี.ค. 2565	7
24 ก.พ. 2565	7
24 มี.ค. 2565	2

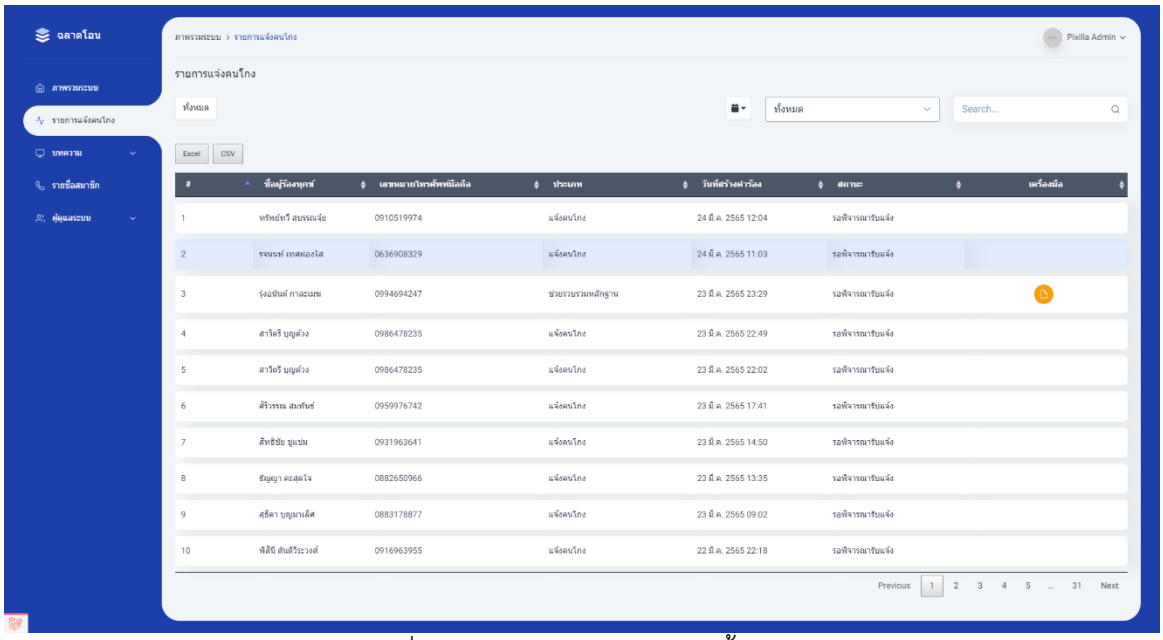
รูปที่ 4 แสดงรายงานสถิติจำนวนรายการแจ้งข้อมูลคนโกง

2.2) รายการแจ้งคนโกง

หน้ารายการแจ้งคนโกง จะแสดงรายชื่อผู้ใช้งานที่แจ้งคนโกงและช่วยรวมหลักฐานทั้งหมดในรูปแบบตาราง ประกอบด้วย

(1) ชื่อผู้ร้องทุกข์ – แสดงชื่อและนามสกุล ของผู้ร้องทุกข์
(2) เลขหมายโทรศัพท์มือถือ – แสดงเลขหมายโทรศัพท์ของผู้ร้องทุกข์
(3) ประเภท – แสดงประเภทของการแจ้ง แบ่งออกเป็น แจ้งคนโกง และช่วยรวมหลักฐาน
(4) วันที่สร้างคำร้อง – แสดงวันที่และเวลาที่ผู้ร้องทุกข์สร้างคำร้อง
(5) สถานะ – แสดงสถานะของรายการแจ้งคนโกงที่ผู้เสียหายแจ้งเข้ามาผ่านทางเว็บไซต์ฉลาดโอน แบ่งออกเป็น รับแจ้ง รอพิจารณารับแจ้ง และยกเลิก
(6) เครื่องมือ – แสดงไฟล์แนบของการแจ้งความดำเนินคดีของผู้เสียหาย โดยจะปรากฏเฉพาะรายการที่เป็นการช่วยรวมหลักฐานเท่านั้น

แสดงรายละเอียดดังรูปที่ 5

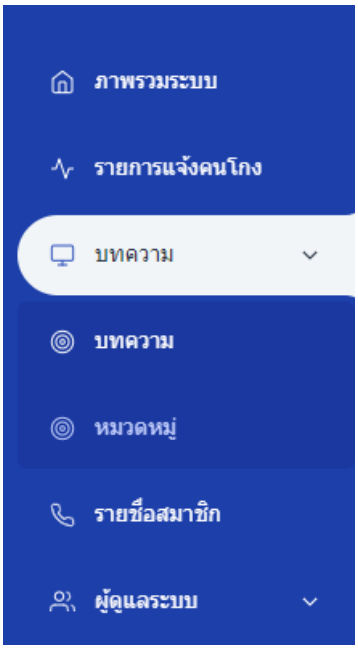


รูปที่ 5 แสดงรายการแจ้งคนโกงทั้งหมด

ในเมนูนี้ ผู้ใช้งานสามารถนำออกเอกสาร กรองรายชื่อตามวันที่ต้องการดูข้อมูล หรือค้นหาข้อมูลที่ต้องการเป็นรายบุคคลไป

2.3) บทความ

หน้าบทความจะแบ่งเป็น 2 ส่วนคือ บทความและหมวดหมู่ แสดงดังรูปที่ 3



รูปที่ 6 แสดงรายการส่วนย่อยของบทความ

2.3.1 บทความ

ส่วนแรกเป็นบทความต่าง ๆ ที่เขียนทั้งหมดของเว็บไซต์ฉลาดโอน โดยแสดงรายละเอียดรูปแบบตาราง ประกอบด้วย

(1) ชื่อบทความ – ชื่อบทความที่ลงบทเว็บไซต์ฉลาดโอน

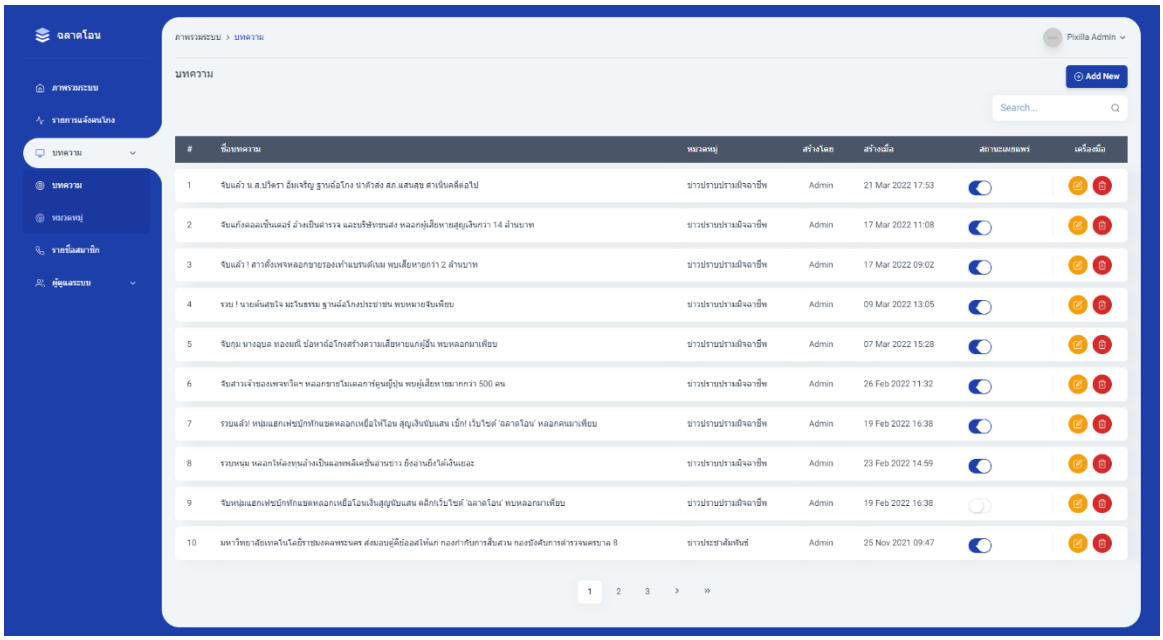
(2) หมวดหมู่ – หมวดหมู่ของบทความ ประกอบด้วย 4 หมวดหมู่ ได้แก่ เตือนภัยไซเบอร์ กฎหมายน่ารู้ ข่าวประชาสัมพันธ์ ข่าวปราบปรามมิจฉาชีพ

(3) สร้างโดย – ชื่อผู้ใช้งานที่เป็นผู้สร้างบทความ

(4) สร้างเมื่อ – วันและเวลาที่สร้างบทความ

(5) สถานะเผยแพร่ - สถานะของบทความ สามารถเลือกเปิดหรือปิดบนเว็บไซต์ฉลาดโอนได้

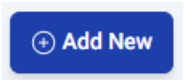
(6) เครื่องมือ – การจัดการกับบทความ สามารถแก้ไขบทความ หรือลบบทความได้ แสดงรายละเอียดดังรูปที่ 7



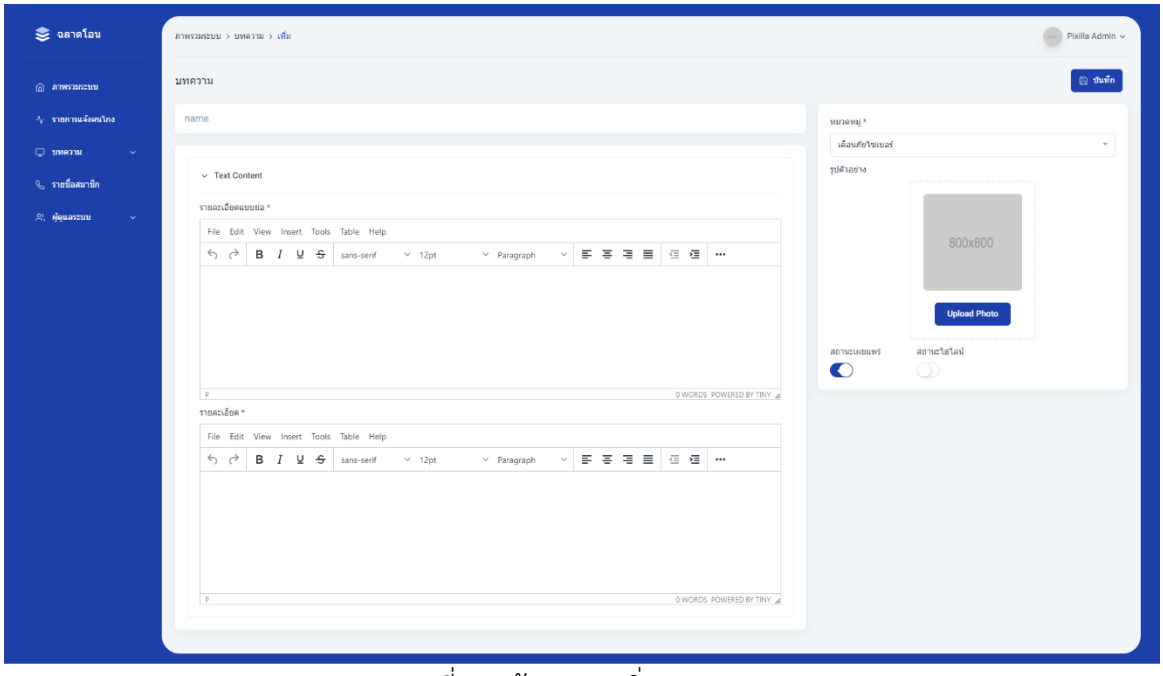
รูปที่ 7 หน้าจอการจัดการบทความ

การเพิ่มบทความ

การเพิ่มบทความผู้ใช้งานสามารถเพิ่มบทความใหม่ ๆ ลงไปได้ โดยกดปุ่ม



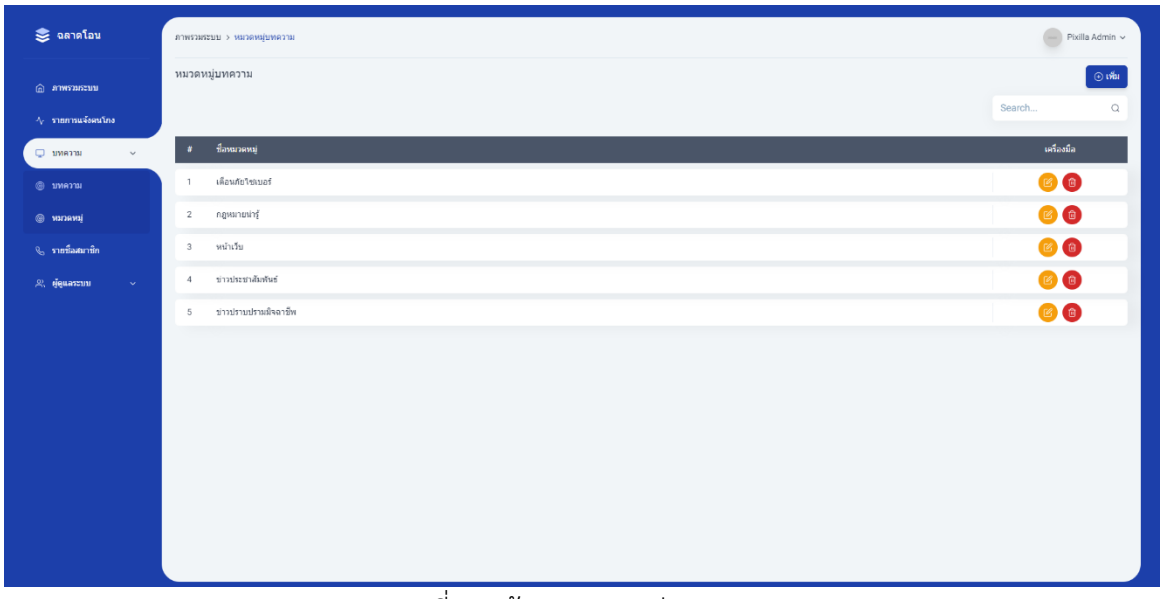
ทางด้านบนขวามือ ของรูปที่ 7 เมื่อคลิกปุ่มแล้วจะแสดงหน้าจอให้กรอกข้อมูลต่างๆ เมื่อกรอกข้อมูลครบถ้วนแล้วให้กดปุ่มบันทึก ดังรูปที่ 8



รูปที่ 8 หน้าจอการเพิ่มบทความ

2.2.2 หมวดหมู่บทความ

ในส่วนของหมวดหมู่บทความจะแสดงหมวดหมู่ของบทความที่มีอยู่และสามารถเพิ่มหรือแก้ไขได้ ดังรูปที่ 9

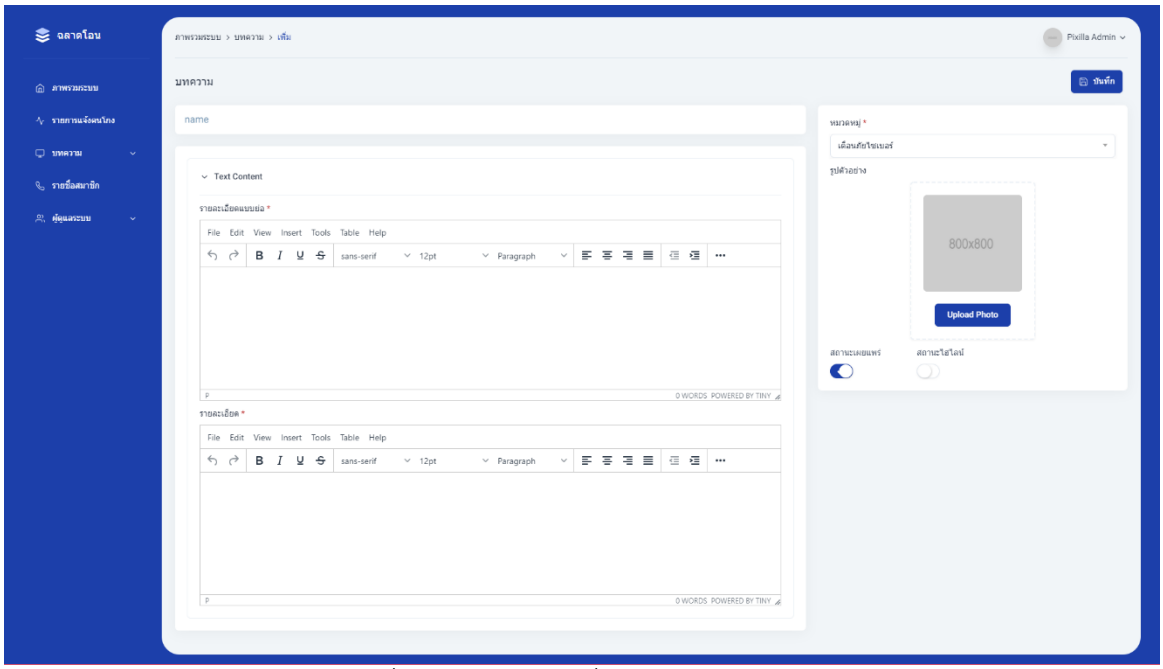


รูปที่ 9 หน้าจอหมวดหมู่บทความ

การเพิ่มหมวดหมู่บทความ

การเพิ่มหมวดหมู่บทความผู้ใช้งานสามารถคลิกปุ่ม 

ด้านบนขวามือจากรูปที่ 9 เมื่อคลิกเข้ามาแล้วจะแสดงหน้าจอให้เพิ่มหมวดหมู่ หากกรอกเสร็จสิ้นแล้วให้กดปุ่มบันทึก ดังรูปที่ 10



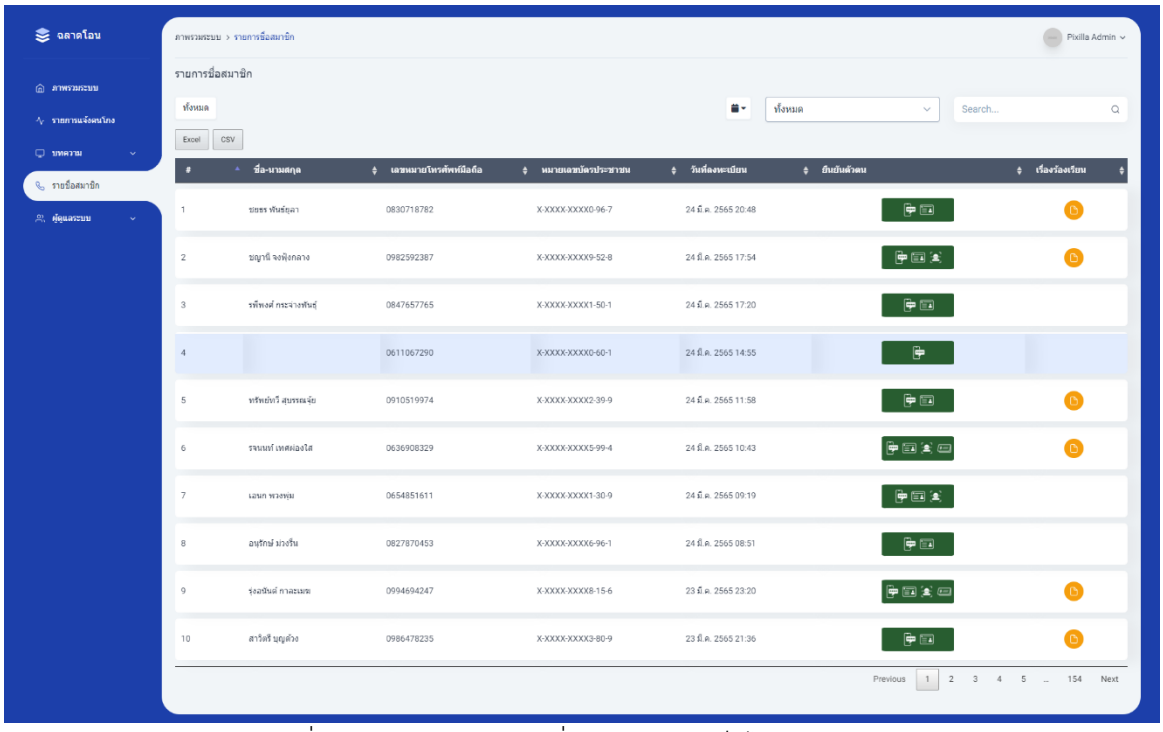
รูปที่ 10 หน้าจอการเพิ่มหมวดหมู่บทความ

2.4) รายชื่อสมาชิก

หน้ารายชื่อสมาชิก จะแสดงรายสมาชิกผู้ใช้งานที่ลงทะเบียนกับเว็บไซต์ฉลาดโอนทั้งหมดในรูปแบบตาราง ประกอบด้วย

(1) ชื่อ-นามสกุล – แสดงชื่อและนามสกุล ของผู้ใช้งานแต่ละราย
(2) เลขหมายโทรศัพท์มือถือ – แสดงเลขหมายโทรศัพท์ของผู้ใช้งานแต่ละราย
(3) หมายเลขบัตรประชาชน – แสดงหมายเลขจากบัตรประจำตัวประชาชนของผู้ใช้งานแต่ละราย
(4) วันที่ลงทะเบียน – แสดงวันและเวลาที่ผู้ใช้งานลงทะเบียนกับเว็บไซต์ฉลาดโอน
(5) ยืนยันตัวตน – แสดงสถานะของการยืนยันตัวตนของผู้ใช้งาน แบ่งออกเป็น 4 ระดับ ได้แก่ เลขหมายโทรศัพท์ บัตรประชาชน รูปถ่ายใบหน้า และรูปภาพสมุดบัญชี
(6) เรื่องร้องเรียน – แสดงเอกสารการร้องเรียนของผู้ใช้งานแต่ละราย

แสดงรายละเอียดดังรูปที่ 11



รูปที่ 11 หน้าจอแสดงรายชื่อสมาชิกของเว็บไซต์ฉลาดโอน

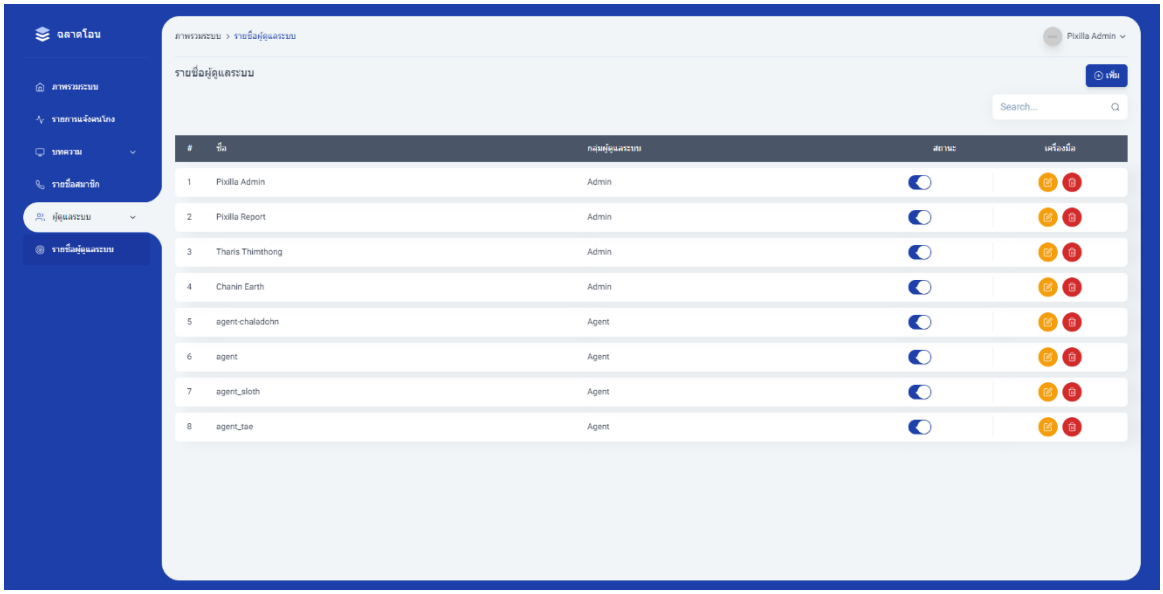
ในเมนูนี้ ผู้ใช้งานสามารถนำออกเอกสาร กรองรายชื่อตามวันที่ต้องการดูข้อมูล หรือค้นหาข้อมูลที่ต้องการเป็นรายบุคคลไป

2.5) ผู้ดูแลระบบ

ในส่วนของผู้ดูแลระบบประกอบไปด้วยรายชื่อผู้ดูแลระบบ

2.5.1 รายชื่อผู้ดูแลระบบ

รายชื่อของผู้ดูแลระบบจะแสดงรายละเอียดต่าง ๆ ในรูปแบบตาราง สามารถเพิ่ม แก้ไข หรือลบได้ ดังรูปที่ 12

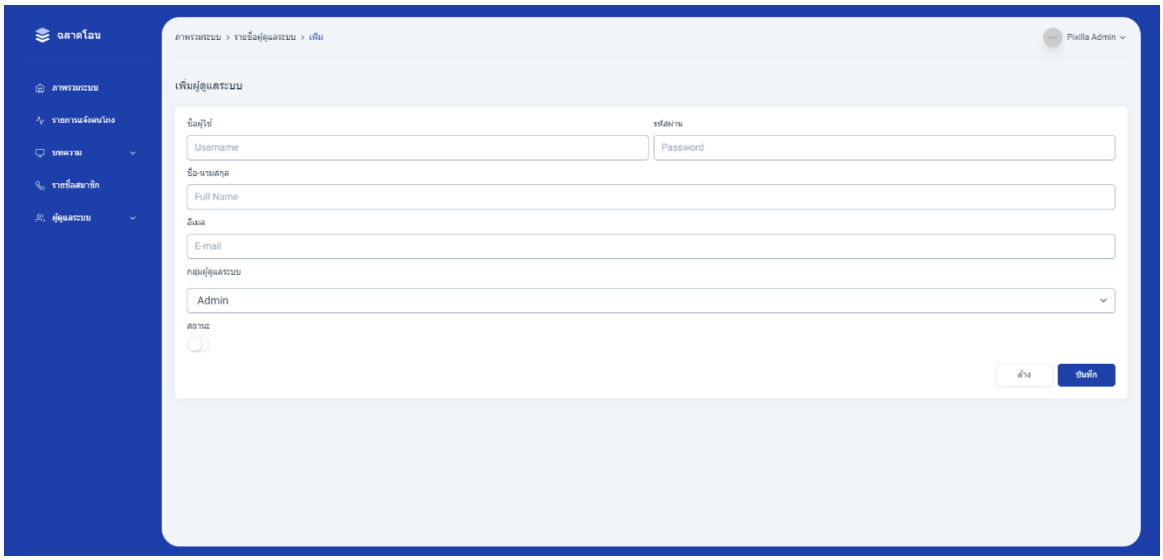


รูปที่ 12 หน้าจอแสดงรายชื่อผู้ดูแลระบบ

การเพิ่มผู้ดูแลระบบ

การเพิ่มผู้ดูแลระบบสามารถทำได้โดยกดปุ่ม 

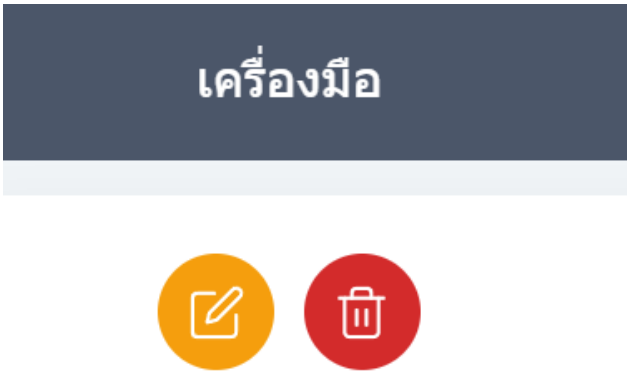
ด้านบนขวามือของรูปที่ 12 เมื่อกดเข้าไปแล้วจะแสดงรายละเอียดต่างๆ กรอกจนครบแล้วกดบันทึก ดังรูปที่ 13



รูปที่ 13 หน้าจอการกรอกรายละเอียดการเพิ่มผู้ดูแลระบบ

การแก้ไขหรือลบผู้ดูแลระบบ

การแก้ไขหรือลบผู้ดูแลระบบผู้ใช้งานสามารถแก้ไขหรือลบได้จากแถบเครื่องมือ โดยมีปุ่มสีเหลืองสำหรับการแก้ไข และปุ่มสีแดงสำหรับลบบทความ ดังรูปที่ 14



รูปที่ 14 ปุ่มสำหรับการแก้ไขหรือลบผู้ดูแลระบบ

สรุปผลการอบรมผู้ใช้งานระบบ

สรุปผลการอบรมผู้ใช้งานระบบ

โครงการพัฒนาระบบต้นแบบเพื่อสนับสนุนงานป้องกันและปราบปรามมิจฉาชีพออนไลน์ที่ไม่ระบุตัวตน (ระยะที่ 1) : กรณีศึกษา เขตพื้นที่กองบังคับการตำรวจนครบาล 8 ได้ดำเนินการพัฒนาระบบเพื่อให้เป็นไปตามวัตถุประสงค์เพื่อออกแบบและพัฒนาระบบตนแบบสำหรับป้องกันและปราบปรามมิจฉาชีพแบบออนไลน์สำหรับพนักงานสอบสวนและประชาชน และดำเนินการจัดอบรมให้ผู้ใช้งานทั่วไปและผู้ดูแลระบบ ดังนี้

1. การจัดอบรมเชิงปฏิบัติการ

1.1 หลักการและเหตุผล

ตามที่สำนักงานกองทุนวิจัยและพัฒนา สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ ได้ว่าจ้างมหาวิทยาลัยเทคโนโลยีราชมงคล พระนคร เป็นที่ปรึกษาดำเนินงานโครงการพัฒนาระบบต้นแบบเพื่อสนับสนุนงานป้องกันและปราบปรามมิจฉาชีพออนไลน์ที่ไม่ระบุตัวตน (ระยะที่ 1)

ในการนี้ ทางคณะผู้วิจัย ได้ดำเนินการพัฒนาระบบต้นแบบเพื่อสนับสนุนงานป้องกันและปราบปรามมิจฉาชีพออนไลน์ที่ไม่ระบุตัวตนเสร็จสิ้นเป็นที่เรียบร้อย จึงเห็นควรให้มีการดำเนินการถ่ายทอดเทคโนโลยีให้กับเจ้าหน้าที่ตำรวจ เพื่อให้สามารถใช้งานระบบได้อย่างมีประสิทธิภาพมากขึ้น และสามารถดูแล หรือแก้ไขระบบเบื้องต้นได้

1.2 วัตถุประสงค์

1) เพื่อให้ผู้เข้ารับการอบรมได้เรียนรู้ และรู้จักการใช้ระบบต้นแบบเพื่อสนับสนุนงานป้องกันและปราบปรามมิจฉาชีพออนไลน์ที่ไม่ระบุตัวตน ได้อย่างมีประสิทธิภาพ
2) เพื่ออำนวยความสะดวกในการติดตาม และปราบปรามมิจฉาชีพออนไลน์ที่ไม่ระบุตัวตน
3) เพื่อให้ผู้ใช้งานสามารถ แก้ไขปัญหาเบื้องต้น กรณีระบบฉลาดโอนมีปัญหาได้

1.3 กำหนดการฝึกอบรม

จัดอบรบแบบออนไลน์ โดยแบ่งออกเป็น 3 รอบ ดังนี้

1) การใช้งานระบบต้นแบบป้องกันและปราบปรามมิจฉาชีพออนไลน์ รอบที่ 1 วันจันทร์ที่ 22 พฤศจิกายน 2564 เวลา 09.00 น. - 12.00 น.
2) การใช้งานระบบต้นแบบป้องกันและปราบปรามมิจฉาชีพออนไลน์ รอบที่ 2 วันจันทร์ที่ 22 พฤศจิกายน 2564 เวลา 13.00 น. - 16.00 น.
3) การดูแลระบบต้นแบบป้องกันและปราบปรามมิจฉาชีพออนไลน์ วันอังคารที่ 23 พฤศจิกายน 2564 เวลา 09.00 - 12.00 น.

กำหนดการอบรม
“การใช้งานระบบต้นแบบป้องกันและปราบปรามมิจฉาชีพออนไลน์” (รอบที่ 1)
โครงการการพัฒนาระบบต้นแบบเพื่อสนับสนุนงานป้องกัน และปราบปรามมิจฉาชีพออนไลน์ที่ไม่ระบุตัวตน (ระยะที่ 1) : กรณีศึกษา เขตพื้นที่กองบังคับการตำรวจนครบาล 8

วันจันทร์ที่ 22 พฤศจิกายน 2564

.....

09.00 - 09.30 น.	ที่มาของโครงการ
09.30 - 09.45 น.	วัตถุประสงค์ของโครงการ
09.45 - 11.00 น.	เว็บไซต์ฉลาดโอนดอทคอม
	- เช็กก่อนโอน
	- ลงทะเบียนและยืนยันตัวตน
	- แจ้งคนโกง
11.00 - 11.30 น.	การใช้งาน Line Bot “Metro Police Connect”
11.30 - 12.00 น.	ตอบข้อซักถาม

กำหนดการอบรม
“การใช้งานระบบต้นแบบป้องกันและปราบปรามมิจฉาชีพออนไลน์” (รอบที่ 2)
โครงการการพัฒนาระบบต้นแบบเพื่อสนับสนุนงานป้องกัน ฆและปราบปราม มิจฉาชีพออนไลน์ที่ไม่ระบุตัวตน (ระยะที่ 1) : กรณีศึกษา เขตพื้นที่กองบังคับการตำรวจนครบาล 8

วันจันทร์ที่ 22 พฤศจิกายน 2564

.....

13.00 - 13.30 น.	ที่มาของโครงการ
13.30 - 13.45 น.	วัตถุประสงค์ของโครงการ
13.45 - 15.00 น.	เว็บไซต์ฉลาดโอนดอทคอม
	- เช็กก่อนโอน
	- ลงทะเบียนและยืนยันตัวตน
	- แจ้งคนโกง
15.00 - 15.30 น.	การใช้งาน Line Bot “Metro Police Connect”
15.30 - 16.00 น.	ตอบข้อซักถาม

กำหนดการอบรม
“การดูแลระบบต้นแบบป้องกันและปราบปรามมิจฉาชีพออนไลน์”
โครงการการพัฒนาระบบต้นแบบเพื่อสนับสนุนงานป้องกัน และปราบปรามมิจฉาชีพออนไลน์ที่ไม่ระบุตัวตน (ระยะที่ 1) : กรณีศึกษา เขตพื้นที่กองบังคับการตำรวจนครบาล 8

วันอังคารที่ 23 พฤศจิกายน 2564

.....

09.00 - 09.30 น.	ที่มาของโครงการ
09.30 - 09.45 น.	วัตถุประสงค์ของโครงการ
09.45 - 10.15 น.	การดูรายงานแจ้งคนโกง
10.15 – 11.00 น.	การจัดการบทความบนเว็บไซต์ฉลาดโอน
11.00 - 11.30 น.	ระบบจัดการผู้ใช้งานบนเว็บไซต์
11.30 - 12.00 น.	ตอบข้อซักถาม

1.1.5 ผู้เข้าร่วมการอบรม
เจ้าหน้าที่ตำรวจจาก กองบังคับการตำรวจนครบาล 8

1) การอบรมการใช้งานระบบต้นแบบป้องกันและปราบปรามมิจฉาชีพออนไลน์ รอบที่ 1

รายชื่อผู้เข้าร่วมอบรบ
"การใช้งานระบบต้นแบบป้องกันและปราบปรามมิจฉาชีพออนไลน์ รอบที่ 1"
วันจันทร์ที่ 22 พฤศจิกายน 2564 เวลา 09.00 – 12.00 น.

ลำดับ	ชื่อ-นามสกุล	หน่วยงาน	ตำแหน่ง	ลายมือชื่อ
1.	ส.ต.อ.บุญสวรรค์ ทับทอง			
2.	ส.ต.อ.สุภี ศศิวรรณ			
3.	ด.ต.วัชริศ สุวรรณวงศ์			
4.	ส.ต.อ.สุวัฒนา สุภาวดี			
5.	ส.ต.อ.นภัทร์ มนูญวงศ์			
6.	ร.ต.ท.กรวัฒน์ จ้อยเจือ			
7.	ส.ต.อ.ปิยะกูล ราชนา			
8.	พ.ต.อ.นิภพล สุชนิยม			
9.	ด.ต.หญิง นันทพร			
10.	พ.ต.ท. วิทยา สมการ			
11.	ร.ต.ต. ปกรณ์ ศักดิ์ดี			
12.	ด.ต. ไพโรจน์ พิเสิศ			
13.	ด.ต. สำรอง รอดคำทุย			
14.	น.ส. มาลินี เนียมเฟือง			
15.	ส.ต.อ. เอกราช แจ้งคำ			
16.	ร.ต.ท. จิรชยุตม์ ทองแจ่ม			
17.	ด.ต. ปิยบุตร พุ่มเจริญ			
18.	น.ส. อารีญา ช้างหล่อ			
19.	นายภัทรพล ธรรมมารมย์			
20.	น.ส. อรวรรณ แก้วประดิษฐ์			

2) การอบรมการใช้งานระบบต้นแบบป้องกันและปราบปรามมิจฉาชีพออนไลน์ รอบที่ 2

รายชื่อผู้เข้าร่วมอบรม
"การใช้งานระบบต้นแบบป้องกันและปราบปรามมิจฉาชีพออนไลน์ รอบที่ 2"
วันจันทร์ที่ 22 พฤศจิกายน 2564 เวลา 13.00 – 16.00 น.

ลำดับ	ชื่อ-นามสกุล	หน่วยงาน	ตำแหน่ง	ลายมือชื่อ
1.	ส.ต.ท.ปรัชญ์ บัวจีน			
2.	ส.ต.ท.เกียรติภูมิ วิริยกาญจนสกุล			
3.	ร.ต.อ.สิทธิชัย พรมเรียน			
4.	ส.ต.อ.กฤษณรักษ์ ดำจุติ			
5.	พ.ต.ท. สามารถ ด้วงทรง			
6.	ร.ต.ต. บุญส่ง โชติสิทธิเกียรติ			
7.	ร.ต.ท.นัณฑิต ค้าสม			
8.	ร.ต.อ. สามารถ วงศ์สายจันทร์			
9.	ร.ต.อ. นรา หนูช่วย			
10.	ด.ต. ภูมิมินทร์ ยิ่งยง			
11.	นายฐิติกร กิ่งวงศา			
12.	ร.ต.ต. ธนพล พักษา			
13.	ส.ต.อ. อภิชัย เชียวชอุ่ม			
14.	ส.ต.อ. ธเนศชัย พลเยี่ยม			
15.	ส.ต.ท. กิตติพศ เจนจบ			
16.	ส.ต.ต. จักรินทร์ บุณยกิตียาการ			
17.	ส.ต.อ. ชัญญานุช ศรีสวัสดิ์			
18.	ร.ต.ต. พงศ์ภรณ์ ทวีแก้ว			
19.	นายสมนึก ก้าวหน้าวาณิช			
20.	น.ส. นิมนวล บัตลยะราช			

3) การอบรมผู้ดูแลระบบต้นแบบป้องกันและปราบปรามมิจฉาชีพออนไลน์

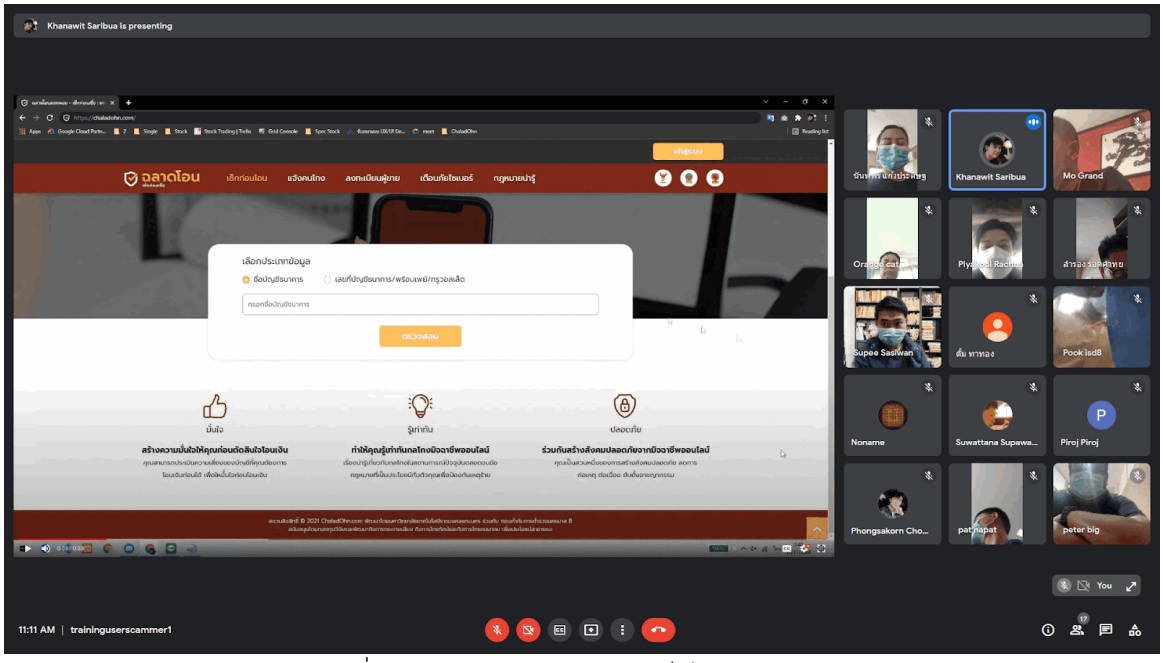
รายชื่อผู้เข้าร่วมอบรม
"การดูแลระบบต้นแบบป้องกันและปราบปรามมิจฉาชีพออนไลน์ รอบที่ 1"
วันอังคารที่ 23 พฤศจิกายน 2564 เวลา 09.00 – 12.00 น.

ลำดับ	ชื่อ-นามสกุล	หน่วยงาน	ตำแหน่ง	ลายมือชื่อ
1.	ร.ต.อ. วิทูร สังข์สอาด			
2.	ร.ต.ท. ทัตเทพ หอมงาม			
3.	ส.ต.อ. เอกราช แจ้งคำ			
4.	ส.ต.อ. ปิยะกูล ราชนา			
5.	ส.ต.อ. นภัทร์ มนูญวงศ์			
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				

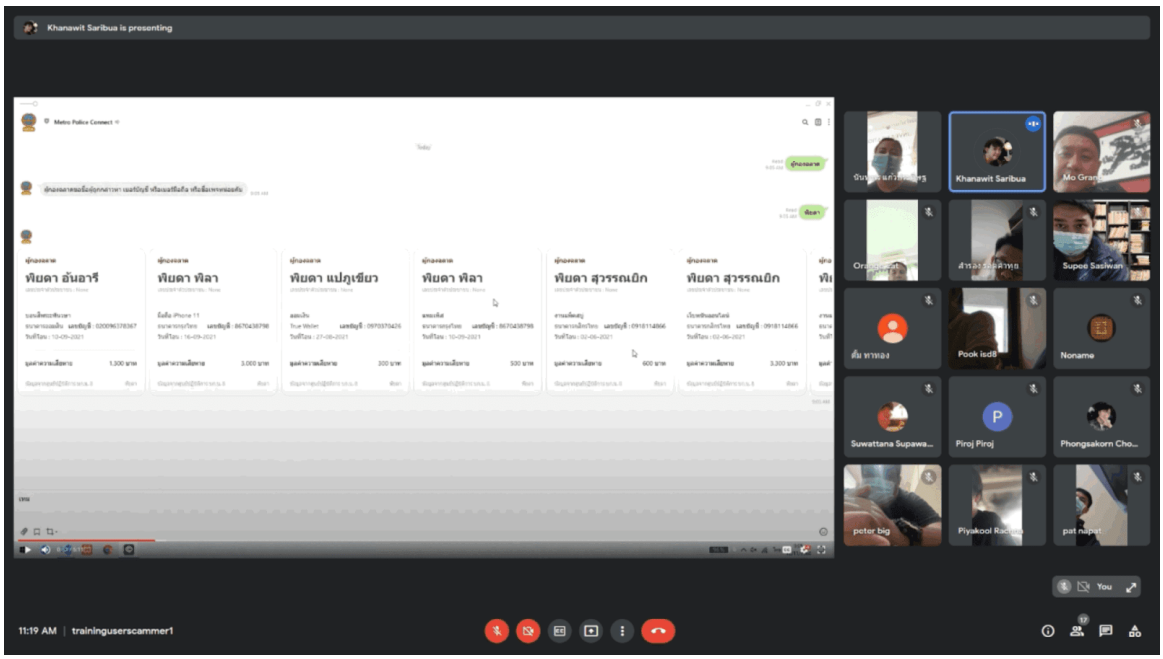
1.2 ภาพบรรยากาศการอบรม

การจัดอบรม การใช้งานระบบต้นแบบป้องกันและปราบปรามมิจฉาชีพออนไลน์ ครั้งนี้ เป็นการประชุมแบบออนไลน์ เนื่องจากสถานการณ์แพร่ระบาดของโรคติดเชื้อไวรัสโคโรนา (COVID-19) ทั้งที่ทางคณะผู้วิจัย ได้มุ่งเน้นการมีส่วนร่วมกับผู้เข้าอบรมในการทดลองการใช้งานระบบ รวมถึงเปิดรับความเห็นเพื่อนำไปปรับปรุงในลำดับถัดไป

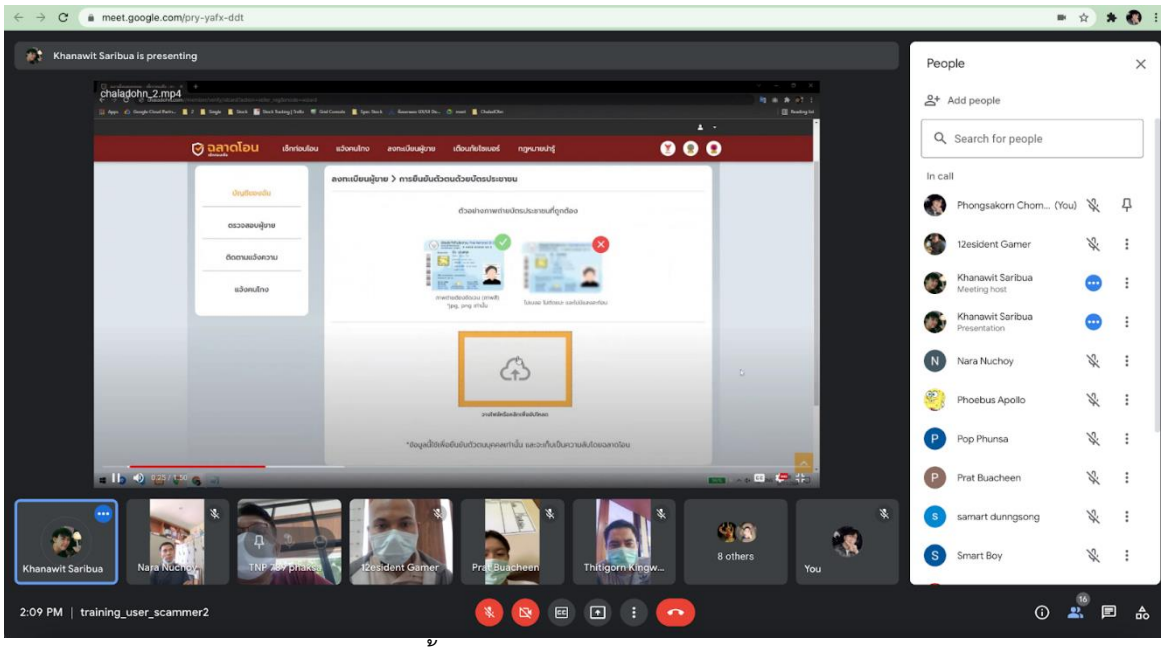
1.2.1 การอบรมผู้ใช้งานทั่วไป



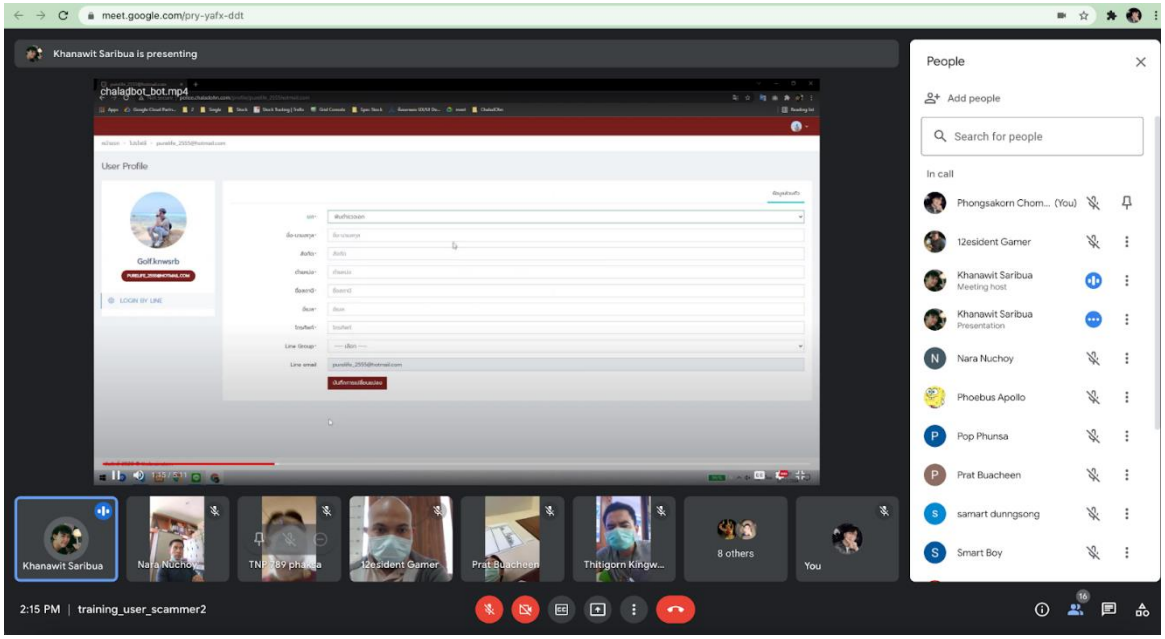
รูปที่ 1 การนำเสนอการใช้งานเว็บไซต์ฉลาดโอน



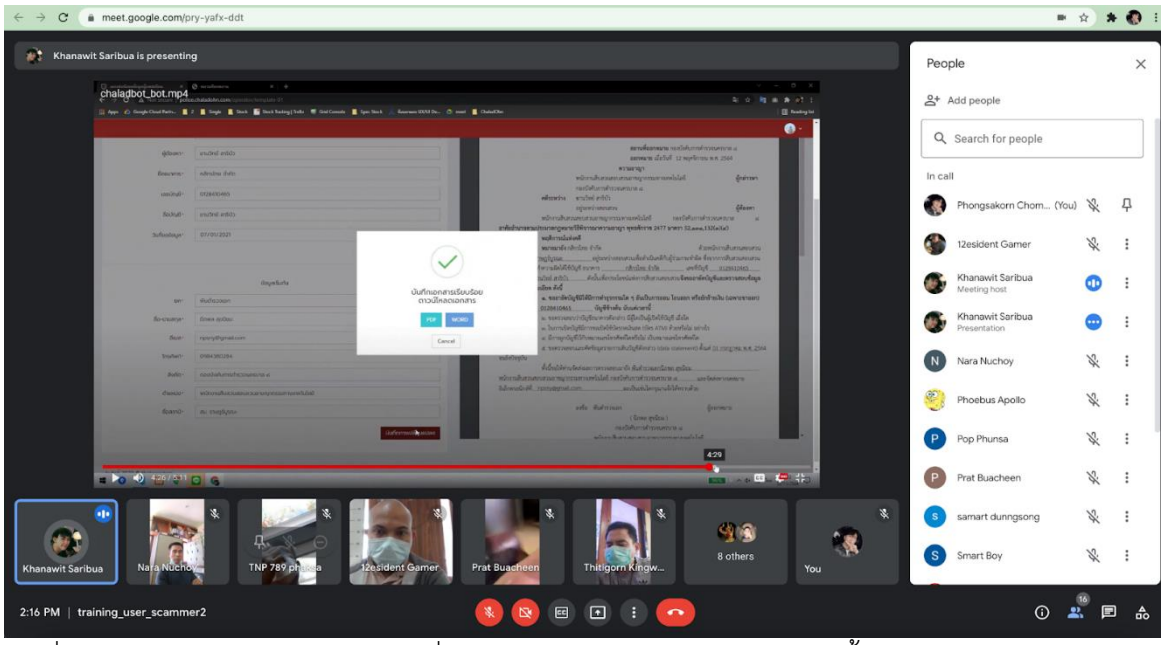
รูปที่ 2 อธิบายการใช้ Line Bot “Metro Police Connect” เพื่อตรวจสอบรายชื่อผู้กระทำความผิด



รูป 3 อธิบายขั้นตอนการยืนยันตัวตนด้วยบัตรประชาชน

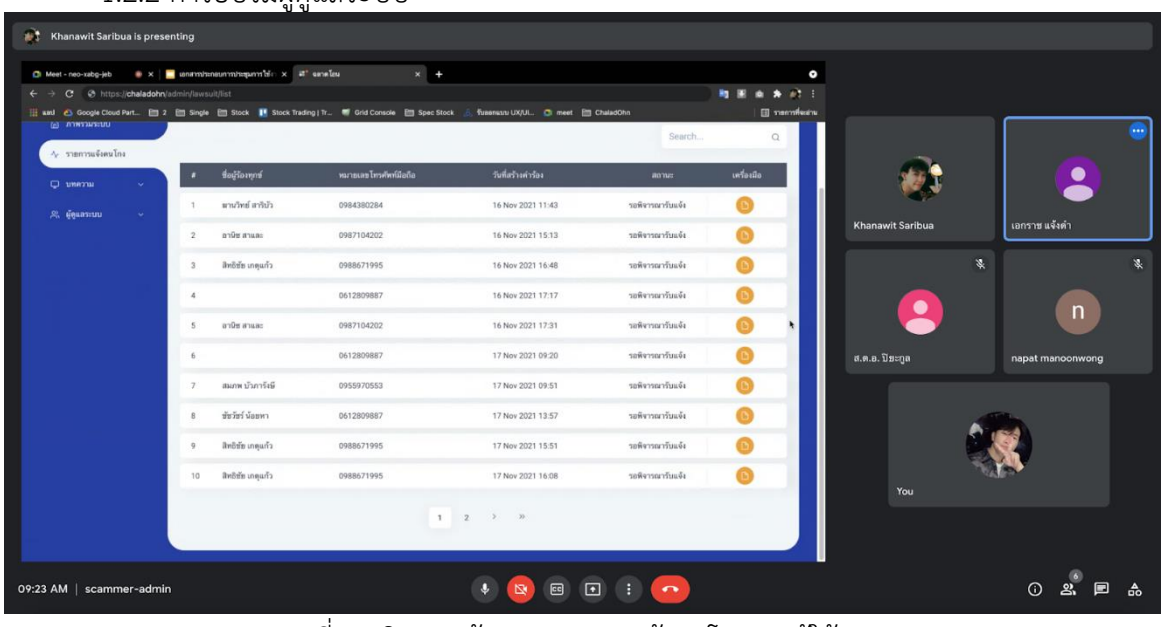


รูปที่ 4 อธิบายการกรอกข้อมูลเพื่อใช้ Line Bot “Metro Police Connect” ในการสร้างคำขอแลกเปลี่ยนข้อมูลกับหน่วยงานภายนอก

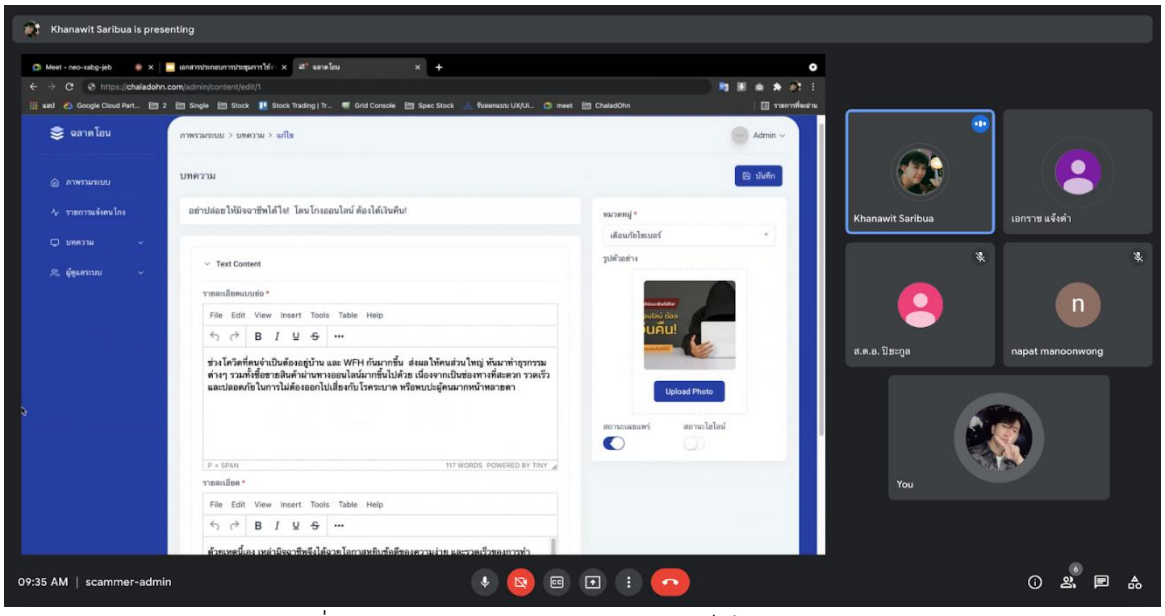


รูปที่ 5 อธิบายการบันทึกคำขอแลกเปลี่ยนข้อมูลกับหน่วยงานภายนอก รวมทั้งการนำออกในรูปแบบไฟล์ PDF หรือไฟล์ Word

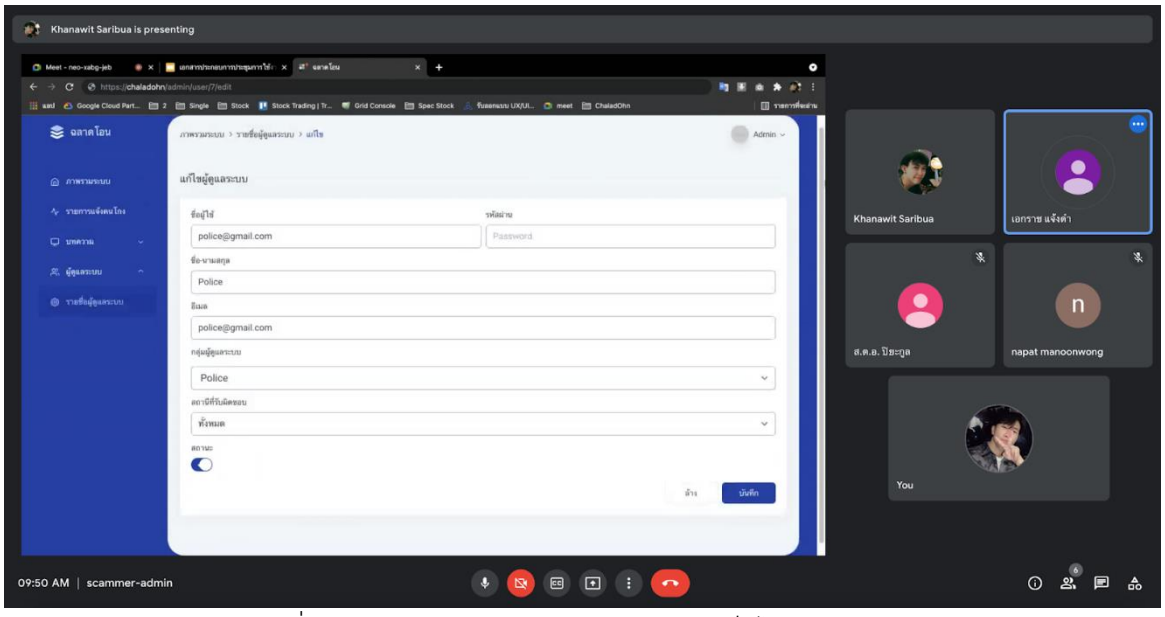
1.2.2 การอบรมผู้ดูแลระบบ



รูปที่ 6 อธิบายหน้าสรุปรายงานแจ้งคนโกงจากผู้ใช้งาน



รูปที่ 7 อธิบายการจัดการบทความบนเว็บไซต์ฉลาดโอน



รูปที่ 8 อธิบายหน้าการจัดการผู้ใช้งานของเว็บไซต์ฉลาดโอน

การจัดตั้งทีมงานสนับสนุนทางเทคนิค

ทางคณะผู้วิจัยฯ จะจัดให้มีเจ้าหน้าที่ผู้มีความรู้และประสบการณ์ทางเทคนิคในการแก้ไขปัญหาอันเกี่ยวกับการใช้งานระบบต้นแบบเพื่อสนับสนุนงานป้องกันและปราบปรามมิจฉาชีพออนไลน์ที่ไม่ระบุตัวตน ทั้งทางเว็บไซต์และตู้คีออส เพื่อรองรับการให้บริการพนักงานสอบสวน จำนวน 2 คนในวันและเวลาทำการ เตรียมความพร้อมในกรณีที่มีเห็นที่ต้องแก้ไขปัญหาเร่งด่วน ในวันเวลาราชการ ตั้งแต่เวลา 09.00 น. ถึง 18.00 น. ระยะเวลา 12 เดือน ตั้งแต่วันที่ 24 มีนาคม 2565 ถึงวันที่ 23 มีนาคม 2566 โดยแบ่งระดับปัญหาออกเป็น 3 ระดับ ดังนี้

- ระดับที่ 1 (Tier 1) ตอบคำถามทั่วไปเกี่ยวกับระบบฉลาดโอนและการให้บริการ
- ระดับที่ 2 (Tier 2) ตอบคำถามเกี่ยวกับการใช้งานและปัญหาทางเทคนิค
- ระดับที่ 3 (Tier 3) ตอบคำถามเกี่ยวกับปัญหาทางเทคนิคเชิงลึก และปัญหาที่ซับซ้อน

รายชื่อเจ้าหน้าที่สนับสนุนทางเทคนิค

ชื่อ – นามสกุล	**เบอร์โทรศัพท์**
นางสาวพรรษา กล่ำกล่อมจิตต์	0614890131
นายสมภพ บัวภารังษี	0614890132

นอกจากนี้ ยังมีเจ้าหน้าที่ที่ให้บริการ และความช่วยเหลือประชาชนจากช่องทาง LINE Official Account “ฉลาดโอน.com” โดยให้บริการทุกวัน ตั้งแต่เวลา 09.00 น. ถึง 18.00 น. ระยะเวลา 12 เดือน ตั้งแต่วันที่ 24 มีนาคม 2565 ถึงวันที่ 23 มีนาคม 2566

ตัวชี้วัดความสำเร็จ

ภาคผนวกในส่วนนี้จะอธิบายเกี่ยวกับผลลัพธ์การดำเนินโครงการ โดยอ้างอิงจากตัวชี้วัดระดับผลลัพธ์ตามที่ได้มีการกล่าวไว้ ซึ่งได้มีการกำหนดตัวชี้วัดความสำเร็จระดับผลลัพธ์ไว้ทั้งสิ้น 3 ข้อ ดังนี้

1. พนักงานสอบสวนในเขตพื้นที่ศึกษา สามารถรวบรวมหลักฐานเพื่อดำเนินคดีกับผู้ถูกกล่าวหาในชั้นศาลเพิ่มขึ้น ในอัตราร้อยละ 50

จากการดำเนินโครงการ และเปิดตัวเว็บไซต์ฉลาดโอนอย่างเป็นทางการ เมื่อวันที่ 2 กุมภาพันธ์ 2565 จนถึงวันที่ 28 กุมภาพันธ์ 2565 รวมระยะเวลาทั้งสิ้น 25 วัน เว็บไซต์ฉลาดได้ช่วยรวมเอกสารหลักฐานในรูปแบบไฟล์ PDF เพื่อให้ประชาชนนำไปประกอบการแจ้งความดำคดีต่อเจ้าพนักงานสอบสวน ในพื้นที่ศึกษา โดยแสดงผลการดำเนินงาน ดังตารางที่ 1

ตารางที่ 1 ตารางแสดงผลจำนวนคดีที่พนักงานสอบสวนในเขตพื้นที่ศึกษา สามารถรวบรวมหลักฐานเพื่อดำเนินคดีกับผู้ถูกกล่าวหาในชั้นศาล

รายการ	**จำนวนเคส**		
	ม.ค. 65	**ก.พ. 65**	
	ตำรวจ	**ตำรวจ**	**ฉลาดโอน**
จำนวนคดีที่พนักงานสอบสวนในเขตพื้นที่ศึกษา สามารถรวบรวมหลักฐานเพื่อดำเนินคดีกับผู้ถูกกล่าวหาในชั้นศาล	29	13	3

นอกจากการที่เว็บไซต์ฉลาดโอนได้มีการช่วยรวมเอกสารหลักฐานให้กับประชาชนในพื้นที่ศึกษาแล้ว ยังมีการรวบรวมเอกสารเพื่อประกอบการดำเนินคดีนอกพื้นที่ศึกษาอีกเช่นกัน โดยแสดงผลการดำเนินงาน ดังตารางที่ 2

ตารางที่ 2 ตารางแสดงผลจำนวนการช่วยรวบรวมหลักฐานนอกพื้นที่ศึกษา

รายการ	**จำนวนเคส**	
	ก.พ. 65	**มี.ค. 65**
ผลการช่วยรวบรวมหลักฐานนอกพื้นที่	105	53

2. จำนวนคดีมิจฉาชีพธุรกรรมออนไลน์ที่ไม่สามารถระบุตัวตนผู้ถูกกล่าวหาได้ในเขตพื้นที่ศึกษาลดลง ในอัตราร้อยละ 50

นอกจากนี้จากกการดำเนินโครงการ ตลอดระยะที่ได้มีการเปิดตัวเว็บไซต์ฉลาดโอน จำนวนคดีที่ไม่สามารถระบุตัวตนของผู้ถูกกล่าวหาทั้งในเขตพื้นที่และนอกเขตพื้นที่ยังลดลงอีกด้วย โดยแสดงผลการดำเนินงาน ดังตารางที่ 3 และตารางที่ 4

ตารางที่ 3 ตารางแสดงผลจำนวนคดีมิจฉาชีพธุรกรรมออนไลน์ที่ไม่สามารถระบุตัวตนผู้ถูกกล่าวหาได้ในเขตพื้นที่ศึกษา

รายการ	**จำนวนเคส**		
	ม.ค. 65	**ก.พ. 65**	
	ตำรวจ	**ตำรวจ**	**ฉลาดโอน**
จำนวนคดีมิจฉาชีพธุรกรรมออนไลน์ที่ไม่สามารถระบุตัวตนผู้ถูกกล่าวหาได้ในเขตพื้นที่	3	1	0

ตารางที่ 4 ตารางแสดงผลจำนวนคดีมิจฉาชีพธุรกรรมออนไลน์ที่ไม่สามารถระบุตัวตนผู้ถูกกล่าวหาได้นอกเขตพื้นที่ศึกษา

รายการ	จำนวนเคส	
	ก.พ. 65	มี.ค. 65
ผู้ถูกกล่าวหาที่ไม่สามารถระบุตัวตน	16	6

3. มีผู้ซื้อสินค้าออนไลน์ลงทะเบียนในระบบยืนยันตัวตนไม่น้อยกว่า 5,000 คน และไม่น้อยกว่า 20,000 ครั้ง

จากการดำเนินโครงการตลอดระยะเวลาที่ผ่านมา ได้มีผู้สนใจลงทะเบียนและยืนยันตัวตนกับระบบฉลาดโอน ทั้งสิ้น 5,136 คน โดยแบ่งรูปแบบการลงทะเบียนและยืนยันตัวตน ออกเป็น 5 รูปแบบ ดังตารางที่ 5 ซึ่งถือว่าจากระยะเวลาที่ได้มีการเปิดตัวเว็บไซต์ฉลาดโอนค่อนข้างได้รับผลตอบรับที่ดีจากประชาชน นอกจากสถิติการลงทะเบียนยืนยันตัวตนแล้ว ผลตอบรับในการใช้งานเว็บไซต์ฉลาดโอนยังมีสถิติมากกว่า 119,000 ครั้ง โดยแสดงรายละเอียด ดังตารางที่ 6

ตารางที่ 5 ตารางแสดงผลจำนวนการลงทะเบียนและยืนยันตัวตนในระบบฉลาดโอน

การลงทะเบียนและยืนยันตัวตน	**จำนวน (คน)**
บัญชีไลน์	3,900
เลขหมายโทรศัพท์	1,073
เลขหมายโทรศัพท์ + บัตรประชาชน	177
เลขหมายโทรศัพท์ + บัตรประชาชน + ภาพถ่ายใบหน้า	149
เลขหมายโทรศัพท์ + บัตรประชาชน + ภาพถ่ายใบหน้า + บัญชีธนาคาร	93
รวม	5,136

ตารางที่ 6 ตารางแสดงผลจำนวนการเข้าใช้งานเว็บไซต์ฉลาดโอนในฟังก์ชันต่าง ๆ ตั้งแต่วันที่ 1 กุมภาพันธ์ 2565 – 20 มีนาคม 2565

รายการ	**จำนวน (ครั้ง)**
การเช็กคนโกง	119,190
การเช็กตัวตน	161
การแจ้งคนโกง	290
การช่วยรวมหลักฐาน	161
รวม	119,802

รายงานผลการดำเนินงานฉบับย่อสำหรับตีพิมพ์ในวารสารสำนักงาน กสทช.

1. บทนำ

ด้วยความก้าวหน้าของเทคโนโลยีการสื่อสารและเทคโนโลยีอินเทอร์เน็ต ผนวกกับสถานการณ์การระบาดของเชื้อไวรัสโคโรน่าสายพันธุ์ใหม่ (COVID-19) จึงมีผลทำให้ธุรกรรมออนไลน์ ซึ่งครอบคลุมถึงการสั่งซื้อสินค้าต่าง ๆ ที่ไม่เว้นแม้แต่อาหาร ผ่านสื่อสังคมออนไลน์และแอปพลิเคชันต่าง ๆ ซึ่งรวมทั้งแอปพลิเคชันของธนาคาร เติบโตขึ้นเป็นอย่างมาก อย่างไรก็ตาม แม้ว่าความก้าวหน้าทางเทคโนโลยีสารสนเทศและการสื่อสารโทรคมนาคมจะช่วยเพิ่มความสะดวกสบายให้กับผู้ใช้บริการ แต่ก็แฝงไปด้วยภัยคุกคามจากผู้ไม่ประสงค์ดีที่อาศัยช่องโหว่ ทั้งจากคน ระบบ และกระบวนการ ตลอดจนข้อกฎหมายที่ยังมีจุดอ่อน และยังต้องการการพัฒนาให้เท่าทันเทคโนโลยีที่พัฒนาไปอย่างรวดเร็ว โลกอินเทอร์เน็ตจึงกลายเป็นช่องทางให้มิจฉาชีพแอบแฝงเข้ามาหาผลประโยชน์ด้วยกลโกงรูปแบบต่าง ๆ โดยมิจฉาชีพบางส่วนใช้การเปลี่ยนเลขหมายโทรศัพท์มือถือที่เป็นแบบเติมเงินไปเรื่อย ๆ และใช้เครือข่ายอินเทอร์เน็ตสาธารณะเป็นเครื่องมือหลักในการกระทำความผิดเพื่อหลอกเหยื่อซึ่งอาจเป็นผู้ซื้อหรือผู้ขายที่ไม่ได้ทำการตรวจสอบตัวตนจริงของบุคคลที่ทำธุรกรรมด้วยอย่างละเอียดถี่ถ้วน

ด้วยเหตุนี้ กองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมเพื่อประโยชน์สาธารณะ (กทปส.) สำนักงาน กสทช. จึงได้มีประกาศรับคัดเลือกผู้ขอรับการส่งเสริมสนับสนุนจากเงินกองทุน กทปส. เพื่อดำเนินโครงการจัดทำแนวทางพัฒนาระบบต้นแบบเพื่อสนับสนุนงานป้องกันและปราบปรามมิจฉาชีพออนไลน์ที่ไม่สามารถระบุตัวตน และศึกษาระบบการติดตาม ป้องกันต่อต้านการกระทำความผิดทางธุรกรรมการเงินผ่านช่องทางออนไลน์ หรือการทุจริตทางการเงินจากทั้งในและต่างประเทศเพื่อพัฒนาเป็นต้นแบบในการติดตามหาผู้กระทำความผิดมาดำเนินคดี และได้คัดเลือกให้คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนลีราชมงคลพระนคร ซึ่งร่วมกับกองกำกับการสืบสวน กองบังคับการตำรวจนครบาล 8 เป็นผู้ดำเนินโครงการ ซึ่งโครงการนี้มีวัตถุประสงค์คือ เพื่อศึกษา ออกแบบและพัฒนาระบบต้นแบบสำหรับป้องกันและปราบปรามมิจฉาชีพแบบออนไลน์สำหรับพนักงานสอบสวนและประชาชน โดยมีการศึกษาทบทวนระบบที่เกี่ยวข้องเพื่อลดความซ้ำซ้อน และทบทวนงานวิจัยที่เกี่ยวข้อง และมีการบูรณาการความร่วมมือกับหน่วยงานหรือเจ้าหน้าที่ที่เกี่ยวข้อง เช่น สำนักงานตำรวจแห่งชาติ ธนาคาร เป็นต้น โดยมีการจัดประชุมเสวนาเพื่อแลกเปลี่ยนความคิดเห็นและข้อมูลระหว่างคณะผู้วิจัยและตัวแทนหน่วยงานที่เกี่ยวข้อง ทั้งก่อนและหลังการออกแบบและพัฒนาระบบต้นแบบ

2. ทฤษฎีที่เกี่ยวข้อง

2.1 การกระทำความผิดฐานฉ้อโกง

การกระทำความผิดฐานฉ้อโกงนั้นก็คือการหลอกลวงคนอื่นด้วยการแสดงข้อความอันเป็นเท็จหรือปกปิดความจริงที่ควรบอก ซึ่งเป็นการกระทำโดยทุจริต และการหลอกลวงทำให้ได้ทรัพย์สินไปจากผู้ถูกหลอกลวงหรือคนอื่น ๆ หรือทำให้ผู้ถูกหลอกลวงหรือคนอื่นต้องทำ ถอนหรือทำลายเอกสารสิทธิ ต้องระวางโทษจำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 6,000 บาท หรือทั้งจำทั้งปรับ ซึ่งในปัจจุบันส่วนมากจะเป็นความผิดฐานฉ้อโกงแบบนี้ ซึ่งการฉ้อโกงนั้นมีหลายลักษณะ เช่น การฉ้อโกงประชาชน การฉ้อโกงแรงงาน การหลอกกินอาหารและเครื่องดื่มฟรี เป็นต้น สามารถแบ่งได้ตามประมวลกฎหมายอาญา มาตรา 341 – 348 (สถาบันนิติธรรมาลัย, 2564) ทั้งนี้ความผิดฐานฉ้อโกง ถือเป็นความผิดที่ยอมความกันได้ ซึ่งหมายถึงผู้เสียหายและผู้กระทำความผิด สามารถเจรจา คืนทรัพย์สิน หรือชำระค่าเสียหายเพื่อยุติคดี แต่ยกเว้น "ความผิดฐานฉ้อโกงประชาชน" ผู้เสียหายต้องดำเนินการแจ้งความ หรือฟ้องคดีภายในเวลา 3 เดือน

นับตั้งแต่ทราบเรื่องและรู้ตัว ผู้กระทำผิด ไม่เช่นนั้น คดีจะขาดอายุความ อย่างไรก็ตาม ความผิดฐานฉ้อโกงตามประมวลกฎหมายอาญา มาตรา 341 – 348 ถือเป็นความผิดที่ยอมความกันได้ ซึ่งหมายถึง ผู้เสียหายและผู้กระทำความผิด สามารถเจรจา คืนทรัพย์สิน หรือชำระค่าเสียหายเพื่อยุติคดี แต่ยกเว้น "ความผิดฐานฉ้อโกงประชาชน" ผู้เสียหายต้องดำเนินการแจ้งความ หรือฟ้องคดีภายในเวลา 3 เดือน นับตั้งแต่ทราบเรื่องและรู้ตัว ผู้กระทำผิด ไม่เช่นนั้นคดีจะขาดอายุความ

นอกจากนี้ การกระทำความผิดในรูปแบบการฉ้อโกงออนไลน์ ยังสามารถเชื่อมโยงไปยังความผิดอื่น ๆ ที่ถูกประกาศไว้ใน พระราชบัญญัติอื่น ๆ ได้อีกด้วย เช่น พ.ร.บ.คอมพิวเตอร์ - พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 (ราชกิจจานุเบกษา, 2560) (มีมาตราที่เกี่ยวข้อง ได้แก่ มาตรา 5-8 และ 14) พ.ร.บ. คอมพิวเตอร์ - พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 พ.ร.บ. เงินกู้ – พระราชกำหนดการกู้ยืมเงินที่เป็นการฉ้อโกงประชาชน พ.ศ. 2527 (มาตรา 4) เป็นต้น (ปุณิกา และ ปริยานุช, 2560) และพ.ร.บ. ลิขสิทธิ์ - พระราชบัญญัติลิขสิทธิ์ (ฉบับที่ 3) พ.ศ. 2558 (มาตรา 31) เป็นต้น (Wichianlaw, 2561)

2.2 ประเภทของการฉ้อโกง

รูปแบบการฉ้อโกงในยุคปัจจุบันอาจแบ่งได้เป็นหลายรูปแบบ อย่างไรก็ตามในรายงานฉบับย่อนี้ แบ่งออกเป็น 8 รูปแบบ ดังนี้

1) การฉ้อโกงโดยหลอกลวงให้ร่วมลงทุนในลักษณะแชร์ลูกโซ่
2) การฉ้อโกงโดยหลอกลวงให้ทำรายการที่ตู้เอทีเอ็ม
3) การฉ้อโกงโดยส่งอีเมล์มาทำความรู้จักคุ้นเคยและหลอกลวงให้โอนเงินเข้าบัญชี
4) การฉ้อโกงโดยปลอมตัวและปลอมที่อยู่อีเมล์มาหลอกลวงให้โอนเงินผิดบัญชี
5) การฉ้อโกงโดยอ้างการรักษาพยาบาลมาหลอกลวงเอาเงิน
6) การฉ้อโกงโดยอ้างการเรี่ยไรเงินไปช่วยเหลือทางราชการหรือผู้ด้อยโอกาส
7) การฉ้อโกงโดยใช้ศาสนาเป็นเครื่องมือในการหลอกลวง
8) การฉ้อโกงโดยอ้างว่าเป็นเจ้าหน้าที่ในกระบวนการยุติธรรมและหลอกลวงเอาเงิน

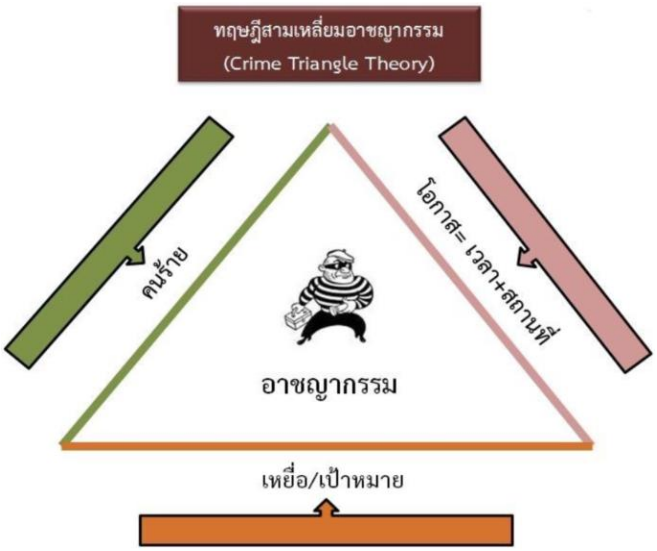
สำหรับกรณีของการฉ้อโกงออนไลน์ ผ่านทางสื่อสังคมออนไลน์สามารถแบ่งออกเป็นรูปแบบที่แตกต่างกันได้ดังนี้

1) การหลอกลวงขายสินค้าในรูปแบบต่าง ๆ โดยมีเจตนาทุจริตที่จะไม่ขายสินค้าจริงๆ หรือไม่มีสินค้าอยู่จริง โดยนำภาพสินค้าของคนอื่นมาลงโพสต์เพื่อขายให้เหยื่อหลงเชื่อ
2) การหลอกลวงขายสินค้าที่ลงโพสต์ไว้ว่าเป็นของแท้แต่ส่งของเลียนแบบหรือของปลอม หรือของคนละประเภทกับที่โพสต์ขาย
3) การหลอกลวงว่าจะให้กู้ยืมเงินในอัตราดอกเบี้ยต่ำ โดยให้ผู้เสียหาย โอนเงินค่าธรรมเนียม หรือค่าดอกเบี้ยงวดแรก หรือค่ามัดจำ เป็นต้น
4) การหลอกลวงด้วยการตีสนิทเข้ามาจีบ (ส่วนใหญ่ใช้รูปโปรไฟล์ ชาวต่างชาติหน้าตาดีสวย เท่ห์) และหลอกว่าจะส่งของมาให้ จากนั้นจะมีผู้ร่วมขบวนการโทรมาติดต่อหลอกว่าเป็นพนักงานบริษัทขนส่งให้โอนค่าธรรมเนียมเพื่อดำเนินการนำพัสดุออกจากด่านศุลกากร โดยส่วนมากจะอ้างว่ามีเงินสดจำนวนมากอยู่ในพัสดุดังกล่าว
5) การหลอกลวงด้วยการแฮกข้อมูลสื่อสังคมออนไลน์ของผู้อื่น โดยที่เจ้าของข้อมูลไม่ได้อนุญาต และทำการหลอกลวงของยืมเงินจากผู้อื่นที่เกี่ยวข้องกับสื่อสังคมออนไลน์นั้น ๆ

2.3 ทฤษฎีป้องกันอาชญากรรม

ทฤษฎีหนึ่งที่ใช้ในการแก้ไขปัญหาอาชญากรรมให้บรรลุเป้าหมาย เรียกว่าทฤษฎีสามเหลี่ยมอาชญากรรม (Crime Triangle Theory) ทฤษฎีนี้ได้อธิบายถึงสาเหตุหรือองค์ประกอบของการเกิดอาชญากรรม ประกอบด้วยด้านต่าง ๆ ของสามเหลี่ยม 3 ด้าน (สุรพงษ์ ชัยจันทร์, 2561) ดังรูปที่ 1 ซึ่งประกอบด้วย

1) ผู้กระทำผิด/คนร้าย หมายถึง ผู้ที่มีความต้องการจะก่อเหตุหรือลงมือกระทำความผิด
2) เหยื่อ/เป้าหมาย หมายถึง บุคคล สถานที่ หรือวัตถุสิ่งของ ที่ผู้กระทำผิดหรือคนร้ายมุ่งหมายกระทำต่อเป้าหมายที่ต้องการ
3) โอกาส หมายถึง ช่วงเวลา และสถานที่ที่เหมาะสมที่ผู้กระผิดหรือคนร้าย สามารถจะลงมือกระทำความผิดหรือก่ออาชญากรรม



รูปที่ 2-1 ทฤษฎีสามเหลี่ยมอาชญากรรม (สุรพงษ์ ชัยจันทร์, 2561)

เมื่อเหตุการณ์หรือสถานการณ์ครบองค์ประกอบทั้ง 3 ด้าน จะทำให้เกิดอาชญากรรมขึ้น อย่างไรก็ตาม เพื่อลดหรือแก้ไขปัญหาอาชญากรรม สามารถทำให้องค์ประกอบการเกิดอาชญากรรมด้านใดด้านหนึ่งหายไปได้ มีดังนี้

1) ด้านผู้กระทำผิดหรือคนร้าย ต้องพยายามลดหรือควบคุมจำนวนผู้กระทำความผิด หรือคนร้ายในพื้นที่ที่รับผิดชอบ โดยมุ่งเน้นใช้ทฤษฎีบังคับใช้กฎหมาย เช่น การเฝ้าระวังบุคคลพ้นโทษที่เข้ามาอยู่ในพื้นที่ การกำหนดมาตรการควบคุมแหล่งอบายมุขหรือสถานบริการ การระดมกวาดล้างอาชญากรรมอย่างสม่ำเสมอ และการจับกุมผู้กระทำความผิดตามหมายจับ เป็นต้น รวมทั้งการประสานงานกับหน่วยงานที่เกี่ยวข้อง เพื่อร่วมกันแก้ไขปัญหายาเสพติดให้โทษ และปัญหาการว่างงาน เป็นต้น

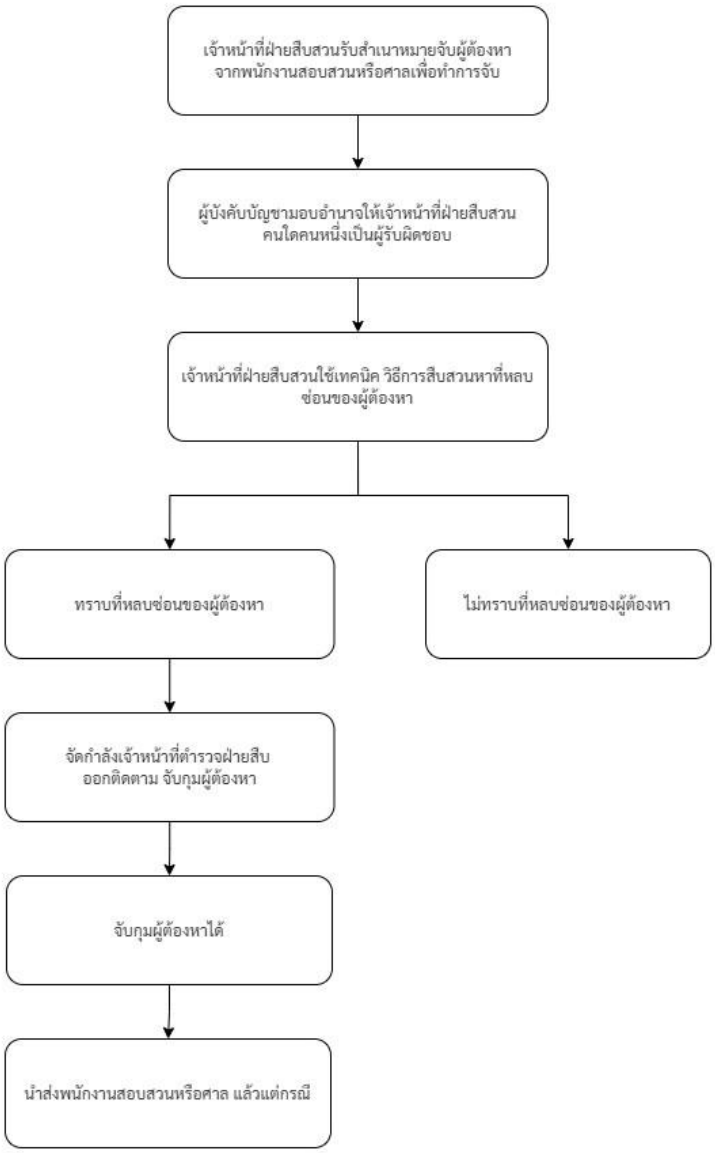
2) ด้านเหยื่อหรือเป้าหมาย ผู้เสียหายหรือเหยื่อ ซึ่งมักจะหมายถึงประชาชนทั่วไปต้องรู้จักการป้องกันตนเอง ครอบครัว และชุมชนหรือสังคม ตำรวจจะต้องเข้าไปช่วยเหลือประชาชนในพื้นที่ โดยมีการประชาสัมพันธ์ให้ความรู้ ข้อมูลข่าวสารที่เป็นประโยชน์ต่อการป้องกันอาชญากรรม หรือไม่ให้ตกเป็นเหยื่ออาชญากรรม เช่น การแต่งตัว การใส่เครื่องประดับหรือของที่มีค่า การหลอกลวงของคนร้ายในลักษณะต่าง ๆ เป็นต้น

3) ด้านโอกาส ที่ผู้กระทำความผิดหรือคนร้ายจะลงมือก่ออาชญากรรมนั้นจะต้องอาศัย เวลาและสถานที่ที่เหมาะสมในการก่อเหตุ จึงต้องพยายามหาวิธีการเพื่อที่จะตัดช่องโอกาสของคนร้าย โดยแยกย่อยได้ดังดังนี้

- เวลา ต้องพยายามตัดช่องโอกาสในเรื่องเวลาที่จะเกิดเหตุ โดยมุ่งเน้นการปรากฏตัวของเจ้าหน้าที่ตำรวจสายตรวจ การตั้งจุดตรวจค้น เป็นต้น
- สถานที่ สำหรับเรื่องการตัดช่องโอกาสในเรื่องสถานที่นั้น สามารถกระทำได้หลายวิธี เช่น วิธีการปรับสภาพแวดล้อมและใช้ประโยชน์สภาพแวดล้อมในการลดโอกาสการก่ออาชญากรรม การจัดการพื้นที่ให้ปลอดภัย และการเพิ่มประสิทธิภาพเครื่องมือเครื่องใช้ทางเทคโนโลยีใหม่ ๆ

2.4 แนวคิดการติดตามจับกุมผู้ต้องหา

คณะผู้วิจัยได้ทำการศึกษาเกี่ยวกับกระบวนการสืบสวนจับกุมผู้ต้องหาตามหมายจับของเจ้าหน้าที่ฝ่ายสืบสวนเพื่อนำส่งให้พนักงานสอบสวนหรือศาล แล้วสรุปได้เป็นแผนภาพได้ดังรูปที่ 2



รูปที่ 2 ขั้นตอนการสืบสวนจับกุมผู้ต้องหาตามหมายจับของเจ้าหน้าที่ฝ่ายสืบสวน

2.4 การทบทวนระบบที่เกี่ยวข้อง

2.4.1 ระบบสารสนเทศข้อมูลอาชญากรรมสำนักงานตำรวจแห่งชาติ (CRIMES)

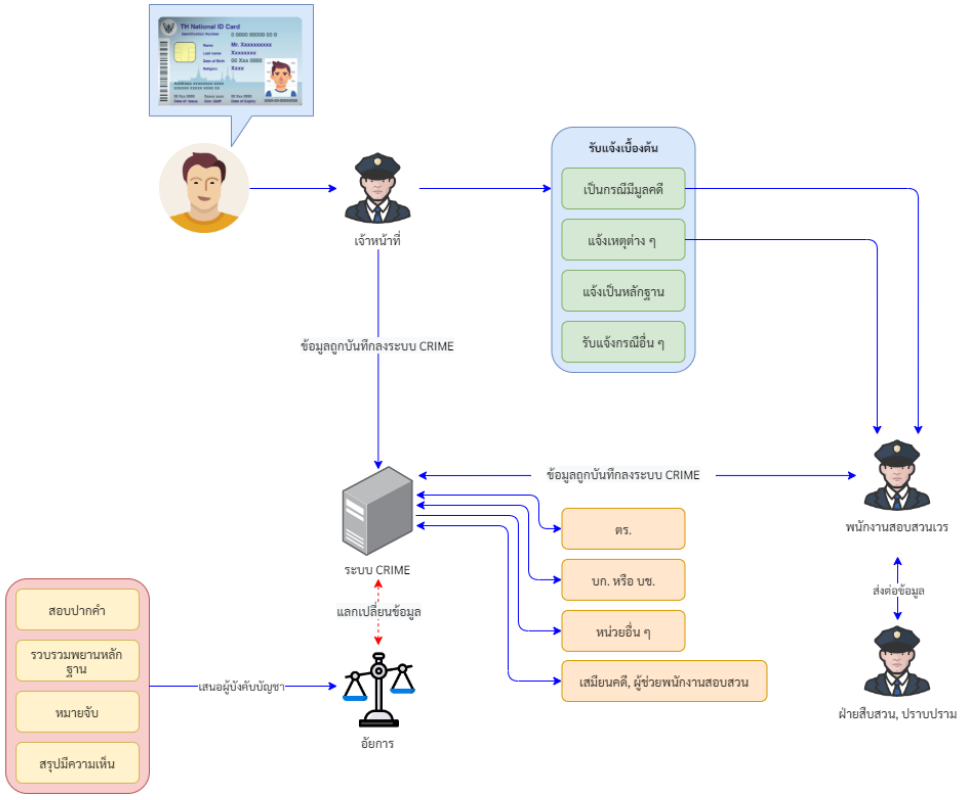
ระบบ CRIMES เป็นแหล่งรวบรวมข้อมูล ทั้งในด้านงานสอบสวน งานป้องกันปราบปราม งานจราจร รวมไปทั้งเป็นจุดศูนย์กลางสู่การเชื่อมต่อไปยังฐานข้อมูลของหน่วยงานอื่น ทั้งในส่วนของสำนักงานตำรวจแห่งชาติเอง หรือหน่วยงานภายนอก เป็นเครื่องมือช่วยในการสืบสวน อำนวย

ความยุติธรรม ดำรงความถูกต้องของข้อมูล อำนวยความสะดวกให้กับเจ้าหน้าที่ผู้ปฏิบัติงานโดยเฉพาะงานระดับสถานีตำรวจ ลดขั้นตอนการบันทึกข้อมูลสนับสนุนงานต่าง ๆ ช่วยให้ประชาชนที่มาติดต่อได้รับการอำนวยความสะดวกและความยุติธรรมได้อย่างโปร่งใสและรวดเร็ว

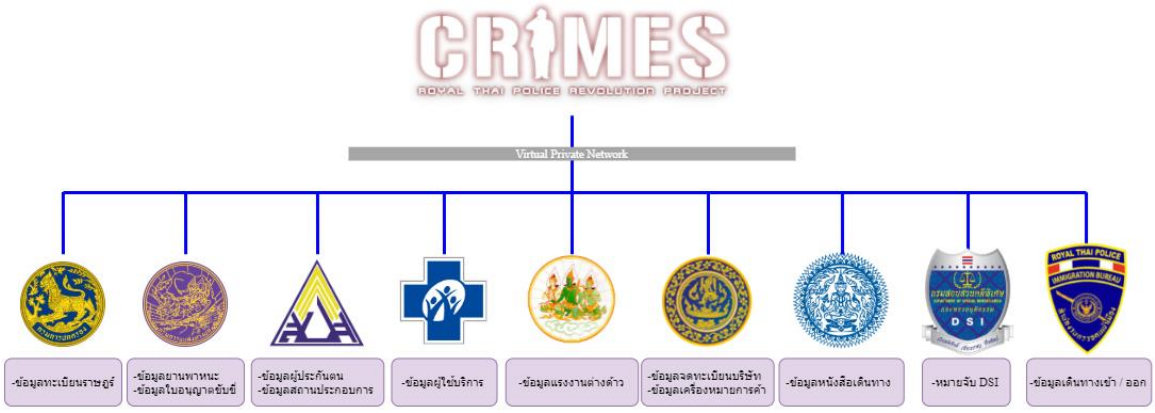
ระบบ CRIMES ถูกออกแบบให้มีการทำงานดังรูปที่ 3 กล่าวคือเมื่อประชาชนมาแจ้งความร้องทุกข์ที่สถานีตำรวจ เจ้าหน้าที่ตำรวจเวรประชาสัมพันธ์ จะสอบถามและบันทึกข้อมูลเบื้องต้นในระบบคอมพิวเตอร์ เพื่อคัดกรองเรื่อง และแนะนำให้ผู้มาแจ้งความร้องทุกข์ไปพบพนักงานสอบสวน ข้อมูลเบื้องต้นจะถูกส่งผ่านระบบคอมพิวเตอร์ ไปยังพนักงานสอบสวนเพื่อสืบค้นข้อมูล และบันทึกข้อมูลในชั้นการพิจารณาของพนักงานสอบสวน และข้อมูลจะถูกส่งผ่านระบบต่อไปยังฝ่ายสืบสวนป้องกันปราบปราม ซึ่งจะมีการเชื่อมโยงระบบกับหน่วยงานอื่นๆ เช่น การเชื่อมต่อขอข้อมูลบุคคลจากทะเบียนราษฎร์ ทะเบียนประวัติอาชญากร และข้อมูลประกันสังคม เป็นต้น ดังรูปที่ 4 (มนตรี สีทอง, 2564)

2.4.2 ศูนย์รับเรื่องร้องเรียนปัญหาออนไลน์ 1212 OCC

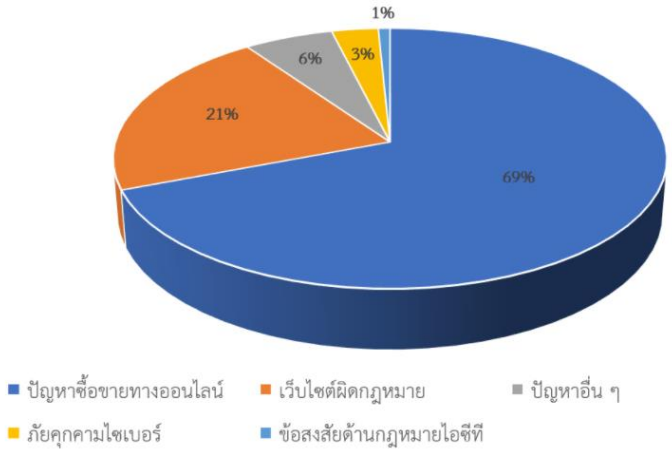
ศูนย์รับเรื่องร้องเรียนปัญหาออนไลน์ 1212 Online Complaint Center หรือ 1212 OCC เป็นหนึ่งในโครงการ “SMEs go online ซื้อขายมั่นใจ มีปัญหาเมื่อไร เราดูแล” ดำเนินการภายใต้โครงการขับเคลื่อนเศรษฐกิจและสังคมดิจิทัล ที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม มอบหมายให้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ดำเนินการ จัดตั้งขึ้นเพื่อเป็นศูนย์กลางการรับเรื่องร้องเรียนปัญหาที่เกิดจากการซื้อขายทางออนไลน์ การกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ รวมถึงการกระทำความผิดทางเทคโนโลยีสารสนเทศ ภัยคุกคามทางไซเบอร์ ตลอดจนปัญหาทางออนไลน์อื่นๆ ที่เกี่ยวข้อง ให้แก่ผู้บริโภคหรือผู้ประกอบการทั้งภาครัฐและเอกชน สำหรับภาพรวมการรับเรื่องร้องเรียนผ่าน 1212 OCC ในปี 2564 ที่ผ่านมา มีทั้งสิ้น 54,348 เรื่อง โดยปัญหาที่มีการร้องเรียนมากที่สุดคือ ปัญหาซื้อขายทางออนไลน์ มีจำนวน 37,584 เรื่อง คิดเป็น 69% รองลงมาเป็นปัญหาเว็บไซต์ผิดกฎหมาย มีจำนวน 11,476 เรื่อง คิดเป็น 21% ตามมาด้วย ปัญหาอื่น ๆ และสอบถามข้อสงสัย มีจำนวน 3,200 เรื่อง คิดเป็น 6% ปัญหาภัยคุกคามไซเบอร์ มีจำนวน 1,667 เรื่อง คิดเป็น 3% และข้อสงสัยด้านกฎหมายไอซีที มีจำนวน 421 เรื่อง คิดเป็น 1% ดังแสดงในรูปที่ 5



รูปที่ 3 ขั้นตอนการรับแจ้งความและบันทึกข้อมูลลงบนระบบ CRIMES



รูปที่ 4 การเชื่อมโยงกับหน่วยงานภายนอกของระบบ CRIMES



รูปที่ 5 สัดส่วนเรื่องร้องเรียนผ่าน 1212 OCC

2.4.3 ระบบสารสนเทศอื่นๆ ที่เกี่ยวข้อง

1) ระบบตรวจสอบข้อมูลผู้ลงทะเบียน เป็นระบบของสำนักงาน กสทช. ที่ร่วมกับผู้ให้บริการเครือข่ายโทรศัพท์มือถือ เพื่อใช้ตรวจสอบประวัติผู้เป็นเจ้าของเลขหมายโทรศัพท์เคลื่อนที่

2) ระบบแจ้งอายัดบัญชีธนาคาร เกิดจากความร่วมมือระหว่างสมาคมธนาคารไทย สถาบันเพื่อการยุติธรรมแห่งประเทศไทย และกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี เป็นระบบที่ให้อำนาจตามกฎหมายกับพนักงานสอบสวน ในการอายัดเงินในบัญชีของคนร้ายด้วยการส่งหนังสือโดยใช้วิธีการทางอิเล็กทรอนิกส์ และมีการเข้ารหัสข้อมูลด้วย Public Key และ Private Key เพื่อเพิ่มความปลอดภัยของข้อมูล

3) ระบบตรวจสอบข้อมูลบัตรประชาชนผ่านระบบเว็บเซอร์วิส มีการให้บริการตรวจสอบข้อมูลทะเบียนประวัติบุคคลสัญชาติไทย และบุคคลซึ่งไม่มีสัญชาติไทยจากฐานข้อมูลทะเบียนกลาง โดยการกำกับของกรมการปกครอง กระทรวงมหาดไทย

4) ระบบยื่นคำฟ้องอิเล็กทรอนิกส์สำหรับประชาชน (e-Filing) ศาลยุติธรรมได้ดำเนินการการจัดตั้งแผนกคดีซื้อขายออนไลน์ในศาลแพ่ง และได้มีการเปิดตัวเมื่อวันที่ 27 มกราคม 2565 ซึ่งจะมุ่งส่งเสริมการดำเนินคดีเพื่อยกระดับการคุ้มครองผู้บริโภคให้ครอบคลุมถึงการบริโภควิถีใหม่ เช่น กลุ่มการซื้อขายสินค้าออนไลน์ โดยให้ใช้ระบบศาลอิเล็กทรอนิกส์เต็มรูปแบบในทุกขั้นตอนของกระบวนการพิจารณา เพื่อให้ผู้บริโภคที่คิดว่าจะใช้สิทธิทางศาลฟ้องคดี ได้รับความสะดวก เพื่อยกระดับการให้บริการแก่ประชาชนได้ครอบคลุมและรวดเร็วขึ้น

2.4.4 เว็บไซต์อื่น ๆ

จากการศึกษา ทางคณะผู้วิจัยพบว่า มีหลายเว็บไซต์ที่น่าสนใจและมีความเกี่ยวข้องกับงานวิจัยนี้ ดังนี้

1) เว็บไซต์ VerMe เป็นเว็บไซต์ที่มีการพัฒนามาเป็นแพลตฟอร์มเพื่อใช้ในการยืนยันตัวตนผู้ขายของออนไลน์ตาม Facebook, Line, Instagram, Twitter และเว็บบอร์ดต่าง ๆ เพื่อให้ผู้ซื้อมั่นใจว่าชำระเงินกับคนที่มีตัวตนจริง ๆ โดยผู้ขายจะมี บัตร VerME ในการยืนยันตัวตนว่าเป็นผู้ขายจริงไม่ใช่มิจฉาชีพ ทางฝั่งผู้ซื้อสามารถนำ ID บนบัตร VerME ของผู้ขายไปตรวจสอบได้เพื่อให้เกิดความมั่นใจในการซื้อขายกัน (Verme, 2565)

2) เว็บไซต์ Blacklistseller เป็นเว็บไซต์ที่ร่วมต้านภัยฉ้อโกงออนไลน์โดนผู้เสียหายที่โดนมิจฉาชีพออนไลน์โกงเงินสามารถนำข้อมูลเหล่านั้นมาสร้างเป็นรายงานและฐานข้อมูลเพื่อช่วยในการเตือนสังคมป้องกันไม่ให้มีผู้โดนหลอกเพื่อมากขึ้น (Blacklistseller, 2565)

3) เว็บไซต์เช็คคนโกง เป็นเว็บไซต์เว็บไซต์สำหรับเช็คคนโกง หลอกให้โอนเงินสำหรับการซื้อของออนไลน์ ผู้ใช้ควรเช็คก่อนโอนเงิน ผู้ที่โดนโกงสามารถโพส ใส่ข้อมูลไม่ครบถ้วน เช่น ชื่อ นามสกุล บัญชีที่โอน วันที่โอน หลักฐานการแจ้งความ หรือข้อมูลการแชท ที่ช่วยให้ผู้ซื้อทำการเช็คคนโกงได้ก่อนการโอนเงิน โดยเช็คให้ชัวร์ก่อนโอน เช็คชื่อ เช็คเลขที่บัญชี เช็คเบอร์โทรศัพท์ เช็คทุกอย่างที่ทราบข้อมูล ลองค้นหาใน Google หรือ Facebook แม้กระทั่ง Twitter แล้วนำข้อมูลเหล่านั้นมาเช็คในเว็บคนโกง.com (เช็คคนโกง, 2565)

4) เว็บไซต์ Whoscheat เป็นเว็บไซต์สำหรับตรวจสอบข้อมูลมิจฉาชีออนไลน์เช่นกัน โดยในระบบมีการทำการตรวจสอบเลขบัญชีธนาคารของมิจฉาชีพ เบอร์โทรศัพท์มือถือ เลขประจำตัวประชาชน และชื่อ-นามสกุล ของมิจฉาชีพ เพื่อเป็นการป้องการให้ไม่โดนโกงเช่นกัน (Whoscheat, 2565)

5) เว็บไซต์ pantipmarket เป็นเว็บไซต์สำหรับซื้อขายของออนไลน์ซึ่งการซื้อขายของในหลายสินค้าและหมวดเช่นเดียวกัน ตัวอย่าง ซื้อ-ขายอสังหาริมทรัพย์ ซื้อ-ขายพระเครื่อง ซื้อ-ขายยานพาหนะ ซื้อ-ขายคอมพิวเตอร์ และอื่น ๆ มากมาย ซึ่งนอกจากเว็บไซต์ pantipmarket จะเป็นแพลตฟอร์มจะสร้างพื้นการซื้อ-ขายสินค้าต่าง ๆ ระบบยังมีการสร้างรายการเลขที่บัญชีที่หลอกลวง และรายการสินค้าที่ถูกขโมยด้วย

3. การดำเนินการ

ก่อนที่จะมีการดำเนเนการเกี่ยวกับการออกแบบและพัฒนาระบบ คณะผู้วิจัยได้ดำเนินการจัดประชุมประชุมกับหน่วยงานต่าง ๆ รวมทั้งสรุปผลจากการจัดงานเสวนาวิชาการกลุ่มย่อย (Focus Group) ครั้งที่ 1 ร่วมกับตัวแทนจากหน่วยงานต่าง ๆ ได้แก่ กองกำกับการสืบสวน กองบังคับการตำรวจนครบาล 8 สำนักงานกฎหมายและคดี สำนักงานตำรวจแห่งชาติ กองป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สถาบันเพื่อการยุติธรรมแห่งประเทศไทย บริษัทเอซิสโปรเฟสชั่นนัล เซ็นเตอร์ จำกัด สำนักบริหารและจัดการเลขหมายโทรคมนาคม กสทช. สำนักอนุญาตประกอบกิจการโทรคมนาคม 2 สำนักงาน กสทช. สำนักงานป้องกันและปรามการฟอกเงิน สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ บริษัท บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด บริษัท ดีแทค ไตรเน็ต จำกัด เพื่อระดมแนวคิดสำหรับนำไปประยุกต์ใช้ในการพัฒนาระบบต้นแบบ นอกจากนี้ยังมีการประชุมออนไลน์อีกหลังครั้ง ร่วมกับผู้แทนจากหน่วยงานต่างๆ เช่น เว็บไซต์ Blacklistseller กรมการปกครอง กองบัญชาการตำรวจนครบาล ธนาคารแห่งประเทศไทย และฝ่ายให้คำปรึกษา สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA)

3.1 การออกแบบและพัฒนาระบบต้นแบบ

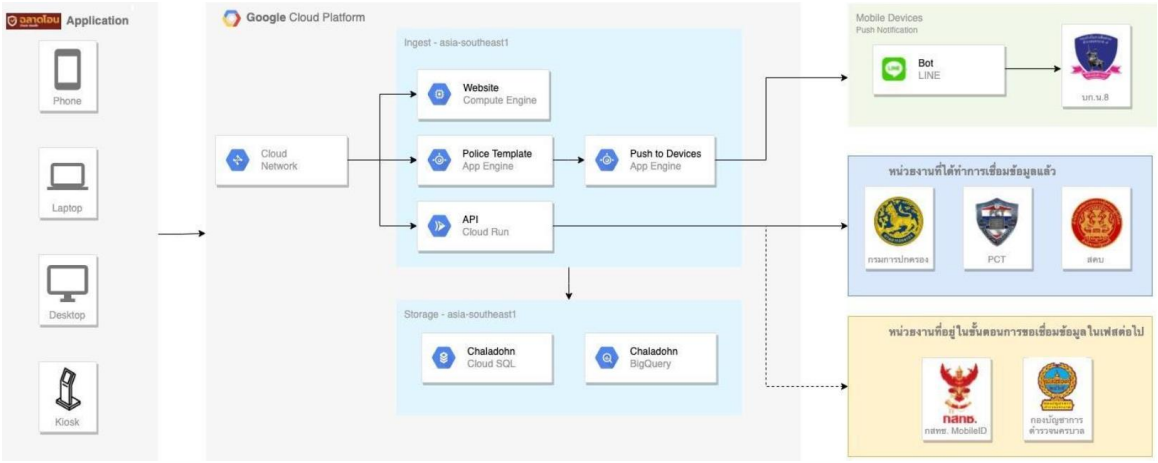
จากการที่ได้ประมวลและวิเคราะห์ข้อมูลที่ได้ทั้งจากการศึกษาทบทวนเกี่ยวกับระบบ งานวิจัยที่เกี่ยวข้อง ระเบียบ ข้อกฎหมาย ขั้นตอนและวิธีการทำงานของตำรวจ ตลอดจนข้อคิดเห็นจากการประชุมเสวนาและการประชุมออนไลน์ คณะผู้วิจัยจึงได้ข้อสรุปเบื้องต้นว่า เพื่อหลีกเลี่ยงประเด็นเรื่องกฎระเบียบและข้อกฎหมายต่างๆ ระบบต้นแบบที่พัฒนาขึ้นจะต้องเป็นระบบที่ทำงานในเชิงป้องกัน จึงเป็นที่มาของการออบแบบและพัฒนาระบบต้นแบบสำหรับการป้องกันและปราบปรามมิจฉาชีพออนไลน์ที่ไม่ระบุตัวตน

(ดังรูปที่ 6-9) อย่างไรก็ตาม เพื่อให้ง่ายต่อการจดจำและการสื่อสารประชาสัมพันธ์ คณะผู้วิจัยจึงได้ตั้งชื่อระบบว่า “ฉลาดโอน” ซึ่งระบบนี้มีส่วนหลักเป็นเว็บไซต์ที่ทำหน้าที่เป็นตัวกลางในการแจ้งข้อมูลการทำธุรกรรมด้วยการโอนเงินที่มีความปลอดภัยโดยผู้ซื้อ (ผู้โอนเงิน) และผู้ขาย (ผู้รับโอน) ที่ผ่านการยืนยันตัวตนแล้ว ตลอดจนเป็นฐานข้อมูลมิจฉาชีพที่มีประวัติหรืออยู่ระหว่างการดำเนินคดีฉ้อโกงในโลกออนไลน์ โดยระบบนี้มุ่งเน้นออกแบบให้เป็นระบบนิเวศสำหรับการร่วมมือของภาคส่วนที่เกี่ยวข้องเพื่อลดปัญหามิจฉาชีพออนไลน์ นอกจากนี้ คณะผู้วิจัยยังได้เปิดช่องทาง LINE Official Account ฉลาดโอน.com ไว้เป็นช่องทางในการสื่อสารระหว่างผู้เสียหายที่มีความประสงค์จะติดต่อขอความช่วยเหลือกับผู้ประสานงานของระบบต้นแบบด้วย

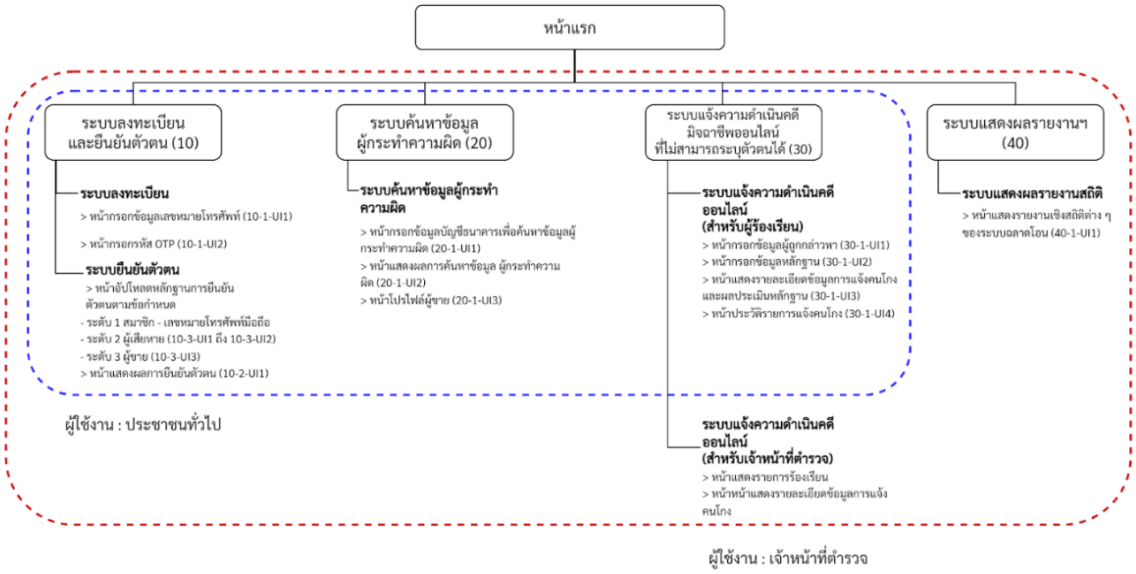
ส่วนหนึ่งของระบบที่ค่อนข้างมีความสำคัญ คือ ระบบการลงทะเบียนและการยืนยันตัวตน เป็นระบบสำหรับให้ผู้ใช้งานสามารถเข้ามาใช้บริการต่าง ๆ อาทิ การตรวจสอบบัญชีผู้กระทำความผิด การตรวจสอบบัญชีผู้ขายที่ยืนยันตัวตน การแจ้งความดำเนินคดีออนไลน์ ตลอดจนการรวบรวมเอกสารหลักฐานประกอบการแจ้งความ ผ่านระบบต้นแบบฯ โดยการใช้งานผู้ใช้งานจำเป็นต้องยืนยันตัวตน เพื่อเป็นการระบุตัวตนว่าด้วยการพิสูจน์และยืนยันตัวตน เพื่อช่วยลดความเสี่ยงจากเหตุการณ์ฉ้อโกงออนไลน์ รวมทั้งสร้างความมั่นใจในความปลอดภัยต่อการทำธุรกรรมให้กับผู้ทำธุรกรรม ทั้งนี้ผู้ใช้งานต้องทำการลงทะเบียนและยืนยันตัวตนก่อน จากนั้นจึงจะสามารถเข้าใช้งานระบบต้นแบบฯ ในส่วนอื่น ๆ ต่อได้ และเพื่อให้สอดคล้องกับข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยมีขั้นตอนการลงทะเบียนและยืนยันตัวตนแสดงดังรูปที่ 10

อย่างไรก็ตาม หลังจากที่ได้มีการออกแบบและพัฒนาระบบต้นแบบ และดำเนินการทดลองให้มีใช้งาน คณะผู้วิจัยได้จัดงานเสวนาวิชาการกลุ่มย่อย (Focus Group) ครั้งที่ 2 ร่วมกับตัวแทนจากหน่วยงานต่าง ๆ ซึ่งในครั้งนี้ ได้ผู้แทนจากธนาคารแห่งประเทศไทย สมาคมธนาคารไทย สมาคมสถาบันการเงินของรัฐ และสำนักงานอัยการจังหวัดเชียงใหม่ และอีกหลายหน่วยงาน เข้าร่วมวิพากษ์ และให้ความคิดเห็นเพื่อให้คณะผู้วิจัยได้นำไปปรับปรุงพัฒนาระบบต้นแบบต่อไปในอนาคต

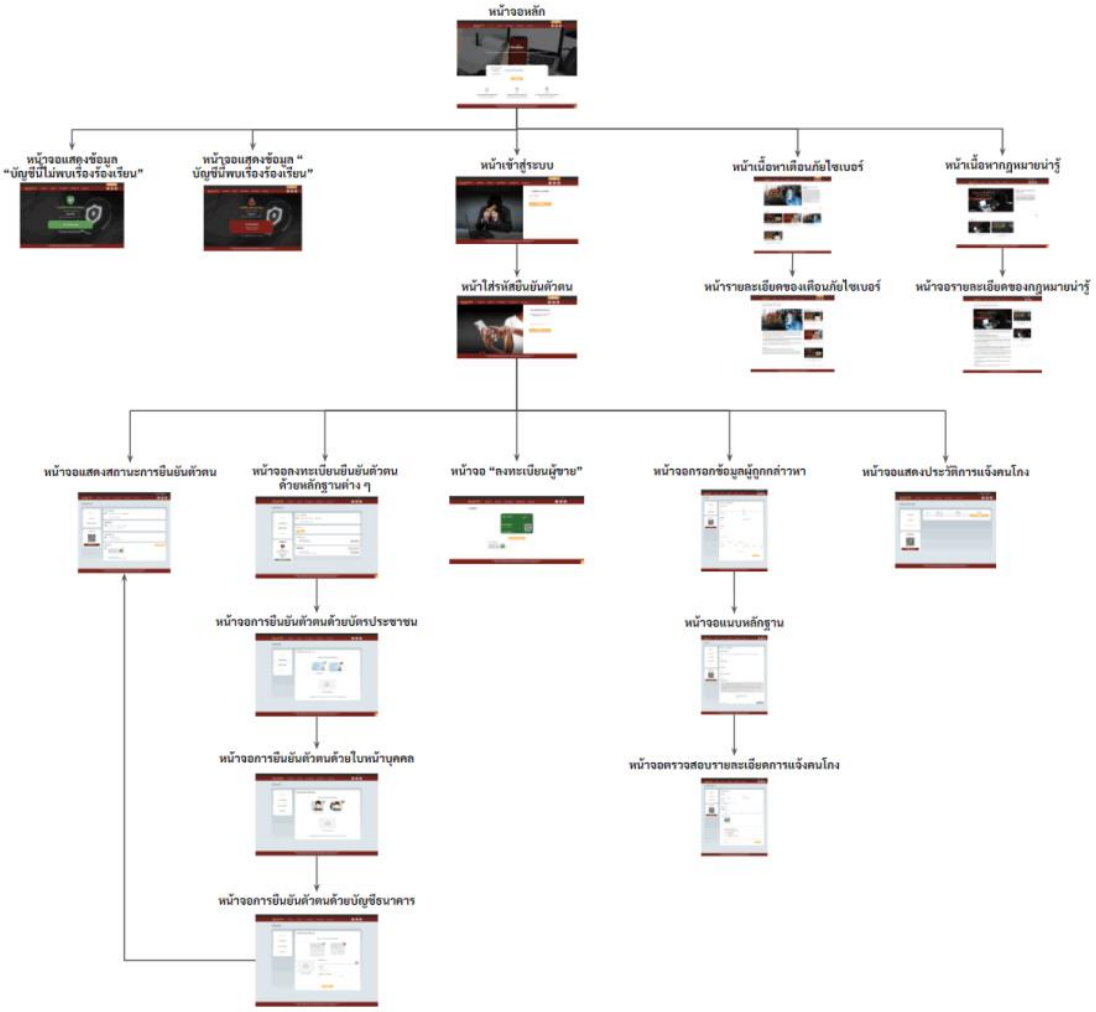
รูปที่ 6 ภาพรวมของระบบต้นแบบ



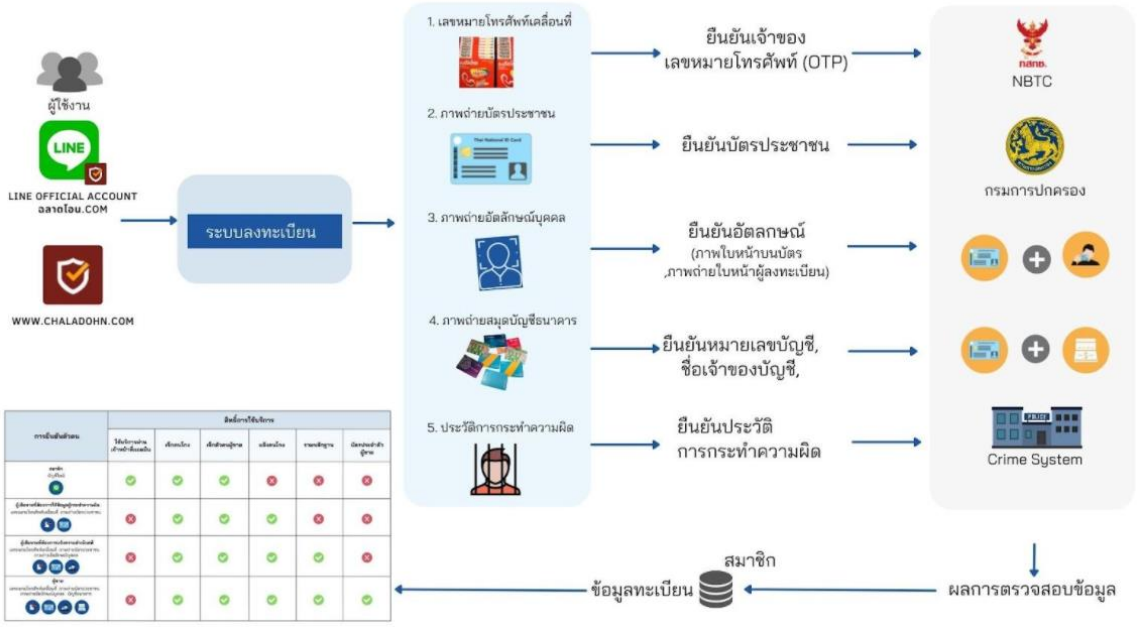
รูปที่ 7 แผนภาพกระแสข้อมูล (Dataflow Diagram) ของระบบต้นแบบ



รูปที่ 8 ภาพแผนผังโครงสร้างข้อมูล (System Sitemap) ของระบบต้นแบบ



รูปที่ 9 ภาพแผนผังโครงสร้างข้อมูล (System Sitemap) ของระบบต้นแบบ



รูปที่ 10 ภาพรวมขั้นตอนการลงทะเบียนและยืนยันตัวตน

3.2 การประชาสัมพันธ์

เพื่อให้มีผู้เข้าถึงและเข้าใช้งานเว็บไซต์ คณะผู้วิจัยได้ดำเนินการประชาสัมพันธ์เว็บไซต์ฉลาดโอน ด้วยการดำเนินการให้ Influencer ซึ่งถือเป็นกลุ่มคนที่มีอิทธิพลต่อความคิดและการตัดสินใจของกลุ่มเป้าหมาย ให้ช่วยทำการประชาสัมพันธ์เว็บไซต์ฉลาดโอนและนำเสนอการใช้งาน รวมถึงการเผยแพร่เรื่องราวเกี่ยวกับเว็บไซต์ฉลาดโอนที่จะเป็นประโยชน์กับผู้ใช้งานอื่น ๆ โดยมีการเผยแพร่ทางช่องยูทูบ เมื่อวันที่ 15 กุมภาพันธ์ 2565 ผ่านลิงก์ (https://www.youtube.com/watch?v=cK0O1jDr1-g) ดังรูปที่ 11 นอกจากนี้ คณะผู้วิจัยได้ดำเนินการจัดทำสื่อวิดีทัศน์อีก 1 รายการ เพื่อแนะนำเว็บไซต์ฉลาดโอนให้กับผู้ใช้งานทั่วไป โดยมีเนื้อหาคลอบคลุมที่มาของฉลาดโอน ฟังก์ชันของระบบฉลาดโอน โดยมีการเผยแพร่ทางช่องยูทูบ เมื่อวันที่ 2 มีนาคม 2565 ผ่านลิงก์ (https://www.youtube.com/watch?v=Gx-BhcKiQEw) ดังรูปที่ 12

นอกจากสื่อวิดีทัศน์ที่ทางคณะผู้วิจัยได้ดำเนินการเพื่อประชาสัมพันธ์แล้ว ยังมีสื่อออนไลน์ต่างๆ รวมถือสื่อสิ่งพิมพ์ ได้นำเว็บไซต์ฉลาดโอนไปเผยแพร่ในแง่ต่างๆ ซึ่งรวมถึงการใช้เป็นช่องทางในการตรวจสอบข้อมูลผู้ขายก่อนที่ผู้ซื้อจพทำการการโอนเงินค่าสินค้าหรือบริการ ซึ่งเป็นฟังก์ชันหนึ่งของระบบต้นแบบที่คณะผู้วิจัยพัฒนาขึ้น

รูปที่ 11 ภาพจากสื่อวิดีทัศน์จากช่องยูทูป DOM

รูปที่ 12 ภาพจากสื่อวิดีทัศน์จากช่องยูทูปฉลาดโอน

4. ผลการดำเนินการ

สำหรับผลการดำเนินงาน สามารถสรุปสถิติการเข้าใช้งานผ่านเว็บไซต์ของระบบต้นแบบ ตั้งแต่ช่วงวันที่ 1 กุมภาพันธ์ 2565 ถึง 20 มีนาคม 2565 รวมระยะเวลา 48 วัน ได้ดังนี้

4.1 สถิติการเข้าใช้งานผ่านเว็บไซต์

1) สถิติการลงทะเบียนยืนยันตัวตนบนเว็บไซต์ฉลาดโอน แสดงได้ดังตารางที่ 1
2) สถิติการเข้าใช้งานเว็บไซต์ฉลาดโอนแยกตามฟังก์ชัน แสดงได้ดังตารางที่ 2
3) สถิติการเช็กคนโกงผ่านเว็บไซต์ฉลาดโอน แสดงได้ดังตารางที่ 3
4) สถิติการแจ้งคนโกงผ่านเว็บไซต์ฉลาดโอน แสดงได้ดังตารางที่ 4

ตารางที่ 1 สถิติการลงทะเบียนยืนยันตัวตนบนเว็บไซต์ฉลาดโอนในช่วง 48 วันแรก

รายการ	จำนวน (คน)
เลขหมายโทรศัพท์	1,073
เลขหมายโทรศัพท์ + บัตรประจำตัวประชาชน	177
เลขหมายโทรศัพท์ + บัตรประจำตัวประชาชน + ภาพถ่ายใบหน้าของผู้ลงทะเบียน	149
เลขหมายโทรศัพท์ + บัตรประจำตัวประชาชน + ภาพถ่ายใบหน้าของผู้ลงทะเบียน + บัญชีธนาคาร	93
รวม	1,492

ตารางที่ 2 สถิติการลงทะเบียนยืนยันตัวตนบนเว็บไซต์ฉลาดโอนแยกตามฟังก์ชันในช่วง 48 วันแรก

รายการ	จำนวน (ครั้ง)
การเช็กคนโกง	119,190
การเช็กตัวตน	161
การแจ้งคนโกง	290
การช่วยรวมหลักฐาน	84
รวม	119,725

ตารางที่ 3 สถิติการเช็คคนโกงผ่านเว็บไซต์ฉลาดโอนในช่วง 48 วันแรก

รายการตรวจสอบ	จำนวน (คน)	ร้อยละ (%)
ชื่อบัญชีธนาคาร	59,583	50
เลขที่บัญชีธนาคาร	39,949	34
หมายเลขโทรศัพท์หรือ SMS	19,658	16
รวม	119,190	100

ตารางที่ 4 สถิติการแจ้งคนโกงผ่านเว็บไซต์ฉลาดโอนในช่วง 48 วันแรก

รายการตรวจสอบ	จำนวน (คน)	ร้อยละ (%)
บัญชีธนาคาร	456	81
พร้อมเพย์	57	10
ทรูวอลเล็ต	44	8
PayPal	3	1
รวม	560	100

4.2 สถิติการเข้าใช้งานผ่านช่องทาง LINE Official Account ฉลาดโอน.com

จากการรวบรวมสถิติของผู้เสียหายที่เข้าใช้งานผ่านช่องทาง LINE Official Account ฉลาดโอน.com ของฉลาดโอน ตั้งแต่วันที่ 1 กุมภาพันธ์ 2565 – 20 มีนาคม 2565 พบว่ามีผู้ลงทะเบียนผ่าน line official account เป็นจำนวน 3,900 คน (อัปเดต 20 มี.ค. 65) แสดงดังรูปที่ 9-2 และมีผู้ติดต่อเพื่อสอบถามการเข้าใช้งานระบบฉลาดโอนกับเจ้าหน้าที่เป็นจำนวน 1,657 คน (อัปเดต 20 มี.ค. 65) โดยทางคณะผู้วิจัยแบ่งประเภทการใช้บริการออกเป็น 3 ประเภท ได้แก่ การให้บริการ การติดต่อเจ้าหน้าที่ และอื่น ๆ แสดงดังตารางที่ 5

ตารางที่ 5 สถิติของผู้เสียหายที่เข้าใช้งานผ่านช่องทาง LINE Official Account ฉลาดโอน.com ในช่วง 48 วันแรก

วันที่	ผู้ใช้งาน	การให้บริการ						ติดต่อเจ้าหน้าที่			อื่น ๆ
		เช็กคนโกง	เช็กหลักฐาน	เช็กตัวตน	ประเมินบัญชีโซเชียล	ช่วยรวมหลักฐาน	แจ้งคนโกง	สอบถาม	แจ้งปัญหาการใช้งาน	ข้อเสนอแนะ	
1 ก.พ. 65	2						1				
2 ก.พ. 65	-										
3 ก.พ. 65	1						1				
4 ก.พ. 65	14	2				2	9	1			2
5 ก.พ. 65	80	17	5	1	1	9	22	4			23
6 ก.พ. 65	317	67	1	3	6	45	58	33	4	1	102
7 ก.พ. 65	66	4			1	11	19	8	4		19
8 ก.พ. 65	49	7	1	1		10	16	3	1		12
9 ก.พ. 65	51	4		1		14	21	7	1		4
10 ก.พ. 65	33	9		2		4	15	4			1
11 ก.พ. 65	24	3		2		2	10	2			5
12 ก.พ. 65	14	3		1		1	5				4
13 ก.พ. 65	15					3	11	1			1
14 ก.พ. 65	16	2		2		5	4	3			1
15 ก.พ. 65	117	33	1	5	6	18	26	25			10
16 ก.พ. 65	128	22		6	10	27	28	27			12
17 ก.พ. 65	64	18		4	3	16	8	9			10
18 ก.พ. 65	59	13		2	1	5	20	17			6
19 ก.พ. 65	36	7		3	3	5	10	10			1
20 ก.พ. 65	27	5	1	2	2	2	11	2			2
21 ก.พ. 65	32	6	1		1	9	11	5			2
22 ก.พ. 65	22	2		1	4	3	4	4			3
23 ก.พ. 65	30	8		1	2	4	5	7			2
24 ก.พ. 65	23	8		2	1	3	6	5			2
25 ก.พ. 65	35	6		5	2	5	9	6			3
26 ก.พ. 65	69	3	1	3	3	10	33	9			8
27 ก.พ. 65	35	6			2	4	14	5			4
28 ก.พ. 65	15	3			1		5				3
1 มี.ค. 65	27	3	1			3	15	8			2
2 มี.ค. 65	28	12				2	11	7			1
3 มี.ค. 65	23	3	1	1		2	15	4			
4 มี.ค. 65	20	3		1		2	4	10			1
5 มี.ค. 65	15	1				3	8	3			2
6 มี.ค. 65	11	2			1	2	2	7			1
7 มี.ค. 65	8	3			2	4	1	2			
8 มี.ค. 65	7	1				2	1	5			
9 มี.ค. 65	13	2			1	2	3	4			5
10 มี.ค. 65	12	1				2	7	5			1
11 มี.ค. 65	18			1	1	7	4	5	1		
12 มี.ค. 65	11	1		1	2	3	1	2			1
13 มี.ค. 65	15	3			1	7	2	3			1
14 มี.ค. 65	14	3		2	1	4	3	4			1
15 มี.ค. 65	8			1		1	1	3			
16 มี.ค. 65	15	1		2		3	5	3			2
17 มี.ค. 65	9	1		2		1	2	4			1
18 มี.ค. 65	11	3				1	3	4			
19 มี.ค. 65	9	1			1	1	2	4			
20 มี.ค. 65	9	1					1	6			1
รวม	1657	303	13	58	58	269	473	290	11	1	261

4.3 การใช้ประโยชน์โดยเจ้าหน้าที่ตำรวจ

หลังจากที่มีการเปิดให้ประชาชนเข้าตรวจสอบและแจ้งข้อมูลคนโกง เจ้าหน้าที่ตำรวจในเขตพื้นที่กองบังคับการตำรวจนครบาล 8 ได้นำข้อมูลมิจฉาชีพไปช่วยในการติดตามจับกุมผู้ต้องหาได้หลายราย ดังรูปที่ 13

รูปที่ 13 ภาพการจับกุมผู้ต้องหาและสอบสวนผู้ต้องหาจากข้อมูลเว็บไซต์ฉลาดโอน

5. อภิปรายและสรุปผลการดำเนินการ

จากผลการดำเนินการในครั้งนี้จะเห็นได้ว่า ระบบต้นแบบ “เว็บไซต์ฉลาดโอน” สามารถใช้เป็นเครื่องมือช่วยลดปัญหาการหลอกลวง การฉ้อโกง จากมิจฉาชีพออนไลน์ โดยระบบนี้สามารถนำไปใช้งานได้จริงอย่างมีประสิทธิภาพสูง เนื่องจากมีการบูรณาการฐานข้อมูล และบูรณาการความร่วมมือกับภาคส่วนต่างๆ โดยเฉพาะเหน้าที่ตำรวจ มีการเก็บรวบรวมข้อมูลและมีการดำเนินการต่างๆ อย่างเป็นระบบ เมื่อดำเนินการพัฒนาระบบต่างๆ เสร็จแล้ว ระบบต้นแบบนี้สามารถใช้เป็นแหล่งในการตรวจสอบข้อมูลมิจฉาชีพหรือคนโกง แม้จะไม่ครอบคลุมทั้งหมด เนื่องจากมิจฉาชีพมีการปรับเปลี่ยนรูปแบบและวิธีการในการโกงรูปแบบใหม่ทุกวัน แต่ก็สามารถเป็นเครื่องมือสนับสนุนงานสืบสวนและติดตามจับกุมผู้ต้องหาที่เกี่ยวข้องกับการฉ้อโกงออนไลน์ได้ด้วย

อย่างไรก็ตาม เพื่อให้ระบบมีความสมบูรณ์และมีประสิทธิภาพมากยิ่ง จำเป็นจะต้องมีการพัฒนาระบบ “เว็บไซต์ฉลาดโอน” ต่อไป นอกจากนี้ เพื่อให้เกิดความยั่งยืนของระบบและโครงการ คณะผู้วิจัยจำเป็นต้องเร่งประสานเพื่อส่งมอบระบบให้กับหน่วยงานที่จะทำหน้าที่ดูและระบบต่อไป

บรรณานุกรม

ปุณิกา และ ปริยานุช. (2560). พระราชบัญญัติห้ามเรียกดอกเบี้ยเกินอัตราพ.ศ. ๒๕๖๐. Retrieved May 10, 2021, From http://web.krisdika.go.th/data/law/law2/%CB04/%CB04-20-2560-a0001.htm

มนตรี สีทอง. (2564). ระบบสารสนเทศสำนักงานตำรวจแห่งชาติ. Retrieved May 10, 2021, From https://www.police9.go.th/media/documents/summary-crimes.pdf

ราชกิจจานุเบกษา. (2560). พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐. Retrieved May 9, 2021, From http://www.ratchakitcha.soc.go.th/DATA/PDF/2560/A/010/24.PDF

สถาบันนิติธรรมาลัย. (2564). หมวด ๓ ความผิดฐานฉ้อโกง (มาตรา ๓๔๑ – ๓๔๘). Retrieved May 10, 2021, From https://www.drthawip.com/criminalcode/1-53

สุรพงษ์ ชัยจันทร์. (2561). การปฏิบัติงานเชิงรุกเพื่อการป้องกนัอาชญากรรมตำรวจภูธรภาค 7. Retrieved May 10, 2021, From http://www.dsdw2016.dsdw.go.th/doc_pr/ndc_2560-2561/PDF/8575s/รวม.pdf

Blacklistseller. (2022). Read Blacklistseller Online fraud detection center. Retrieved May 15, 2022, from https://www.blacklistseller.com/home/admin_volunteer

Checkkonkong. (2022). Check scammers online. Checkkonkong. Retrieved May 15, 2022, https://xn--12cfanl6g3mua5b.com/

Pantipmarket. (2022). Buy-Sell online on pantipmarket. Retrieved May 15, 2022, from https://www. pantipmarket.com/

Verme. (2022). Online seller identity verification service. Retrieved May 15, 2022, from https://verme.me/how-to

Whoscheat. (2022). Check for scammers - Check for scammers, scammers accounts for sure before transferring money. Retrieved May 15, 2022, from https://www.whoscheat.com

Wichianlaw. (2561). ทนายความและที่ปรึกษากฎหมายลิขสิทธิ์. Retrieved May 10, 2021, From https://wichianlaw.blogspot.com/2018/05/blog-post_8.html

ต้นฉบับบทความที่นำเสนอคณะกรรมการจัดงานประชุมวิชาการ 2022 7th International Conference on Business and Industrial Research พิจารณา (การพิจารณาเป็นแบบ Blind-review จึงมีการปกปิดข้อมูลที่เกี่ยวข้องกับชื่อผู้เขียน ชื่อต้นสังกัด และหน่วยงานที่เกี่ยวข้อง)

Website Development for Avoiding of Online Shopping Scams in Thailand: Chaladohn

***Abstract*—This paper presents the website called Chaladohn (cha-lad-ohn). This website was designed and developed to aid Thai victims from online scammers; a collaborative project by the Faculty of [redacted] and the Investigation Division, Metropolitan Police Division 8. The major key features provided by this website are checking and alerting users about scammers from names, surnames, telephone numbers, bank accounts, and/or e-wallet accounts. Therefore, online shoppers can avoid scams if the checked results show evidence. Furthermore, users can add new lists of scammers into the database of the system when they identify themselves and provide reliable evidence. After the research and development, the website went through beta testing and received an average voting score of 4.43±0.73 from 30 subjects, which is considered excellent. Furthermore, in real practice, police officers can utilize the information from the system for arresting scammers within a few weeks after launching this website.**

Keywords—Online shopping, cybercrime, online scams, online frauds, victims.

I. Introduction

Emerging of the Coronavirus disease 2019 (COVID-19) has driven Thai people to participate in the world of Internet. Governments in many countries, including Thailand, issued the COVID-19 prevention and protection measures. These measures become the mechanism that drives the e-commerce growth and also changes life styles of Thai people, since they can go online shopping and spend by using e-payment conveniently. It was reported in [1] that while the lockdown in Thailand, e-commerce growth was about 140% and 75% in 2020 and 2021 respectively. This is consistent with the study as mentioned in [2] that Thai e-commerce has been expected to grow from 3 billion USD in 2018 to 13 billion USD by 2025. This might be inferred that e-commerce is setting to become the main channel for business in the near future. Therefore, the major players in Thai e-commerce market (e.g., JD Central, Shopee and Lazada) can take this opportunity for rising revenues.

Not only the COVID-19 pandemic but also the rival of the mobile network operators (who compete with each other to provide better services), the Thailand 4.0 and National e-Payment policies, including the government's Rao Chana (We Win) financial aid scheme, drive Thai people to familiarize with buying and paying via their mobile phones. However, because of growing of e-commerce, the online shopping market in cyber space becomes a new playground for the thieves or scammers. The shoppers who have low cybersecurity awareness may be scammed and lose their money from online shopping with fake online shops.

Therefore, to get rid of the online shoppers from online scammers, specifically cases that involve minor transaction (e.g., 200, 500 or 1,000 bath) that victims usually ignore to ask for assistance or report to police officers; creating a consumer pain point, special tools to help Thai consumers to consider before transferring money or payment are required. This is the reason this project was designed and developed.

II. Backgroind Information and Related Works

A. Cybercrime and Online Scams

Many people may confuse about the difference between terms 'cybercrime' and 'online scams', since these two terms often overlap. For the definition of cybercrime, there is no single definition [3] However, from a general understanding, cybercrime is illegal activity directed at mobile phones, networked devices, and computers [4]. Furthermore, as mentioned in [5], its definition is any crime conducted utilizing computers, mobile devices and other telecommunication tools to cause anxiety and fear to people and harm, damage or destroy things. There are two categories, consisting of computer-focused and computer-assisted and cybercrimes. Computer-assisted cybercrimes includes fraud, money laundering, child pornography, and cyber stalking. For computer-focused cybercrimes, they are website defacement, hacking and phishing, etc.

However, as mentioned in [6] online scams are defined as fraudulent schemes associated with networked devices that could range from stealing money to a possibility of being life threatening. Focusing on online scams, they are now on the rise in people and/or business organizations are not safe when doing online activities or transactions via Internet networks (e.g., online shopping and fake charities seeking donations) [7]. For online shopping scams, they usually involve scammers pretending to be legitimate online sellers, either with fake websites or fake ads on a genuine

retailer's site [8]. Online scams may be classified as subsets of cybercrimes, whereas, they have lower degree of activities, and mostly conducted for taking money from victims.

B. Related Works

From the survey, it was found that there are several prior works associated with online scams and frauds, for example:

- Verma et al. [9] conducted the analysis study about the components and pattern of online scams websites in order to give more information for people.
- Lee [10] analyzed online fraud victimization in Chinese online communities using the data from Baidu Tieba--a Chinese version of Craigslist. The studied results present that different kinds of fraud are perpetrated online and that victimization methods are related to particular kinds of media.
- Hirel [11] studied using the data from website that users can post ads to sell and/or buy personal belongings. The study identified online scam triggers including bad keywords, multiple locations, personal email and rogue picture and VoIP to detect online scams. They found a lot of ads based on scam trigger, while 53 % of the data tend to be scams.
- Yoshida et al. [12] proposed the online shopping frauds detection system without data mining primarily. For their approach, they applied the nature of business and/or economic crimes. For example, fraudsters tend to buy good that can be changed into cash easily.
- Weng et al. [13] developed the system called AnTi-Fraud (ATF) to detect online frauds for large-scale e-commerce platforms and implement it in parallel on a large-scale platform. The evaluation results from testing with Taobao platform of Alibaba show that ATF can also achieve an accuracy of 98.16%.
- Anupriya and Kanimozhi [14] presented how neural network algorithm and Machine Learning algorithm combined to obtain a high fraud coverage and also with a low false alarm rate. For this study, Deep learning was applied for fraudulent detection based on the user's behavior from their records of transactions.

However, from the abovementioned, some of them are about the studies and analysis, while some are development of detection systems. In addition, it was found from the survey about several websites available in several countries. For example:

- Scamwatch: it is operated by the Australian Competition and Consumer Commission (ACCC). This website provides information to small businesses and consumers about how to recognize scams, avoid and report [15].
- Canadian Anti-Fraud Centre: this website is used to collect information on fraud and identity theft. It can provide information on past and current scams affecting consumers [16].
- Citizens Advice: this website is used by consumers in the UK. It covers most categories, including scams [17].
- Action Fraud: this is the UK's national reporting center for online fraud and cybercrime where a consumer should report online fraud if he or she had experienced cybercrime, scam or defraud [18].
- National Cyber Security Center: the website of this center supports critical organizations in the UK, the wider public sector, industry, SMEs and the general public. This website provides the channel to report incidents and provide effective incident response to minimize harm and support with recovery [19].
- Scam Alert: this website is operated by the National Crime Prevention Council (NCPC)—the agency of Singapore government. This organization which is a non-profit organization committed to promoting public concern and raising awareness about crime and to propagating the guidelines of self-aid in crime prevention. Victims can share their stories and call the anti-scam helpline for consulting [20].

Nevertheless, those websites are in other countries, all of them cannot support Thai victims who were scammed in the Kingdom of Thailand. Fortunately, It was found that there are a few websites that attempt to do the similar things, including:

- Verme [21]: this website was created by the private organization in order to become a secure platform for online selling and buying. Everyone who has been identified will have the VerME card to show to others in the online shopping community.
- Blacklistseller and Whoscheat [22-23]: each website was developed and is currently operated by the group of volunteers and/or private organizations. Mainly, they receive complaints about scams. Then, names, telephone numbers and/or bank accounts, for example, of the scammers will be recorded in the database. Thus, if other consumers check and the name, the telephone number or the bank account match the record in the database, the information about the scammer will show.
- 1212 OCC [24]: this website is operated by the Electronic Transactions Development Agency (ETDA)—the government organization in Thailand. The number 1212 is the call center number, while the term 'OCC' stands for Online Complaint Center. Thai consumers can call to complain about online scams, cyberthreats and any related issues everyday at any time. Then, they will coordinate for problem solving.

One can see that there are similar concepts of websites but all of them do not work together with the police organization. This is the obvious gap for developing 'Chaladohn'.

III. Design and Development

According to related works as mentioned the previous section, pros and cons of each work were considered and analyzed. Then, the system was designed to have four sub-systems, consisting of:

- registration and identification system (or the electronic know your customer – registration system)

- verification and search engine for the scammers' information
- complaint system
- reporting system

From the concept design, the system overview has been created as shown in Fig.1. To register as a user, the designed system requires face recognition process to ensure that he or she is the same person with the face shown on the ID citizen card. Of course, for this process, this system must be linked to the Department of Provincial Administration (DOPA) system [25]. the Chaladohn website was mainly developed using PHP, HTML and Python. Then, after finishing the beta version it has been launched and evaluated. More details about the results are shown in the next section.

IV. Evaluation and Results

After the development of the website called Chaladohn, its beta version was launched and operated. Then, the evaluation form was created and distributed to a group of subjects for assessment using 5-point scale [26]. For the topics in the evaluation form, they were mainly asked in four topics, consisting of the capacity, the design, benefits of the system, and overall.

The evaluation was done by 30 subjects (9 females and 21 males). Most of the evaluators were the students in a department in the faculty of [redacted]. The average age of them was 22.50±1.36 years. The evaluation results are shown in Table I. One can see that the system capacity, the design and overall are evaluated as excellent with scores of 4.425±0.729, 4.411±0.811 and 4.233±0.728 respectively, the benefits of the system are particularly assessed as excellent with the highest score of 4.522±0.768. However, the high score may be from the positive bias of the students.

V. Emperical Use Cases

After launching the website, many cases were reported to the system, Furthermore, the police officers utilized the information from the website for chasing the scammers effectively, for example, the case of Ms.Khanita Kearwkham (น.ส.คณิตา เขียวคำ) who scammed more than 1,400 victims and found 551 records by the Chaladohn system (see Fig. 2 and Fig.3(a)) that was arrested. For this case, each victim lost about 500-3,000 baht or 15-90 USD [27]. Not only the case of Kanita—the scammer but also other cases that were arrested, see Fig.3(b). One can see that this system can help police officers and mitigate the victims apparently.

VI. Discussion, Conclusion and Future Work

The concept of this system or website is not actually a new idea. It is the integrated concepts from several previous works as described in Section II.B. Besides, some sub-system, particularly the complaint system has not been interfaced with the police system because of the limitations of the police regulations. Advance beyond other systems, 'Chaladohn' collaborates and coordinates with one division of Metropolitan Police Offices to utilized the information from Chaladohn's database to arrest online shopping scammers.

After the development of the website called Chaladohn, it was launched and operated. Then the evaluation form was created and distributed to a group of subjects for assessment. For the issues in the evaluation form, they were mainly asked in four topics, consisting of the capacity, design, benefits of the system, and overall. All topics were assessed as excellent, while the average score in each topic was in the range of 4.41-4.52.

However, since this is the first version from the first phase of this website development, there at least a few limitations. First, it supports Thai language only, thus it should be enhanced to support English in case to help foreigners who may be scammed in Thailand. Second, this system operates as a website only, it should be developed more to become an application as well, supporting both Android and iOS. Third, the database of this system should be linked to the crime's database of the National Police Office for data verification and integration. Furthermore, the Chaladohn's database should be share to the Bank of Thailand or the Thai Bankers Association to break money transfer process of scammers.

TABLE I. Evaluation Results

Topic	Average	S.D.	Remark
System capacity	4.425	0.729	Excellent
Design (UX/UI)	4.411	0.811	Excellent
Benefits	4.522	0.768	Excellent
Overall	4.433	0.728	Excellent

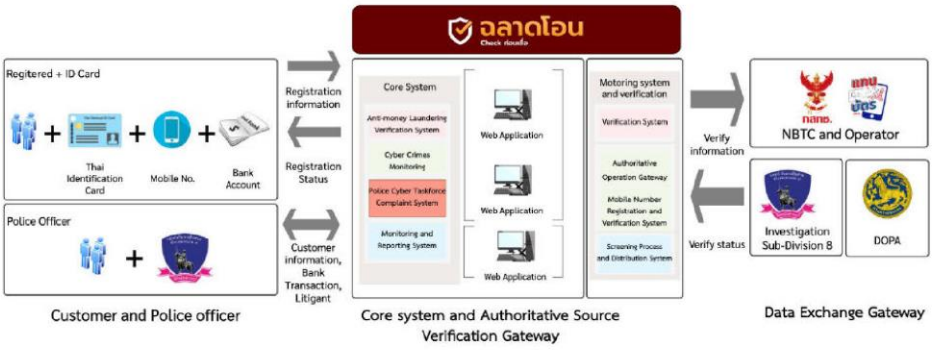
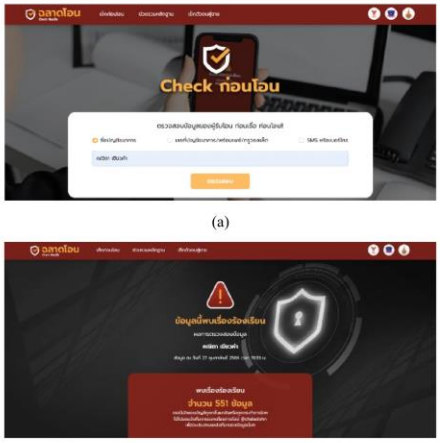


Fig. 1. System overview



(a)

(b)

Fig. 2. User interfaces of Chaladohn (a) Check (b) result

(a)

(b)

Fig. 3. Use cases (a) the case of Kanita--the scammer (b) cases of the male scammers

ACKNOWLEDGMENTS

REFERENCES

[1] S. Leesa-nguansuk, "E-commerce growth stunted," https://www.bangkokpost.com/business/2248475/e-commerce-growth-stunted

[2] S. Leesa-nguansuk, "E-commerce rivalry intensifies," https://www.bangkokpost.com/tech/1654456/e-commerce-rivalry-intensifies

[3] ITU, "Understanding cybercrime: Phenomena, challenges and legal response," https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

[4] Fairtrading, "Scams and cybercrime," https://www.fairtrading.nsw.gov.au/buying-products-and-services/scams#:~:text=Cybercrime%20and%20scams%20often%20overlap,illegal%20activity%20is%20carried%20out.

[5] W. A. Al-Khater, S. Al-Maadeed, A. A. Ahmed, A. S. Sadiq and M. K. Khan, "Comprehensive Review of Cybercrime Detection Techniques," in IEEE Access, vol. 8, pp. 137293-137311, 2020, doi: 10.1109/ACCESS.2020.3011259.

[6] H. Alsaleh, and L. Zhou, "A Heuristic Method for Identifying Scam Ads on Craigslist," European Intelligence and Security Informatics Conference (EISIC), 2018, pp. 69-72, doi: 10.1109/EISIC.2018.00019.

[7] E. B. B. Palad, M. S. Tangkeko, L. A. K. Magpantay, and G. L. Sipin, "Document Classification of Filipino Online Scam Incident Text using Data Mining Techniques," 19th International Symposium on Communications and Information Technologies (ISCIT), 2019, pp. 232-237, doi: 10.1109/ISCIT.2019.8905242.

[8] Scamwatch, "Online shopping scams," https://www.scamwatch.gov.au/types-of-scams/buying-or-selling/online-shopping-scams.

[9] R. Verma, A. Choudhary, B. Janardan, Gulshan, and A. K. Shukla, "Components and Pattern Analysis of Online Scam Websites," Journal of Emerging Technologies and Innovative Research, 2020, Vol. 7(11), pp 412-414.

[10] C. S. Lee, "Online Fraud Victimization in China: A Case Study of Baidu Tieba," VICTIMS & OFFENDERS, 2021, Vol. 16(3), pp. 343–362. doi.org/10.1080/15564886.2020.1838372

[11] H. M. Hirei, "Investigating and Validating Scam Triggers: A Case Study of a Craigslist Website," Culminating Projects in Information Assurance, 2020, pp 1-71.

[12] C. S. Lee, "Online Fraud Victimization in China: A Case Study of Baidu Tieba," VICTIMS & OFFENDERS, 2021, Vol. 16(3), pp. 343–362. doi.org/10.1080/15564886.2020.1838372

[13] H. M. Hirei, "Investigating and Validating Scam Triggers: A Case Study of a Craigslist Website," Culminating Projects in Information Assurance, 2020, pp 1-71.

[14] K. Anupriya, and M. C. Kanimozhi, "Scam Detection for Online Shopping using Deep Learning," International Journal of Engineering Research & Technology (IJERT), 2016, Vol. 4(11), pp. 1-6.

[15] Scamwatch, "News and alerts: Scams Awareness Week 2021," https://www.scamwatch.gov.au/

[16] Canadian Anti-Fraud Centre, "Recent scams and fraud," https://www.antifraudcentre-centreantifraude.ca/index-eng.htm

[17] Citizensadvice, "Consumer: Scams," https://www.citizensadvice.org.uk/consumer/

[18] Actionfraud, "News & Alerts, " https://www.actionfraud.police.uk/

[19] The National Cyber Security Centre, "Helping to make the UK the safest place to live and work online," https://www.ncsc.gov.uk/

[20] Scamalert, "Spot the Scam Signs," https://www.scamalert.sg/

[21] Verme, "Online seller identity verification service," https://verme.me/how-to (In Thai)

[22] Blacklistseller, "Read Blacklistseller Online Fraud Monitoring Hub," https://www.blacklistseller.com/home/admin_volunteer (In Thai)

[23] Whoscheat, "Check for scammers - Check for scammers, scammers accounts for sure before transferring money," https://www.whoscheat.com/ (In Thai)

[24] 1212 OCC, "Found illegal websites, online threats, online trading problems or online transaction suspicions.," https://www.1212occ.com/home (In Thai)

[25] Dopa, "Home page news," https://www.dopa.go.th/main/web_index (In Thai)

[26] E-Research Siam, "Chapter 3 Research Methodology," http://e-research.siam.edu/wp-content/uploads/2013/12/IS-CHAPTER_3.pdf

[27] Matichon, "Check the website "smart transfer" catches a girl, the owner of a Twitter page, aged five, tricked into selling Japanese manga models," https://www.matichon.co.th/news-monitor/news_3204091 (In Thai)

เอกสารการยื่นขอตีพิมพ์ผลงานเผยแพร่ในวารสารในประเทศหรือในระดับนานาชาติ

วารสาร
สารสนเทศศาสตร์
Journal of Information Science
Journal of the Department of Information Science, Khon Kaen University, Thailand

iSchool KKU

ฉลาดโอน: การพัฒนาระบบเว็บไซต์และสร้างระบบฐานข้อมูลสำหรับการตรวจสอบข้อมูลมิจฉาชีพออนไลน์และช่วยเหลือเหยื่อ

Chaladohn: Website and Database Development for Checking of Online Scammers' Profiles and Victims Assistance

บทคัดย่อ:

วัตถุประสงค์: เพื่อพัฒนาระบบเว็บไซต์ฉลาดโอนและสร้างระบบฐานข้อมูลมิจฉาชีพออนไลน์ในการใช้เป็นเครื่องมือช่วยลดปัญหาการหลอกลวง การฉ้อโกง จากมิจฉาชีพออนไลน์

วิธีการศึกษา: การวิจัยครั้งนี้ได้นำขั้นตอน SDLC แบบ Waterfall model มาใช้ในการพัฒนาระบบ กลุ่มตัวอย่างที่ทดลองใช้ระบบเว็บไซต์ฉลาดโอนและสร้างระบบฐานข้อมูลมิจฉาชีพออนไลน์ในการใช้เป็นเครื่องมือช่วยลดปัญหาการหลอกลวง การฉ้อโกง จากมิจฉาชีพออนไลน์ในการวิจัยครั้งนี้ คือ ผู้ใช้งานจริงจำนวน 72 คน

ข้อค้นพบ: ผลการวิจัยพบว่าระบบที่ได้พัฒนาขึ้นสามารถใช้งานได้จริงและสามารถตรวจสอบมิจฉาชีพก่อนโอนได้จริงโดยตรวจสอบชื่อบัญชีธนาคาร, เลขที่บัญชีธนาคาร/พร้อมเพย์/ทรูวอลเล็ต, SMS หรือเบอร์โทร อีกทั้งระบบยังช่วยให้สามารถแจ้งชื่อคนโกงได้จริงรวมไปถึงมีระบบฟังก์ชันในการช่วยตรวจสอบและช่วยรวบรวมหลักฐานช่วยให้ผู้เสียหายมีข้อมูลที่ถูกต้อง ครบถ้วน พร้อมสำหรับการแจ้งความดำเนินคดี และจากการใช้งานระบบ กลุ่มตัวอย่าง 72 คน มีความพึงพอใจต่อภาพรวมระบบโดยรวมอยู่ในระดับมาก (เฉลี่ย = 4.14±1.01)

การประยุกต์ใช้จากการศึกษานี้: เว็บไซต์ฉลาดโอนและสร้างระบบฐานข้อมูลมิจฉาชีพออนไลน์ในครั้งนี้ เป็นเครื่องมือหนึ่งที่จะช่วยลดจำนวนอาชญากรรมออนไลน์ได้ เนื่องจากในระบบนี้มีฟังก์ชันที่ทำให้ผู้ซื้อสามารถตรวจสอบข้อมูลผู้ขายหรือผู้รับโอนเงินที่เคยมีผู้แจ้งประวัติฉ้อโกงได้ นอกจากนี้ยังมีระบบที่ช่วยในการรวบรวมเอกสารหลักฐานที่ใช้ในการดำเนินคดี ทำให้ประหยัดเวลาในการติดต่อแจ้งความดำเนินคดี

คำสำคัญ: เว็บไซต์ ฉลาดโอน ฐานข้อมูล มิจฉาชีพออนไลน์ หลอกลวง ฉ้อโกง

[1] สาขาวิชาวิศวกรรมการจัดการอุตสาหกรรมเพื่อความยั่งยืน, คณะวิศวกรรมศาสตร์, มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร, ประเทศไทย; Sustainable Industrial Management Engineering Department, Faculty of Engineering, Rajamangala University of Technology Phra Nakhon, Thailand

[2*] สาขาวิชาเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล, คณะอุตสาหกรรมและเทคโนโลยี, มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์, ประเทศไทย; Information Technology and Digital Innovation Department, Faculty of Industry and Technology, Rajamangala University of Technology Rattanakosin, Thailand

Abstract:

Purpose: To develop a smart website transfer system and create a database of recorded scammer to use as a tool to protect against deceptions and frauds.

Methodology: This research applied the SDLC method of Waterfall model to develop the system. An example group to test the transfer smart website system and create a scammer database system to use as a tool to reduce deception and fraud from scammers: this research has 72 active and real users.

Findings: The results of the research show that the developed system is practical and able to detect scammers before actually transferring, via checking bank s account name, banks account number, PromptPay, True Wallet, SMS, and phone number. The system also clarifies the identity of the scammers as legit or non-legit, as well as having a function system to help examine and collect evidence. This helps the victim to have more accurate and complete information, and be ready for litigation. From using the system for a sample of 72 people, there was a high level of satisfaction. (Mean = 4.14±1.01).

Applications of this study: Chaladohn website and its scammers database system is a tool to help reduce the number of online crimes. Since in this system, there is a function that allows the online shopper to check the information of the online seller or the money transferee who has previously reported fraud. There is also a system that helps in collecting documentary evidence used in litigation. This saves time in communicating with litigation.

Keywords: Website, Chaladohn, Database, Online Scammers, Fraud, Scams

บทนำ

ด้วยความก้าวหน้าของเทคโนโลยีการสื่อสารและเทคโนโลยีอินเทอร์เน็ต ผู้ใช้ที่ต้องการทำธุรกรรมทางการเงินโดยผ่านธนาคารปัจจุบันไม่จำเป็นต้องเดินทางไปยังธนาคารพาณิชย์ในเวลาทำการปกติ เช่น โอนเงินระหว่างบัญชีของบุคคลหนึ่งไปยังอีกบุคคลหนึ่ง ชำระค่าบริการต่าง ๆ หรือตรวจสอบยอดเงินอีกต่อไป เพราะผู้ใช้บริการสามารถเข้าถึงบริการเหล่านั้นผ่านเครือข่ายอินเทอร์เน็ตหรือผ่านแอปพลิเคชันของธนาคารที่ติดตั้งบนโทรศัพท์เคลื่อนที่แบบสมาร์ตโฟนจากจุดใดและเวลาใดก็ได้ ทำให้ธุรกรรมออนไลน์ในประเทศไทยเติบโตขึ้นเป็นอย่างมากและยังมีแนวโน้มเติบโตขึ้นอย่างต่อเนื่องด้วย จากข้อมูลสถิติของธนาคารแห่งประเทศไทย ตั้งแต่ปี 2553 เป็นต้นมา ธุรกรรมการชำระเงินผ่านบริการ Mobile Banking ได้รับความนิยมเพิ่มขึ้นอย่างต่อเนื่อง ดังภาพที่ 1 (ธนาคารแห่งประเทศไทย, 2564) ธุรกรรมออนไลน์ช่วยให้ทุกคนสามารถเป็นผู้ซื้อและผู้ขายได้ง่าย ผ่านการติดต่อสื่อสารกันผ่านสื่อ สังคมออนไลน์ต่าง ๆ หรือผ่านแพลตฟอร์มซื้อขายสินค้าออนไลน์ต่าง ๆ นอกจากการซื้อขายสินค้าออนไลน์

ทั่วไปแล้ว ยังมีการสั่งซื้อสินค้าแบบจ่ายเงินล่วงหน้าหรือ พรีออร์เดอร์ (Pre-order) การสมัครขอเงินกู้ดอกเบี้ยต่ำ และการทำธุรกรรมอื่นๆ ทั้งนี้ได้มีรายงานของเฟซบุ๊กระบุว่า พ.ศ. 2562 ประเทศไทยกลายเป็นประเทศอันดับ 1 ในด้านการรับรู้และการใช้แชทออนไลน์เพื่อการซื้อสินค้าผ่านแพลตฟอร์มซื้อขายสินค้าออนไลน์ ซึ่งสอดคล้องกับการเปิดเผยของทางวีซ่า (VISA) ที่ระบุว่า ประเทศไทยเป็นอันดับหนึ่งในด้านที่ผู้บริโภคใช้จ่ายผ่านโทรศัพท์เคลื่อนที่ในช่วงกลางปี พ.ศ. 2562 และรายงานเมื่อเดือนมกราคม พ.ศ. 2562 (Datareportal, 2020; Gimme, 2562; Nalisa, 2562) ผนวกกับสถานการณ์การระบาดของเชื้อไวรัสโคโรน่าสายพันธุ์ใหม่ (COVID-19) จึงมีผลทำให้ธุรกรรมออนไลน์ ซึ่งครอบคลุมถึงการสั่งซื้อสินค้าต่างๆ ทั้งแบบแบบโอนเงินชำระค่าสินค้าปกติและแบบจ่ายเงินล่วงหน้า ไม่เว้นแม้แต่อาหาร ผ่านสื่อสังคมออนไลน์และแอปพลิเคชันต่างๆ เติบโตขึ้นเป็นอย่างมาก

ถึงแม้ว่าความก้าวหน้าทางเทคโนโลยีสารสนเทศและการสื่อสารโทรคมนาคมจะช่วยเพิ่มความสะดวกสบายให้กับผู้ใช้บริการ แต่ก็แฝงไปด้วยภัยคุกคามจากผู้ไม่ประสงค์ดีที่อาศัยช่องโหว่ ทั้งจากคน ระบบ และกระบวนการ ตลอดจนข้อกฎหมายที่ยังมีจุดอ่อน และยังต้องการการพัฒนาให้เท่าทันเทคโนโลยีที่พัฒนาไปอย่างรวดเร็ว ทำให้ผู้ใช้บริการเกิดความเสียหาย กลายเป็นช่องทางให้มิจฉาชีพแอบแฝงเข้ามาหาผลประโยชน์ด้วยกลโกงรูปแบบต่างๆ โดยใช้การเปลี่ยนเลขหมายโทรศัพท์มือถือที่เป็นแบบเติมเงินไปเรื่อยๆ และใช้เครือข่ายอินเทอร์เน็ตสาธารณะเป็นเครื่องมือหลักในการกระทำความผิดเพื่อหลอกเหยื่อซึ่งอาจเป็นผู้ซื้อหรือผู้ขายที่ไม่ได้ทำการตรวจสอบตัวตนจริงของบุคคลที่ทำธุรกรรมด้วยอย่างละเอียดถี่ถ้วน ทำให้มิจฉาชีพใช้ช่องโหว่ดังกล่าวในการ กระทำความผิดทางออนไลน์ด้วยปัจจัยหลักคือ การที่ผู้เสียหายไม่สามารถที่จะหาหลักฐาน หรือดำเนินการเอาผิดได้โดยง่าย อาทิเช่น การสั่งซื้อของออนไลน์แล้วไม่นำส่งของ สั่งสินค้าแบบจ่ายเงินล่วงหน้าแล้วไม่ส่งของ การตอบรับการสมัครขอเงินกู้ดอกเบี้ยต่ำและการเสียค่าธรรมเนียมเอกสารซึ่งไม่มีการยื่นกู้เงินจริง การซื้อขายของระหว่างบุคคลกับบุคคลที่ไม่ได้ผ่านเว็บไซต์ที่ตรวจสอบความมีตัวตน ตามเว็บประกาศขาย หรือทางสื่อสังคมออนไลน์ Facebook , Instagram หรือ LINE การแฮกเข้าบัญชี Facebook หรือ LINE ของบุคคลอื่น และหลอกให้บุคคลอื่นโอนเงิน หรือ การทำธุรกรรมอื่นๆ ทางออนไลน์ ซึ่งมิจฉาชีพออนไลน์มักจะมีกลโกงแอบแฝงอยู่ในรูปแบบต่างๆ เหล่านี้ จนทำให้ผู้ซื้อและผู้ขายไม่ได้มีการตรวจสอบตัวตนจริงของบุคคลที่ทำธุรกรรมอย่างละเอียดถี่ถ้วน ซึ่งแม้ในความเป็นจริงทางผู้เสียหายจะมีหลักฐานเบื้องต้นเช่น ชื่อบัญชีธนาคาร สลิปการโอนเงินไปยังมิจฉาชีพ หรือตัวแทนของมิจฉาชีพ และเบอร์โทรศัพท์มือถือที่ใช้ติดต่อกัน แต่ก็ไม่สามารถดำเนินคดีเอาผิดได้โดยง่ายเนื่องจากการเปลี่ยนเลขหมายโทรศัพท์มือถือที่เป็นแบบเติมเงินไปเรื่อยๆ และเป็นคดีความที่มีมูลค่าความเสียหายน้อย ทำให้ผู้เสียหายไม่อยากเสียเวลาในการแจ้งความดำเนินคดี ทั้งที่มิจฉาชีพเหล่านี้ได้กระทำความผิดในรูปแบบเดียวกันกับผู้เสียหายเป็นจำนวนมาก และมีมูลค่ารวมเป็นจำนวนมากแต่ก็ไม่ถูกดำเนินคดี

ด้วยเหตุนี้ คณะผู้วิจัยจึงได้ได้คิดค้นและพัฒนาระบบเว็บไซต์ฉลาดโอนและสร้างระบบฐานข้อมูลมิจฉาชีพออนไลน์ขึ้นเพื่อใช้เป็นเครื่องมือช่วยลดปัญหาการหลอกลวง การฉ้อโกง จากมิจฉาชีพออนไลน์ ซึ่งในตัวของระบบเว็บไซต์ฉลาดโอนและสร้างระบบฐานข้อมูลมิจฉาชีพออนไลน์มีฟังก์ชันที่ทำให้ผู้ซื้อ

สามารถตรวจสอบข้อมูลผู้ขายหรือผู้รับโอนเงินที่เคยมีผู้แจ้งประวัติฉ้อโกงได้ นอกจากนี้ยังมีระบบที่ช่วยในการรวบรวมเอกสารหลักฐานที่ใช้ในการดำเนินคดี ทำให้ประหยัดเวลาในการติดต่อเจ้าหน้าที่ตำรวจเพื่อแจ้งความดำเนินคดีทำให้เจ้าหน้าที่ตำรวจสามารถนำข้อมูลไปขยายผลและนำไปสู่การจับคุมได้อย่างรวดเร็ว

วัตถุประสงค์

เพื่อพัฒนาระบบเว็บไซต์ฉลาดโอนและสร้างระบบฐานข้อมูลมิจฉาชีพออนไลน์ในการใช้เป็นเครื่องมือช่วยลดปัญหาการหลอกลวง การฉ้อโกง จากมิจฉาชีพออนไลน์ และประเมินความพึงพอใจต่อระบบเว็บไซต์ฉลาดโอนของผู้ใช้งาน

วิธีการศึกษา

การวิจัยการพัฒนาระบบเว็บไซต์ฉลาดโอนและสร้างระบบฐานข้อมูลมิจฉาชีพออนไลน์ในการใช้เป็นเครื่องมือช่วยลดปัญหาการหลอกลวง การฉ้อโกง จากมิจฉาชีพออนไลน์ แบ่งการทำงานวิจัยเป็น 2 ระยะ ได้แก่ ระยะที่ 1 เป็นการพัฒนาระบบเว็บไซต์ฉลาดโอนและสร้างระบบฐานข้อมูลมิจฉาชีพออนไลน์ ระยะที่ 2 เป็นการประเมินความพึงพอใจต่อระบบเว็บไซต์ฉลาดโอนและสร้างระบบฐานข้อมูลมิจฉาชีพออนไลน์ โดยมีรายละเอียดดังนี้

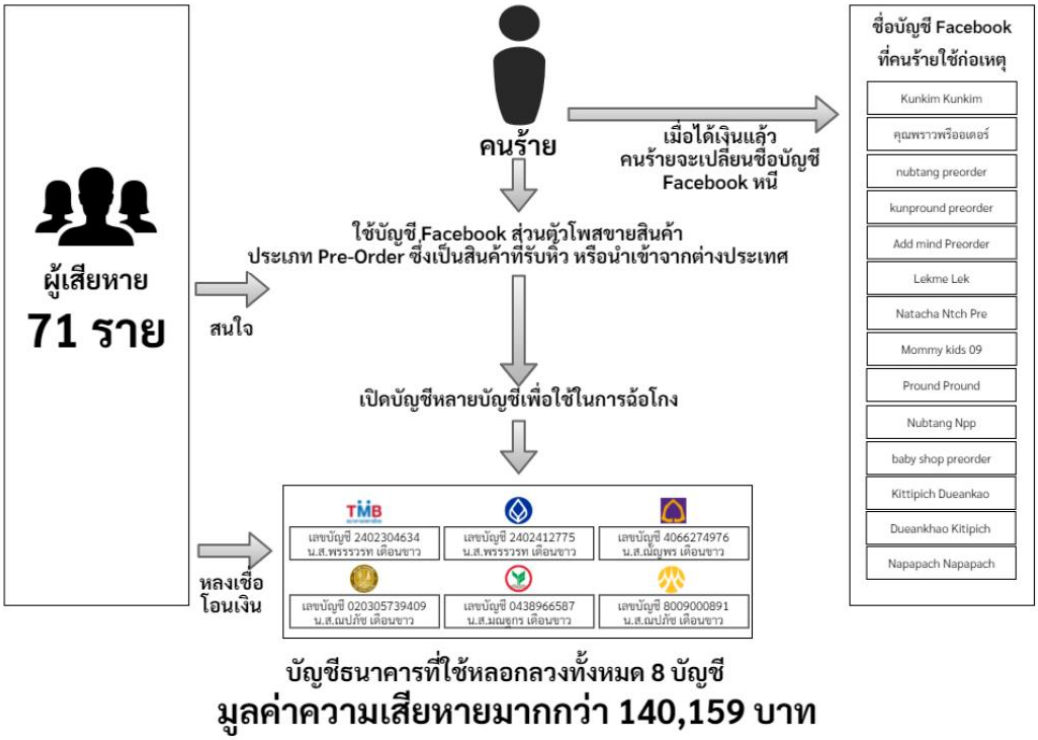
ระยะที่ 1 การพัฒนาระบบเว็บไซต์ฉลาดโอนและสร้างระบบฐานข้อมูลมิจฉาชีพออนไลน์ โดยระยะนี้มีได้นำขั้นตอน SDLC แบบ Waterfall model มาใช้ในการพัฒนาระบบ 6 ขั้นตอนซึ่งจะทำงานแบบชั้นบนสุดลงมาชั้นล่างสุดดังรายละเอียดข้างล่าง

ขั้นตอนที่ 1) เป็นขั้นตอนในการศึกษาข้อมูล เก็บข้อมูลความต้องการ (Requirement) ที่เกี่ยวข้องในการนำมาใช้เพื่อพัฒนาระบบ จากนั้นนำข้อมูลมาทำการวิเคราะห์ความต้องการนั้นออกมาเพื่อที่จะเป็นข้อมูลในการพัฒนาระบบ (Requirement Specification) โดยในงานวิจัยนี้ได้มีการศึกษาและวิเคราะห์ข้อมูลดังนี้

1.1 ศึกษาประเภทของการฉ้อโกง

ในปัจจุบันสภาพสังคมมีความสลับซับซ้อนมาก อาชญากรรมประเภทฉ้อโกงมีความสลับซับซ้อนมากขึ้นตามไปด้วย ถึงแม้ว่าการฉ้อโกงในบางรูปแบบอาจจะมีลักษณะคล้ายคลึงกันกับที่เคยปรากฏในอดีตเมื่อหลายสิบปีก่อน แต่ก็มีการสร้างเครือข่ายองค์กรอาชญากรรม หรือนำเทคโนโลยีสารสนเทศมาใช้ในการฉ้อโกง ซึ่งจะทำให้มีประชาชนที่ไม่รู้เท่าทัน ก็จะหลงเชื่อและตกเป็นผู้ถูกหลอกมากขึ้น ก่อความเสียหายอย่างมากทั้งแก่ตัวบุคคล ชุมชนและประเทศชาติ สำหรับรูปแบบการฉ้อโกงในยุคปัจจุบันสามารถประมวลได้ 8 รูปแบบ ดังต่อไปนี้ 1) การฉ้อโกงโดยหลอกลวงให้ร่วมลงทุนในลักษณะแชร์ลูกโซ่, 2) การฉ้อโกงโดยหลอกลวงให้ทำรายการที่ตู้เอทีเอ็ม, 3) การฉ้อโกงโดยส่งอีเมล์มาทำความรู้จักคุ้นเคยและหลอกลวงให้โอนเงินเข้าบัญชี, 4) การฉ้อโกงโดยปลอมตัวและปลอมที่อยู่อีเมล์มาหลอกลวงให้โอนเงินผิดบัญชี, 5) การฉ้อโกงโดยอ้างการรักษาพยาบาลมาหลอกลวงเอาเงิน, 6) การฉ้อโกงโดยอ้างการ

เรี่ยไรเงินไปช่วยเหลือทางราชการหรือผู้ด้อยโอกาส, 7) การฉ้อโกงโดยใช้ศาสนาเป็นเครื่องมือในการหลอกลวงและ 8) การฉ้อโกงโดยอ้างว่าเป็นเจ้าหน้าที่ในกระบวนการยุติธรรมและหลอกลวงเอาเงิน และสำหรับกรณีของการฉ้อโกง ที่เป็นการฉ้อโกงออนไลน์ ผ่านทาง Facebook, Line, Instagram เป็นต้น สามารถแบ่งออกเป็น 5 รูปแบบ ดังนี้ 1) การหลอกลวงขายสินค้าในรูปแบบต่าง ๆ โดยมีเจตนาทุจริตที่จะไม่ขายสินค้าจริง ๆ หรือไม่มีสินค้าอยู่จริง โดยนำภาพสินค้าของคนอื่นมาลงโพสต์เพื่อขายให้เหยื่อหลงเชื่อ, 2) การหลอกลวงขายสินค้าที่ลงโพสต์ไว้ว่าเป็นของแท้แต่ส่งของเลียนแบบหรือของปลอมหรือของคนละประเภทกับที่โพสต์ขาย, 3) การหลอกลวงว่าจะให้กู้ยืมเงินในอัตราดอกเบี้ยต่ำ โดยให้ผู้เสียหาย โอนเงินค่าธรรมเนียม หรือค่าดอกเบี้ยงวดแรก หรือค่ามัดจำ เป็นต้น, 4) การหลอกลวงด้วยการตีสนิทเข้ามาจีบ (ส่วนใหญ่ใช้รูปโปรไฟล์ ชาวต่างชาติหน้าตาดี สวย เท่ห์) และหลอกว่าจะส่งของมาให้ จากนั้นจะมีผู้ร่วมขบวนการโทรมาติดต่อหลอกว่าเป็นพนักงานบริษัทขนส่งให้โอนค่าธรรมเนียมเพื่อดำเนินการนำพัสดุออกจากด่านศุลกากร โดยส่วนมากจะอ้างว่ามีเงินสดจำนวนมากอยู่ในพัสดุดังกล่าว, 5) การหลอกลวงด้วยการแฮกข้อมูลสื่อสังคมออนไลน์ของผู้อื่น โดยที่เจ้าของข้อมูลไม่ได้ อนุญาต และทำการหลอกลวงของยืมเงินจากผู้อื่นที่เกี่ยวข้องกับสื่อสังคมออนไลน์นั้น ๆ



ภาพที่ 1 กรณีตัวอย่างหลอกให้โอนเงินค่าสินค้าล่วงหน้า

1.2 การศึกษาช่องทางการรับแจ้งเหตุในปัจจุบัน

กรณีที่ถูกมิจฉาชีพทำการฉ้อโกงผ่านช่องทางออนไลน์ ผู้เสียหายสามารถเข้าแจ้งความเพื่อดำเนินคดีกับผู้ขายที่ฉ้อโกงได้ โดยช่องทางในการรับแจ้งเหตุที่เกิดจากการฉ้อโกงออนไลน์ มีดังนี้ 1) เว็บไซต์ Blacklistseller ช่องทางนี้จะเป็นการแจ้งเตือนผู้ซื้อสินค้าออนไลน์ โดยรวบรวมข้อมูลผู้ที่ได้รับ

ความเดือดร้อนจากการซื้อสินค้าออนไลน์ หรือการโอนเงินผ่าน E-Banking เข้ามาแจ้งรายละเอียดให้ผู้อื่น ถือเป็นเว็บไซต์ที่มีข้อมูลจากผู้เสียหายมากที่สุด, 2) สถานีตำรวจ ช่องทางนี้ จะใช้แจ้งความร้องทุกข์ต่อพนักงานสอบสวน สำหรับผู้เสียหายที่ต้องการเอาผิดกับผู้ต้องหา, 3) กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (TCSD) เป็นหน่วยงานสำหรับสืบสวนสอบสวนป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี, 4) ศูนย์รับเรื่องร้องเรียนปัญหาออนไลน์ 1212 OCC เป็นอีกช่องทางหนึ่งสำหรับการรับเรื่องร้องเรียน ดำเนินการภายใต้โครงการขับเคลื่อนเศรษฐกิจและสังคมดิจิทัล ที่กระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม มอบหมายให้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ มีเป้าหมายสำหรับรับเรื่องร้องเรียนปัญหาที่เกิดจากการซื้อขายทางออนไลน์ รวมถึงการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ สามารถแจ้งได้หลายช่องทาง เช่น โทรศัพท์ เว็บไซต์ อีเมล ข้อความ

1.3 การทบทวนวรรณกรรมในประเทศที่เกี่ยวข้อง

จากการทบทวนวรรณกรรมในประเทศที่เกี่ยวข้อง ที่ได้จากการสืบค้นในฐานข้อมูล Thai Journals Online (ThaiJO) ซึ่งเป็นระบบฐานข้อมูลวารสารอิเล็กทรอนิกส์กลางของประเทศไทย ที่เป็นแหล่งรวมวารสารวิชาการที่ผลิตในประเทศไทยทุกสาขาวิชา ทั้งสาขาวิทยาศาสตร์/เทคโนโลยี และมนุษยศาสตร์และสังคมศาสตร์ ThaiJO ด้วยการค้นหาจากคำสำคัญ เช่น มิจฉาชีพออนไลน์ โกงออนไลน์ เป็นต้น ซึ่งพบบทความวิจัยที่เกี่ยวข้อง ดังต่อไปนี้

สถาบันดำรงราชานุภาพ กระทรวงมหาดไทย (2561) ได้ศึกษารูปแบบหรือพฤติกรรมการหลอกลวงในประเด็นต่างๆ ปัจจุบัน ซึ่งจากการศึกษาพบว่ารูปแบบประเด็นในการหลอกลวงออนไลน์มีดังนี้ 1) การฉ้อโกงหลอกลวงให้ร่วมลงทุนในลักษณะแชร์ลูกโซ่ 2) การฉ้อโกงโดยหลอกลวงให้ทำรายการผ่านตู้เอทีเอ็ม 3) การฉ้อโกงโดยใช้ศาสนาเป็นเครื่องมือหลอกลวงประชาชน 4) การถูกหลอกลวงจากตัวแทนประกันชีวิตหลอกให้ทำประกันผ่านโทรศัพท์ 5) การถูกหลอกลวงจากการให้บริการหวยออนไลน์หลอกลวงผ่านเว็บไซต์ 6) การฉ้อโกงโดยอ้างว่าเป็นเจ้าหน้าที่ในกระบวนการยุติธรรมและหลอกลวงเอาเงินโดยอ้างว่าเพื่อช่วยเหลือทางคดีความ 7) การฉ้อโกงทาง เฟสบุ๊ก มาทำความรู้จักคุ้นเคยและหลอกลวงให้โอนเงินเข้าบัญชี 8) กลโกงการทุจริตจากการซื้อ–ขายที่ดิน การสวมรอยต่างๆ 9) การหลอกลวงฝากให้เข้ารับราชการ

พิรุพห์รัตน์ ศรีแจ่ม และ ธันย์พันธ์ ใคร้วานิช (2561) ได้ทำการวิจัยเกี่ยวกับปัจจัยของกลโกงในการทำธุรกรรมทางการเงินในยุคดิจิทัล ซึ่งจากการวิจัยพบว่ารูปแบบกลโกงทุกธุรกรรมการเงิน มีดังนี้ 1) การถูกแอบอ้าง 2) การสั่งสินค้าแบบออนไลน์ 3) การหลอกให้รางวัล 4) การหลอกอาชีพเสริมออนไลน์ 5) การหลอกเรียกเก็บเงิน 6) การหลอกลวงให้บริจาค จากแบบสอบถามออนไลน์จำนวนทั้งหมดที่เก็บข้อมูลมานั้นมีจำนวน 745 ชุดนำข้อมูลที่ได้มารวบรวมเพื่อประกอบการวิเคราะห์และประมวลผลทดสอบความสัมพันธ์ของตัวแปรด้วยสถิติ Analysis of Variance (ANOVA) พบว่าผู้ตอบแบบสอบถามส่วนใหญ่เสียหายจากการถูกแอบอ้าง จำนวน 745 คน สูญเงินเฉลี่ย 731 บาท รองลงมาคือเสียหายจากการสั่ง

สินค้าจำนวน 744 คน สูญเงินเฉลี่ย 895 บาท ต่อมาคือเสียหายจากรางวัลจำนวน 743 คน สูญเงินเฉลี่ย 814 บาท เสียหายจากการหลอกอาชีพจำนวน 743 คน สูญเงินเฉลี่ย 1,154 บาท เสียหายจากการเรียกเก็บจำนวน 742 คน สูญเงินเฉลี่ย 165 บาท และน้อยที่สุดคือเสียหายจากการบริจาคจำนวน 107 คน สูญเงินเฉลี่ย 66 บาท

กรกนก นิลดำและคณะ (2563) ได้ทำการวิจัยเรื่อง วิธีการกลโกง ช่องทางการสื่อสาร และประสบการณ์ในการถูกมิจฉาชีพออนไลน์หลอกลวงของผู้สูงอายุในจังหวัดเชียงราย โดยใช้แบบสอบถามเป็นเครื่องมือในการศึกษากับกลุ่มผู้สูงอายุตั้งแต่ 50 ปี ขึ้นไป ในพื้นที่จังหวัดเชียงราย จำนวน 400 คน ผลการวิจัยพบว่า วิธีการกลโกงที่มิจฉาชีพออนไลน์ใช้หลอกลวงกลุ่มตัวอย่าง มีดังนี้ 1) การฉ้อโกงโดยหลอกลวงให้ร่วมลงทุนในลักษณะลูกโซ่ ร้อยละ 30.5 2) ฉ้อโกงโดยหลอกลวงให้ทำรายการที่ตู้เอทีเอ็มเพื่อให้โอนเงินไปให้ร้อยละ 27.25 3) ฉ้อโกงโดยส่งอีเมล์มาทำความรู้จักคุ้นเคยและหลอกลวงให้โอนเงินเข้าบัญชีมิจฉาชีพ ร้อยละ 11.75 4) การฉ้อโกงโดยปลอมตัวและปลอมที่อยู่อีเมล์มาหลอกลวงให้โอนเข้าบัญชีมิจฉาชีพ ร้อยละ 8.25 5) การฉ้อโกงโดยอ้างการรักษาพยาบาลมาหลอกลวงเงิน ร้อยละ 6.25 6) การฉ้อโกงโดยอ้างการเรี่ยไรเงินไปช่วยเหลือทางราชการหรือผู้ด้อยโอกาส ร้อยละ 7.00 7) การฉ้อโกงโดยใช้ศาสนาเป็นเครื่องมือในการหลอกลวง ร้อยละ 3.75 8) การฉ้อโกงโดยอ้างอิงวาเป็นเจ้าหน้าที่ในกระบวนการยุติธรรมและหลอกลวงเอาเงิน ร้อยละ 5.25 โดยผู้สูงอายุส่วนใหญ่ถูกหลอกลวงผ่านช่องทางเฟสบุ๊ก ร้อยละ 44 รองลงมาคือ แอพพลิเคชั่นไลน์ ร้อยละ 31.25 และน้อยที่สุดคือ อินสตาแกรม ร้อยละ 5.25 และซึ่งเมื่อผู้สูงอายุรู้ว่าตนเองถูกหลอกลวง ผู้สูงอายุส่วนใหญ่ใช้การโพสต์หรือประกาศลงสื่อออนไลน์เพื่อเปิดเผยตัวมิจฉาชีพ ร้อยละ 46.75 รองลงมาคือ แจ้งความกบพนักงานตำรวจ ร้อยละ 25.75 และน้อยที่สุดคือ การตามเอาเงินคืน ร้อยละ 6.50

ณัฐณิชา คุ้มแพทย์ (2563) ได้ทำการวิจัยเกี่ยวกับการละเมิดสิทธิความเป็นส่วนตัวและสิทธิในชื่อเสียงโดยการประจานในพื้นที่ซื้อขายสินค้าออนไลน์จากการสำรวจสภาพปัญหาในพื้นที่เครือข่ายสังคมออนไลน์ พบว่าผู้ประกอบธุรกิจส่วนใหญ่ที่นำข้อความการสนทนาออนไลน์และข้อมูลของผู้บริโภคมาประจานเกิดจากการที่ผู้บริโภคขอยกเลิกคำสั่งซื้อหรือสั่งซื้อแล้วหายเงียบไปโดยไม่โอนเงินให้แก่ผู้ประกอบธุรกิจ โดยโพสต์ของผู้ประกอบธุรกิจที่เป็นการประจานผู้บริโภคที่สามารถเข้าถึงได้ในขณะนี้สามารถแบ่งออกเป็น 2 กรณีหลัก คือ กรณีแรก ผู้บริโภคได้ขอยกเลิกการสั่งซื้อกับผู้ประกอบธุรกิจ ก็จะถูกประจานด้วยข้อความการสนทนาออนไลน์ที่ผู้บริโภคได้ยกเลิกคำสั่งซื้อ รวมถึงรูปบัญชีเครือข่ายสังคมออนไลน์ของผู้บริโภคอีกด้วย ยิ่งไปกว่านั้นกรณีที่ผู้บริโภคเคยติดต่อซื้อขายกับผู้ประกอบธุรกิจมาก่อน ผู้ประกอบธุรกิจก็จะนำข้อมูลเก่า ๆ ซึ่งอยู่ในเนื้อหาการสนทนาที่ผู้ประกอบธุรกิจบันทึกไว้มาประจานต่อสังคม ส่วนกรณีที่สองเป็นกรณีที่ผู้บริโภคไม่ได้บอกยกเลิกคำสั่งซื้อ แต่หายเงียบไปโดยไม่ได้โอนเงินให้ผู้ประกอบธุรกิจ ผู้บริโภคจะถูกประจานในลักษณะคล้ายกับกรณีแรก ดังนั้น ผู้ประกอบธุรกิจจะต้องมีมาตรการที่จะทำให้ผู้บริโภคมั่นใจว่าความเป็นส่วนตัวและความปลอดภัย

ณัฐธรณ์ เดชสกุล และ จอมเดช ตรีเมฆ (2563) ได้ทำการวิจัยเกี่ยวกับการศึกษาสถานการณ์ในปัจจุบันของการฉ้อโกงซื้อขายสินค้าทางอินเทอร์เน็ต รูปแบบของการฉ้อโกงซื้อขายสินค้าทาง

อินเทอร์เน็ต ปัญหาในกระบวนการยุติธรรมในคดีการฉ้อโกงซื้อขายสินค้าทางอินเทอร์เน็ต และแนวคิดและข้อเสนอแนะเกี่ยวกับการฉ้อโกงซื้อขายสินค้าทางอินเทอร์เน็ตจากการศึกษาวิจัย พบว่า พบว่าเหยื่อในการฉ้อโกงซื้อขายสินค้าทางอินเทอร์เน็ตในประเทศไทยส่วนใหญ่เป็นเพศหญิงซึ่งอยู่ในวัยทำงาน โดยสาเหตุเกิดจากความโลภของเหยื่อ ทำให้เกิดเหยื่อขาดความระมัดระวังตัว นอกจากนี้คนร้ายยังสามารถสร้างความน่าเชื่อถือโดยหลองลวงเหยื่อได้อย่างแนบเนียน ในด้านของปัญหาในกระบวนการยุติธรรม ผลการวิจัยค่อนข้างชัดเจนว่ากระบวนการยุติธรรมมีความล่าช้า เนื่องจากเจ้าหน้าที่ขาดความรู้ความชำนาญมีเจ้าหน้าที่รองรับไม่เพียงพอและความยากในการรวบรวมพยานหลักฐาน ดังนั้นแนวคิดและข้อเสนอแนะของผู้ให้ข้อมูลสำคัญจากการศึกษาในครั้งนี้ส่วนใหญ่มีแนวคิดว่าการให้ความรู้แก่เหยื่อและเจ้าหน้าที่ผู้ปฏิบัติงานในกระบวนการยุติธรรมนั้นสามารถแก้ไขปัญหาได้

1.4 การเว็บไซต์ที่มีการให้ข้อมูลเกี่ยวกับมิจฉาชีพออนไลน์

เว็บไซต์ฉลาดโอนได้ทำการรวบรวมข้อมูลจากเว็บไซต์มาเป็นข้อมูลประกอบการพิจารณาเพื่อใช้ในการพัฒนาระบบให้มีประสิทธิภาพมากที่สุด โดยได้ทำการรวบรวมข้อมูลจากเว็บไซต์ต่างๆ ดังนี้

Scamwatch (2565) เป็นเว็บไซต์ที่จัดตั้งขึ้นโดยดำเนินการคณะกรรมการของ (Australian Competition and Consumer Commission: ACCC) ซึ่งเว็บไซต์นี้ให้ข้อมูลแก่ธุรกิจขนาดเล็กและผู้บริโภคเกี่ยวกับวิธีการรับรู้กลโกง หลีกเลี่ยง และรายงาน

Canadian Anti-Fraud Centre (2565) เป็นเว็บไซต์ศูนย์ต่อต้านการทุจริตของแคนาดาเพื่อรวบรวมข้อมูลเกี่ยวกับการฉ้อโกงและการโจรกรรมข้อมูลประจำตัวของมิจฉาชีพออนไลน์ โดยเว็บนี้จะให้ข้อมูลเกี่ยวกับการหลอกลวงในอดีตและการหลอกลวงในปัจจุบันที่มีผลกระทบกับผู้บริโภค

Citizensadvice (2565) เป็นเว็บไซต์ที่ให้ข้อมูลทั่วไปให้แต่พลเมืองสหราชอาณาจักรโดยหมวดหมู่ส่วนใหญ่จะเป็นข้อมูลเกี่ยวกับการหลอกลวงมิจฉาชีพออนไลน์เพื่อเตือนการผู้บริโภคในสหราชอาณาจักร

Actionfraud (2565) เป็นเว็บไซต์รายงานระดับชาติของสหราชอาณาจักรในการเป็นศูนย์กลางการฉ้อโกงออนไลน์และอาชญากรรมทางอินเทอร์เน็ต ที่ผู้เสียหายเกิดการฉ้อโกงทางออนไลน์หรือมีอาชญากรรมไซเบอร์ หลอกลวง เกิดขึ้นให้เข้ามารายงานหรือแจ้งข้อมูลต่างๆ

The National Cyber Security Centre (2565) เป็นเว็บไซต์นี้ที่สนับสนุนองค์กรที่สำคัญในสหราชอาณาจักร ภาครัฐ อุตสาหกรรม SMEs และทั่วไปในวงกว้างสาธารณะ โดยเว็บไซต์นี้มีช่องทางในการรายงานเหตุการณ์และให้การตอบสนองต่อเหตุการณ์เพื่อลดอันตรายแก่ประชาชนอย่างมีประสิทธิภาพ

Scamalert (2565) เป็นเว็บไซต์นี้ดำเนินการโดยสภาป้องกันอาชญากรรม (คสช.) ของรัฐบาลสิงคโปร์องค์กรนี้ซึ่งเป็นองค์กรไม่แสวงหาผลกำไร มุ่งมั่นที่จะส่งเสริมความปลอดภัยให้แก่ประชาชนและสร้างความตระหนักเกี่ยวกับอาชญากรรมและเผยแพร่แนวทางช่วยเหลือตนเองในการเกิดอาชญากรรมการป้องกัน รวมถึงผู้เยหายสามารถแบ่งปันเรื่องราวได้ อีกทั้งมีฟังก์ชันโทรสายด่วนต่อต้านการหลอกลวงสำหรับการให้คำปรึกษาแก่ประชาชนอีกด้วย

VerMe (2565) เว็บไซต์นี้เป็นเว็บไซต์ที่มีการพัฒนามาเป็นแพลตฟอร์มเพื่อใช้ในการยืนยันตัวตนผู้ขายของออนไลน์ตาม Facebook, Line, Instagram, Twitter และเว็บบอร์ดต่างๆ เพื่อให้ผู้ซื้อมั่นใจว่าชำระเงินกับคนที่มีตัวตนจริงๆ โดยผู้ขายจะมี บัตร VerME ในการยืนยันตัวตนว่าเป็นผู้ขายจริงไม่ใช่มิจฉาชีพ ทางฝั่งผู้ซื้อสามารถนำ ID บนบัตร VerME ของผู้ขายไปตรวจสอบได้เพื่อให้เกิดความมั่นใจในการซื้อขาย

Blacklistseller (2565) เว็บไซต์นี้ เป็นเว็บไซต์ที่ร่วมต้านภัยฉ้อโกงออนไลน์โดนผู้เสียหายที่โดนมิจฉาชีพออนไลน์โกงเงินสามารถนำข้อมูลเหล่านั้นมาสร้างเป็นรายงานและฐานข้อมูลเพื่อช่วยในการเตือนสังคมป้องกันไม่ให้มีผู้โดนหลอกเพื่อมากขึ้น

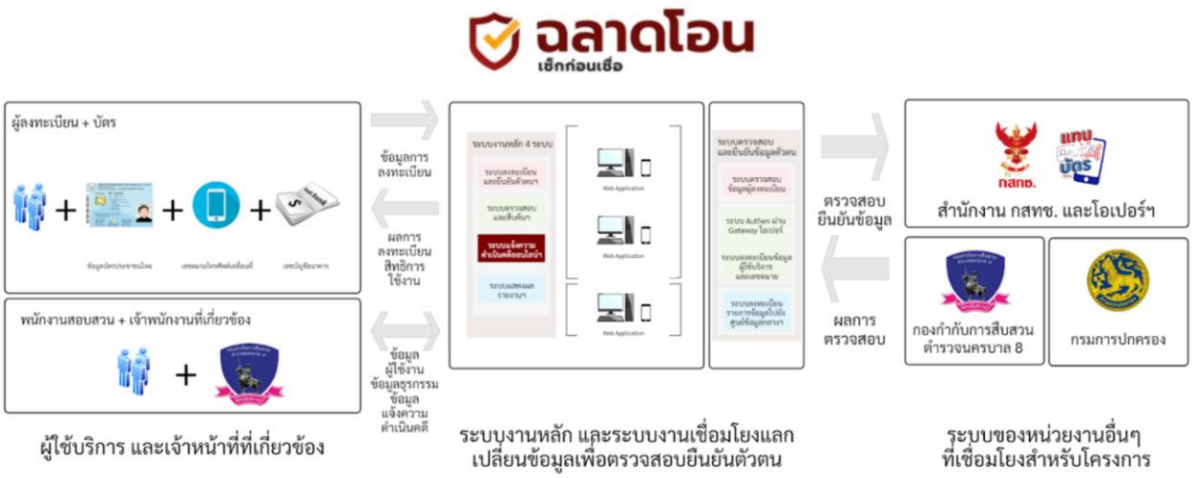
เช็คคนโกง (2565) เว็บไซต์นี้เป็นเว็บไซต์เว็บไซต์สำหรับเช็คคนโกง หลอกให้โอนเงินสำหรับการซื้อของออนไลน์ ผู้ใช้ควรเช็คก่อนโอนเงิน ผู้ที่โดนโกงสามารถโพส ใส่ข้อมูลไม่ครบถ้วน เช่น ชื่อ นามสกุล บัญชีที่โอน วันที่โอน หลักฐานการแจ้งความ หรือข้อมูลการแชท ที่ช่วยให้ผู้ซื้อทำการเช็คคนโกงได้ก่อนการโอนเงิน โดยเช็คให้ชัวร์ก่อนโอน เช็คชื่อ เช็คเลขที่บัญชี เช็คเบอร์โทรศัพท์ เช็คทุกอย่างที่ทราบข้อมูล ลองค้นหาใน Google หรือ Facebook แม้กระทั่ง Twitter แล้วนำข้อมูลเหล่านั้นมาเช็คในเว็บคนโกง

Whoscheat (2565) เว็บไซต์นี้เป็นเว็บไซต์สำหรับตรวจสอบข้อมูลมิจฉาชีพออนไลน์เช่นกัน โดยในระบบมีการทำการตรวจสอบเลขบัญชีธนาคารของมิจฉาชีพ เบอร์โทรศัพท์มือถือ เลขประจำตัวประชาชน และชื่อ-นามสกุล ของมิจฉาชีพ เพื่อเป็นการป้องการให้ไม่โดนโกงเช่นกัน

Pantipmarket (2565) เว็บไซต์นี้เป็นเว็บไซต์สำหรับซื้อขายของออนไลน์ซึ่งการซื้อขายของในหลายสินค้าและหมวดเช่นเดียวกัน ตัวอย่าง ซื้อ-ขายอสังหาริมทรัพย์ ซื้อ-ขายพระเครื่อง ซื้อ-ขายยานพาหนะ ซื้อ-ขายคอมพิวเตอร์ และอื่นๆ มากมาย ซึ่งนอกจากเว็บไซต์ pantipmarket จะเป็นแพลตฟอร์มจะสร้างพื้นการซื้อ-ขายสินค้าต่างๆ ตัวระบบยังมีการสร้างรายการเลขที่บัญชีที่หลอกลวงและรายการสินค้าที่ถูกขโมย อีกด้วย

จากการทบทวนวรรณกรรมรวมถึงการรวบรวมเว็บไซต์ต่างๆ ที่มีการให้ข้อมูลเกี่ยวกับมิจฉาชีพออนไลน์ คนโกง คนหลอกลวง พบว่าเว็บไซต์ต่างๆ ที่มีอยู่ในประเทศไทย ณ ตอนนี้ไม่ได้มีการจับมือกับตำรวจและกรมการปกครองแต่อย่างใด ทำให้ไม่มีการสานต่อช่วยในการดำเนินคดี และจากการศึกษาทบทวนวรรณกรรม ทำให้ผู้วิจัยได้ทำการเก็บข้อมูลที่เป็นประโยชน์มาเป็นข้อมูลในการพัฒนาเป็นระบบเว็บไซต์ของฉลาดโอนเกิดขึ้นโดยใช้งานได้ทั้งบนคอมพิวเตอร์และมือถือ โดยตัวระบบของเว็บไซต์ฉลาดโอนสามารถตรวจสอบข้อมูลของผู้รับโอน ก่อนเชื่อ ก่อนโอนได้ซึ่งจะเช็ค ชื่อบัญชีธนาคาร เลขที่บัญชีธนาคาร/พร้อมเพย์/ทรูวอลเล็ต SMS หรือเบอร์โทร และเช็คตัวตนผู้ขาย อีกทั้งยังช่วยรวบรวมหลักฐานจากผู้โดนโกงเพื่อนำไปดำเนินคดีต่อไปได้

ขั้นตอนที่ 2) เป็นขั้นตอนการดีไซน์ (Design) ซึ่งขั้นตอนนี้เป็นการนำข้อมูลในขั้นตอนที่ 1 ทำการวิเคราะห์ความต้องการ (Requirement Analysis) จนได้ผลลัพธ์ออกมาเป็นการออกแบบระบบเว็บไซต์ฉลาดโอนและสร้างระบบฐานข้อมูลมิจฉาชีพออนไลน์ดังภาพที่ 2



ภาพที่ 2 หน้าตาสรุปการวิเคราะห์ความต้องการของระบบ

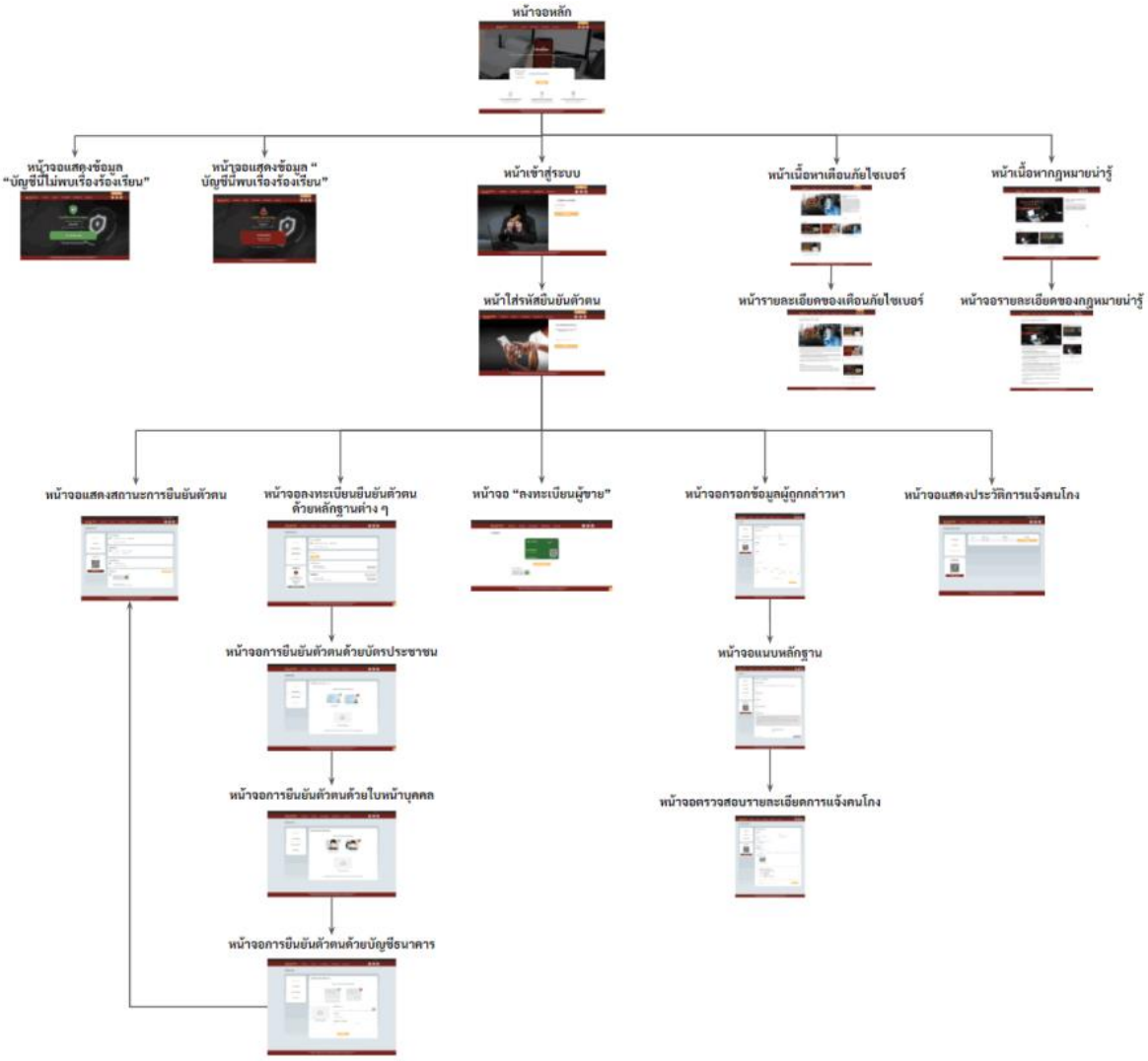
ขั้นตอนที่ 3) เป็นขั้นตอนการดำเนินการ (Implementation) ซึ่งเป็นขั้นตอนในการเขียนโปรแกรม (Coding) ตามการออกแบบในขั้นตอนที่ 2 ที่ได้ดีไซน์วิเคราะห์ความต้องการไว้ดังภาพที่ 3

ขั้นตอนที่ 4) เป็นขั้นตอนทดสอบการทำงานของระบบ (Testing) เมื่อทำการเขียนโปรแกรมเสร็จก็ทำการทดสอบโปรแกรมที่พัฒนาขึ้นเพื่อหาข้อผิดพลาดในการพัฒนาโปรแกรม ซึ่งขั้นตอนนี้ เมื่อพัฒนาโปรแกรมเสร็จแล้วนำไปทดลองใช้กับกลุ่มตัวอย่าง 30 คน เพื่อหาจุดบกพร่องและจุดที่ต้องปรับปรุงของระบบเว็บไซต์ฉลาดโอนและสร้างระบบฐานข้อมูลมิจฉาชีพออนไลน์

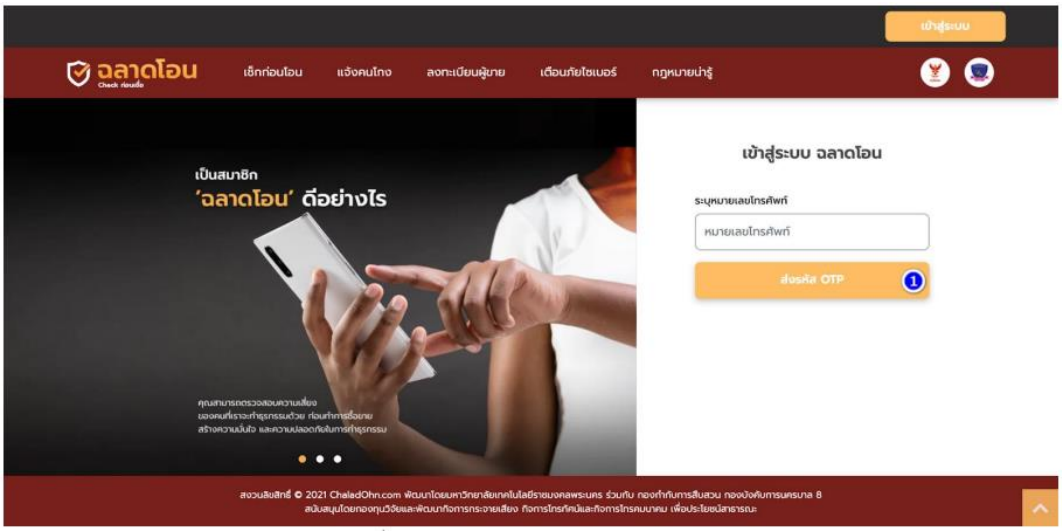
ขั้นตอนที่ 5) เป็นขั้นตอนการนำระบบเว็บไซต์ฉลาดโอนและสร้างระบบฐานข้อมูลมิจฉาชีพออนไลน์ไปเผยแพร่ใช้งานจริงดังภาพที่ 4

ขั้นตอนที่ 6) เป็นระบบเว็บไซต์ฉลาดโอนและสร้างระบบฐานข้อมูลมิจฉาชีพออนไลน์เริ่มใช้งานจริงถ้ามีข้อผิดพลาดเมื่อเจอข้อผิดพลาด (Error) และความต้องการใหม่ที่ต้องการ เพื่อให้ไปสู่การแก้ไขข้อผิดพลาดและพัฒนาซอฟต์แวร์ตามความต้องการใหม่ในอนาคต

ระยะที่ 2 เป็นการประเมินความพึงพอใจต่อระบบเว็บไซต์ฉลาดโอนและสร้างระบบฐานข้อมูลมิจฉาชีพออนไลน์โดยใช้แบบประเมินความพึงพอใจในระบบออนไลน์ผ่าน Google Form ไปสอบถามข้อมูลจากผู้ใช้เว็บจริงจำนวน 72 คน



ภาพที่ 3 ภาพขั้นตอนขอบเขตการดำเนินการพัฒนาโปรแกรม



ภาพที่ 4 ภาพเว็บไซต์หน้าแรกของระบบในการใช้งานจริง

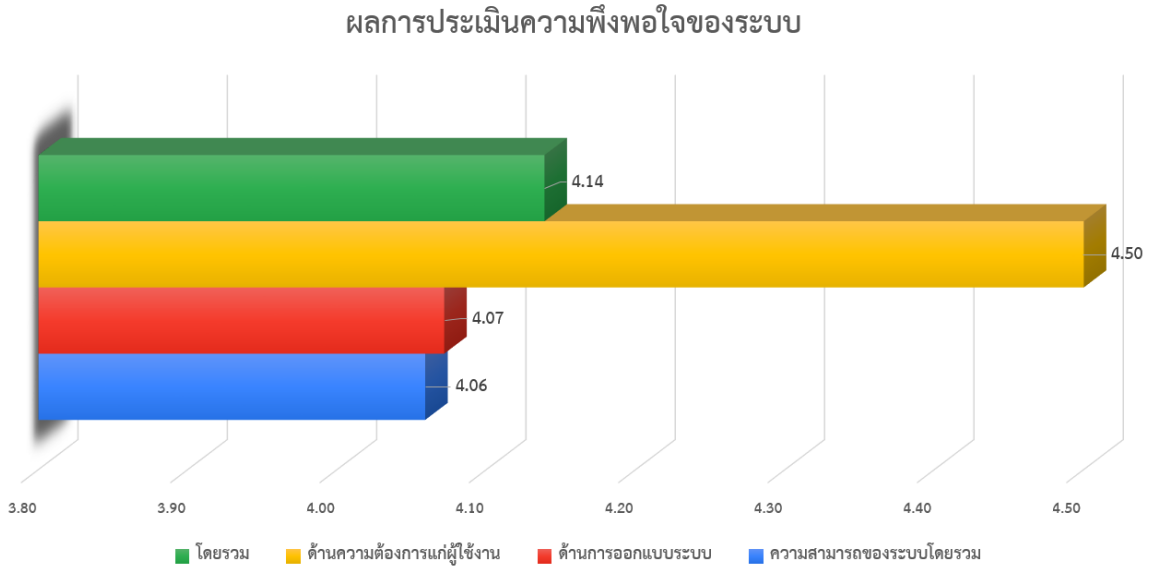
ผลการศึกษา

ผลการศึกษาทั้ง 2 ระยะมีผลการศึกษาดังนี้

ผลระยะที่ 1 ในการพัฒนาระบบเว็บไซต์ฉลาดโอนและสร้างระบบฐานข้อมูลมิจฉาชีพออนไลน์ในการใช้เป็นเครื่องมือช่วยลดปัญหาการหลอกลวง การฉ้อโกง จากมิจฉาชีพออนไลน์ สามารถพัฒนาได้จริงและสามารถใช้งานได้จริงโดยสามารถเข้าผ่าน URL: https://www.ฉลาดโอน.com ซึ่งในระบบแต่ฟังก์ชันการใช้งานสามารถใช้งานได้จริงและครบถ้วน ตัวอย่างเช่น ฟังก์ชันตรวจสอบข้อมูลของผู้รับโอนก่อนเชื่อ ก่อนโอน, ฟังก์ชันแจ้งคนโกง, ฟังก์ชันช่วยรวบรวมหลักฐาน, ฟังก์ชันเช็คตัวตนผู้ขาย และฟังก์ชันอื่นๆ เป็นต้น อีกทั้งระบบเว็บไซต์ฉลาดโอนและสร้างระบบฐานข้อมูลมิจฉาชีพออนไลน์ในการใช้เป็นเครื่องมือช่วยลดปัญหาการหลอกลวง การฉ้อโกง จากมิจฉาชีพออนไลน์ ที่พัฒนาขึ้นสามารถนำไปช่วยในเกิดการจับคุมมิจฉาชีพออนไลน์ได้จริง ดังภาพที่ 5

ภาพที่ 5 ภาพเว็บไซต์ฉลาดโอนนำไปสู่การจับฐานข้อมูลมิจฉาชีพออนไลน์

ผลระยะที่ 2 การประเมินความพึงพอใจต่อระบบเว็บไซต์ฉลาดโอนและสร้างระบบฐานข้อมูลมิจฉาชีพออนไลน์ในการใช้เป็นเครื่องมือช่วยลดปัญหาการหลอกลวง การฉ้อโกง จากมิจฉาชีพออนไลน์ จากผู้ใช้งานจริง 72 คน พบว่า ด้านความสามารถประสิทธิภาพของระบบ มีความพึงพอใจมาก (Mean = 4.06, S.D. = 0.88) ด้านการออกแบบระบบ มีความพึงพอใจมาก (Mean = 4.07, S.D. = 0.81) ด้านความต้องการแก่ผู้ใช้งาน มีความพึงพอใจมากที่สุด (Mean = 4.50, S.D. = 0.83) และด้านภาพรวมของระบบมีความพึงพอใจมาก (Mean = 4.14, S.D. = 1.01) ดังภาพที่ 6



ภาพที่ 6 การสรุปผลการประเมินความพึงพอใจต่อระบบ

สรุปผลการศึกษาและอภิปรายผล

จากผลการวิจัยในครั้งนี้พบว่าระบบเว็บไซต์ฉลาดโอนและสร้างระบบฐานข้อมูลมิจฉาชีพออนไลน์ในการใช้เป็นเครื่องมือช่วยลดปัญหาการหลอกลวง การฉ้อโกง จากมิจฉาชีพออนไลน์ ที่ได้พัฒนาขึ้นสามารถนำไปใช้งานได้จริงและมีประสิทธิภาพสูงมากกว่าเว็บไซต์อื่นๆ ที่มีมาก่อนหน้านี้ เนื่องจากระบบเว็บไซต์ฉลาดโอนมีการเก็บรวบรวมการดำเนินงานอย่างเป็นระบบโดยมีการศึกษาและเก็บข้อมูลจากหลายภาคส่วน ก่อนที่จะนำมาพัฒนาระบบ โดยมีการประชุมสัมมนารับฟังความคิดเห็นจากผู้แทนหน่วยงานต่างๆ ยกตัวอย่างเช่น กองบังคับการตำรวจนครบาล 8, สำนักงานกฎหมายและคดี สำนักงานตำรวจแห่งชาติ, กองป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, สถาบันเพื่อการยุติธรรมแห่งประเทศไทย สถาบันเพื่อการยุติธรรมแห่งประเทศไทย, สำนักบริหารและจัดการเลขหมายโทรคมนาคม กสทช., สำนักอนุญาตประกอบกิจการโทรคมนาคม 2 กสทช., สำนักงานป้องกันและปรามการฟอกเงิน, สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ, บริษัทเอซิสโปรเฟสชั่นนัล เซ็นเตอร์ จำกัด, บริษัท ดีแทค ไตรเน็ต จำกัด และบริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด เป็นต้น จากนั้นเมื่อพัฒนาข้อมูลระบบเว็บไซต์ฉลาดโอนและสร้างระบบฐานข้อมูลมิจฉาชีพออนไลน์เสร็จแล้ว ระบบนี้ได้ถูกนำไปใช้เป็นเครื่องมือช่วยลดปัญหาการหลอกลวง การฉ้อโกง จากมิจฉาชีพออนไลน์ และยังมีขยายผลโดยเจ้าหน้าที่ตำรวจในการติดตามการจับกุมผู้ต้องหาคดีฉ้อโกงที่ปรากฏในระบบ

จากการพัฒนาระบบเว็บไซต์ฉลาดโอนและสร้างระบบฐานข้อมูลมิจฉาชีพออนไลน์ จะเห็นได้ว่าเป็นประโยชน์อย่างมากในการตรวจสอบข้อมูลของผู้รับโอน ก่อนเชื่อ ก่อนโอน, การแจ้งคนโกง, การช่วยรวบรวมหลักฐาน และการเช็คตัวตนผู้ขาย เพื่อเป็นการลดปัญหาการหลอกลวง หรือการฉ้อโกง จาก

มิจฉาชีพออนไลน์ได้ นอกจากนี้ยังเป็นเครื่องมือช่วยเจ้าหน้าที่ตำรวจในการติดตามจับกุมผู้ต้องหาได้ด้วย

กิตติกรรมประกาศ

ขอขอบคุณเงินทุนสนับสนุนเงินจากกองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะ ขอบคุณ มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร ขอบคุณ กองบังคับการตำรวจนครบาล 8 และขอขอบคุณผู้ทรงคุณวุฒิในการเข้าร่วมประชุมสัมมนาทุกท่านเป็นอย่างสูง

เอกสารอ้างอิง

กรกนก นิลดำ, เสริมศิริ นิลดำ, อิงดอย ศรีลาพัฒน์, ภควัฒน์ สวนงาม, วรักษณ์กมล มงคลอัศศิริ และ ปฐมพร ปัญญะติ. (2563). วิธีการกลโกง ช่องทางการสื่อสาร และประสบการณ์ในการถูกมิจฉาชีพออนไลน์หลอกลวงของผู้สูงอายุ ในจังหวัดเชียงราย. **CRRU Journal of Communication Chiang Rai Rajabhat University**, 3(3), 50–67.

เช็คคนโกง. (2565). **เช็คคนโกงออนไลน์. เช็คคนโกง.** Retrieved May 15, 2022, https://เช็คคนโกง.com/

ณัฐณิชา คุ้มแพทย์. (2563). การละเมิดสิทธิความเป็นส่วนตัวและสิทธิในชื่อเสียงโดยการประจาน ในพื้นที่ซื้อขายสินค้าออน ไลน์. **CMU Journal of Law and Social Sciences,** 13(1), 24-53**.**

ณัฐธรณ์ เดชสกุล และ จอมเดช ตรีเมฆ. (2563). ปัญหาการฉ้อโกงซื้อขายสินค้าทางอินเทอร์เน็ตในประเทศไทย. **งานประชุมวิชาการระดับชาติมหาวิทยาลัยรังสิตประจำปี 2563,** 1141-1151.

ธนาคารแห่งประเทศไทย. (2564). **การชำระเงินผ่านระบบการชำระเงินและช่องทางต่าง ๆ**. Retrieved May 15, 2022, from https://www.bot.or.th/App/BTWS_STAT/statistics/ReportPage.aspx?reportID=681&language=th

พิรุฬห์รัตน์ ศรีแจ่ม และ ธันย์พันธ์ ใครัวานิช. (2563). กลโกงการทำธุรกรรมทางการเงินในยุคดิจิทัล. **การประชุมวิชาการระดับชำติครั้งที่ 15 และเครือข่ายวิจัยประชำชื่น ครั้งที่ 5 โลกไร้พรมแดน: ทิศทางการศึกษา สุขภาวะ และนวัตกรรม,** วิทยาลัยครุศาสตร์ร่วมกับสายงานวิจัยและพัฒนา มหาวิทยาลัยธุรกิจบัณฑิตย์.

สถาบันดำรงราชานุภาพ กระทรวงมหาดไทย. (2561). รูปแบบ/พฤติกรรมการหลอกลวงในปัจจุบัน ใช้ประกอบในการลงพื้นที่ครั้งที่ 2 ของทีมขับเคลื่อนฯ ระดับตำบล ป้องกันไม่ให้ประชาชนถูกหลอกในรูปแบบต่างๆ โดยเชื่อมโยง ประเด็นความรู้หัวข้อ วิถีไทย วิถีพอเพียง และรู้สิทธิรู้

หน้าที่ รู้กฎหมาย. **สถาบันดำรงราชานุภาพ สำนักงานปลัดกระทรวงมหาดไทย**, กระทรวงมหาดไทย.http://www.stabundamrong.go.th/web/thainiyom/deceive.pdf

สุรพงษ์ ชัยจันทร์. (2561). **การปฏิบัติงานเชิงรุกเพื่อการป้องกนัอาชญากรรมตำรวจภูธรภาค 7**. Retrieved May 15, 2022, from http://www.dsdw2016.dsdw.go.th/doc_pr/ndc_2560-2561/PDF/8575s/รวม.pdf

Actionfraud. (2565). **News & Alerts**. Retrieved May 15, 2022, https://www.actionfraud.police.uk/

Blacklistseller. (2565). **อ่าน Blacklistseller ศูนย์กลางการตรวจสอบการฉ้อโกงออนไลน์.** Retrieved May 15, 2022, https://www.blacklistseller.com/home/admin_volunteer

Canadian Anti-Fraud Centre. (2565). **Recent scams and fraud.** Retrieved May 15, 2022, https://www.antifraudcentre-centreantifraude.ca/index-eng.htm

Citizensadvice. (2565). **Consumer: Scams.** Retrieved May 15, 2022, https://www.citizensadvice.org.uk/consumer/

Datareportal. (2020). **DIGITAL 2020: THAILAND**. Retrieved May 15, 2022, from https://datareportal.com/reports/digital-2020-thailand

Gimme. (2562). **สัดส่วนผู้คนซื้อขายของผ่านทางมือถือ**. Retrieved May 15, 2022, from https://droidsans.com/thailand-world-top-mobile-purchase/

Nalisa. (2562). **เทรนด์ช้อปปิ้งผ่านแชทออนไลน์มากที่สุดในโลก**. Retrieved May 15, 2022, from https://marketeeronline.co/archives/131754

Pantipmarket. (2565). **ซื้อ-ขาย ของออนไลน์บน pantipmarket.** Retrieved May 15, 2022, https://www. pantipmarket.com/

Scamalert. (2565). **Spot the Scam Signs.** Retrieved May 15, 2022, https://www.scamalert.sg/

Scamwatch. (2565). **News and alerts: Scams Awareness Week 2021**. Retrieved May 15, 2022, https://www.scamwatch.gov.au/

The National Cyber Security Centre. (2565). **Helping to make the UK the safest place to live and work online.** Retrieved May 15, 2022, https://www.ncsc.gov.uk/

Verme. (2565). **บริการยืนยันตัวตนผู้ขายของออนไลน์.** Retrieved May 15, 2022, from https://verme.me/how-to

Whoscheat. (2565). **เช็คคนโกง - ตรวจสอบคนโกง บัญชีมิจฉาชีพให้ชัวร์ก่อนโอนเงิน.** Retrieved May 15, 2022, https://www.whoscheat.com/