รายงานเบื้องต้น (Inception Report)

โครงการขอรับการส่งเสริมและสนับสนุนจากเงินกองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะ
ประเภทที่ ๑/๒๕๕๘ ประจำงวดที่ ๑

โครงการการสร้างความตระหนักรู้ให้กับประชาชนเกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์

ผศ.ดร. วรวัฒน์ เชิญสวัสดิ์
(ผู้รับผิดชอบโครงการ)

ได้รับทุนอุดหนุนจาก
กองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะ
(สำนักงาน กสทช.)

รายงานเบื้องต้น		
ชื่อโครงการ	โครงการการสร้างความตระหนักรู้ให้กับประชาชนเกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์	
ข้อมูลโครงการ	รหัสอ้างอิง: B2-2-09/58	
	วันเริ่มต้นโครงการ: 10 เมษายน 2560	
	วันสิ้นสุดโครงการ: 9 เมษายน 2561	
หน่วยงานผู้รับทุน	มหาวิทยาลัยกรุงเทพ	วิทยาเขตกล้วยน้ำไท เลขที่ 119 ถนนพระราม 4 แขวงพระโขนง เขตคลองเตย กรุงเทพฯ 10110 โทรศัพท์ 02-350-3500 ต่อ 1693 ติดต่อ **ผศ.ดร.วรวัฒน์ เชิญสวัสดิ์** (หัวหน้าโครงการ)
คณะผู้ดำเนินโครงการ	ผู้ช่วยศาสตราจารย์ ดร. วรวัฒน์ เชิญสวัสดิ์ (มหาวิทยาลัยกรุงเทพ) ผู้ช่วยศาสตราจารย์ ดร. กิ่งกาญจน์ สุขคณาภิบาล (มหาวิทยาลัยกรุงเทพ) รองศาสตรจารย์ ดร.ประสงค์ ปราณีตพลกรัง (มหาวิทยาลัยศรีปทุม)	
ข้อมูลรายงานที่ส่ง	วันที่ส่งรายงานเบื้องต้น (งานงวดแรก): 10 พฤษภาคม 2560	
	จัดทำรายงานและนำเสนอโดย: มหาวิทยาลัยกรุงเทพ	

สารบัญ

บทที่ 1 บทนำ

1.1 หลักการและเหตุผลความจำเป็น

ความมั่นคงปลอดภัยด้านไซเบอร์เป็นเรื่องสำคัญยิ่งในโลกยุคดิจิทัลเห็นได้จากการเติบโตของตลาดเทคโนโลยีการสื่อสารการใช้โทรศัพท์มือถือของประชากรไทยเพิ่มสูงขึ้นตั้งแต่ พ.ศ. 2552 จนถึง 2556 โดยมีอัตราการเพิ่มขึ้นร้อยละ 4.14 ในแต่ละปี (ข้อมูลจากสำนักงานสถิติแห่งชาติ ปี พ.ศ. 2557) ค่ายผู้ให้บริการหลักโทรศัพท์มือถือในปัจจุบันได้สรุปยอดผู้ใช้งานมือถือประเทศไทยปี 2558 ทั้งหมด 91.9 ล้านเลขหมาย (โดยแบ่งเป็น AIS 42, DTAC 28.4 และ TrueMove 21.5 ล้านเลขหมาย ข้อมูลจาก www.daat.in.th) ปัจจุบันการใช้โทรศัพท์มือถือเป็นสมาร์ทโฟนที่สามารถเชื่อมต่ออินเทอร์เน็ต เพื่ออำนวยความสะดวกให้ผู้ใช้ทำกิจกรรมต่างๆได้มากมาย เช่น การรับส่งอีเมล์ การถ่ายภาพและเผยแพร่ในเฟซบุ๊ค การโพสต์ข้อความติชมให้กับเพื่อนในเครือข่ายสังคมออนไลน์ การอ่านข่าวและโพสต์ความเห็นในเว็บไซต์ การซื้อขายสินค้าออนไลน์ การทำธุรกรรมธนาคาร เป็นต้น การเข้าถึงอินเทอร์เน็ตจึงเป็นปัจจัยหนึ่งในชีวิตประจำวันซึ่งให้ความสะดวกสบาย ความเพลิดเพลิน และยังเป็นแหล่งความรู้ที่สำคัญ แต่ผู้ใช้จำเป็นต้องมีความรู้เรื่องความมั่นคงปลอดภัยในการใช้คอมพิวเตอร์และเทคโนโลยีการสื่อสาร ซึ่งประกอบด้วยความตระหนักรู้ถึงภัยอันตรายและความเสี่ยง รู้วิธีการป้องกันภัยอันตรายที่อาจจะเกิดขึ้น และรู้วิธีการจัดการกับภัยอันตรายที่เกิดขึ้น

อาชญกรรมไซเบอร์ (อดีตใช้คำว่าอาชญากรรมคอมพิวเตอร์) มีสาเหตุจากผู้ตั้งใจกระทำความผิดและผู้รู้เท่าไม่ถึงการณ์ การรู้เท่าไม่ถึงการณ์ส่วนใหญ่เพราะผู้ใช้งานคอมพิวเตอร์และเทคโนโลยีสื่อสารขาดความตระหนักรู้ถึงความเสี่ยงและภัยอันตรายของการใช้ จากการสำรวจผู้ใช้อินเทอร์เน็ตทั่วไปในสหรัฐอเมริกา (ข้อมูลจากการสำรวจและวิจัยของ Richardson (2011)) พบว่าสถิติของผู้ที่เคยประสบปัญหาเกี่ยวกับความมั่นคงปลอดภัยด้านไซเบอร์ตลอดระยะเวลา 1 ปี (เริ่ม ค.ศ. 2009 ถึง ต้นปี 2010) มีถึงร้อยละ 41.1 จากจำนวนผู้ตอบแบบสอบถามทั้งหมด 285 คน (การสำรวจจากแบบสอบถามซึ่งจัดส่งทางไปรษณีย์และอีเมล์เป็นจำนวน 5,412 ฉบับ (Richardson, 2011)) และในจำนวนผู้ที่เคยมีประสบภัยไซเบอร์เป็นเป้าหมายของการโจมตีถึงร้อยละ 45.6 โดยแบ่งเป็นสามารถระบุได้ 21.6% และไม่สามารถระบุได้ 24.0%

ประเภทของอาชญกรรมทางไซเบอร์ที่ได้รับการแจ้งมากที่สุดในประเทศไทยระหว่าง สิงหาคม 2554 – กรกฎาคม 2555 (ข้อมูลจากบทความ Cyber Threads ปี พ.ศ. 2556 โดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT)) คือการฉ้อฉลหลอกลวงเพื่อผลประโยชน์ รองลงมาคือการพยายามบุกรุกเข้าระบบ ความพยายามรวบรวมข้อมูลของระบบ โปรแกรมไม่พึงประสงค์ และเนื้อหาที่เป็นภัยคุกคามต่อประชาชน เด็กและเยาวชนเป็นกลุ่มผู้ใช้ที่อาจจะถูกหลอกลวงจากมิจฉาชีพผ่านช่องทางสื่อสังคมออนไลน์ได้ไม่ยาก การสร้างความตระหนักรู้ให้กับประชาชนจึงเป็นสิ่งจำเป็นและเร่งเร่งด่วนเพื่อป้องกันอันตรายหรือความเสียหายที่จะเกิดทั้งกับชีวิตและทรัพย์สิน รวมทั้งการสร้างความตระหนักรู้ให้กับผู้ปกครองในการดูแลและสอนบุตรหลานในการใช้อินเทอร์เน็ตอย่างสร้างสรรค์และรู้เท่าทันภัยอันตราย

ถึงแม้ปัจจุบันหน่วยงานรัฐและภาคเอกชนในประเทศไทยได้ตระหนักถึงความสำคัญของความมั่นคงปลอดภัยด้านไซเบอร์ดังเช่น 1) มีการให้ทุนสนับสนุนการวิจัยเรื่องความมั่นคงปลอดภัยด้านไซเบอร์ ในปีงบประมาณ 2556 โดยสำนักวิจัยแห่งชาติ (วช.)อย่างไรก็ตามโครงการวิจัยส่วนใหญ่ที่ได้รับทุนอุดหนุนมุ่งเน้นไปที่การออกแบบและพัฒนาเทคโนโลยี 2) มีการฝึกอบรมและให้ความรู้เรื่องความมั่นคงปลอดภัยด้านไซเบอร์จัดโดยสมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (Thailand Information Security Association: TISA) การ

อบรมนี้มุ่งเน้นไปที่การอบรมและการให้การรับรองบุคลากรภายในองค์กร และมีค่าใช้จ่ายในการฝึกอบรมและสอบวัดผลความรู้ 3) จัดทำหนังสือความรู้ทั่วไปและเอกสารเพื่อเผยแพร่ความรู้เกี่ยวกับความมั่นคงปลอดภัยด้านไซเบอร์จากหลายๆ หน่วยงาน เช่น สำนักพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) และกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) เป็นต้น การเรียนจากหนังสืออาจจะไม่ได้รับการสนใจและไม่สามารถเข้าถึงได้จากทุกกลุ่มผู้ใช้

จากที่กล่าวมา น้ำหนักความสำคัญของความมั่นคงปลอดภัยในด้านไซเบอร์ 1) เน้นการศึกษาและวิจัยเพื่อพัฒนาเครื่องมือป้องกันภัยอันตรายให้กับอุปกรณ์คอมพิวเตอร์และระบบเครือข่าย และ 2) มุ่งให้ความรู้และฝึกอบรมบุคลากรในองค์กรเพื่อลดมูลค่าความเสียหายที่จะเกิดขึ้น จะเห็นว่าประชาชนทั่วไปที่ไม่ได้ทำงานในองค์กรอาจจะไม่สามารถเข้าถึงแหล่งความรู้และไม่ได้รับการฝึกอบรมด้านความมั่นคงปลอดภัยทางไซเบอร์ โครงการวิจัยนี้มุ่งเน้นที่จะเพิ่มช่องทางและวิธีการในการให้ความรู้และสร้างความตระหนักรู้แก่ประชาชนและสังคมถึงความเสี่ยงจากการใช้งานบนโลกไซเบอร์ ภัยคุกคามและอาชญากรรมไซเบอร์ต่างๆ แนวปฏิบัติที่ง่ายและเป็นมาตรฐานเพื่อป้องกันภัยเหล่านั้น รวมถึงการเตรียมความพร้อมให้กับผู้ปกครองที่ไม่มีความรู้ในเรื่องเทคโนโลยี ซึ่งบุตรหลานของตนใช้อินเทอร์เน็ตผ่านคอมพิวเตอร์ หรืออุปกรณ์พกพา

1.2 วัตถุประสงค์ของโครงการ

โครงการวิจัยนี้มุ่งเน้นการสร้างความตระหนักรู้แก้ประชาชน โดยใช้ช่องทางและสื่อที่เหมาะสมกับยุคสมัยปัจจุบัน มุ่งเน้นช่งทางการสื่อสารในเชิงรุก และเน้นการนำเสนอแบบอินเทอร์แอคทีฟที่ผู้ใช้มีส่วนร่วม ซึ่งมีความสอดคล้องกับนโยบายภาครัฐและแผน ดังนี้

1) แผนแม่บทกิจการโทรคมนาคม ฉบับที่ 1 พ.ศ. 2555 - 2559
2) แผนยุทธศาสตร์การวิจัยและพัฒนาเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ฉบับที่ 1 พ.ศ. 2556 - 2560

วัตถุประสงค์ของโครงการมีดังนี้

1) เพิ่มช่องทางและวิธีการในการให้ความรู้และสร้างความตระหนักรู้แก่ประชาชนถึงความเสี่ยงจากการใช้งานบนโลกไซเบอร์ ภัยคุกคามและอาชญากรรมไซเบอร์ต่างๆ
2) พัฒนาสื่อดิจิทัลซึ่งสามารถสื่อสารกับประชาชนทั่วไปให้เกิดความเข้าใจได้ง่ายในแนวปฏิบัติที่ที่เป็นมาตรฐานเพื่อป้องกันภัยคุกคาม
3) สร้างศูนย์การเรียนรู้เสมือนให้กับประชาชนทั่วไปในการตระหนักถึงความเสี่ยงของการใช้งานบนโลกไซเบอร์

1.3 ขอบเขตของโครงการ

ขอบเขตการดำเนินงานที่สำคัญของโครงการ ภายในระยะเวลา 1 ปี มีดังนี้

1) สื่ออินโฟกราฟิกความรู้เรื่องการสร้างความตระหนักรู้ทั้ง 6 หมวด (คำอธิบายในบทที่ 2)
2) ระบบฝึกอบรมเชิงอิเล็กทรอนิกส์ หมายถึง การจัดทำชุดข้อสอบเพื่อสร้างความตระหนักรู้ทั้ง 6 หมวด ในแพลตฟอร์ม e-learning ที่มีอยู่ เช่น Thai Mooc
3) ระบบเกมฝึกอบรมสำหรับเด็กและเยาวชน จำนวน 5 เกม ซึ่งมีกลุ่มเป้าหมายเป็นเด็กและเยาวชน
4) ระบบสืบค้นข้อมูลข่าวเกี่ยวกับอาชญากรรมทางไซเบอร์ รวบรวมข่าวอาชญากรรมทางไซเบอร์และข่าวที่เกี่ยวกับให้ประชาชนได้ตระหนักรู้และระวังภัยที่ผ่านมาล่าสุด 10 ปีที่ผ่านมา พร้อมทั้งเสนอแนะแนวทางป้องกันและจัดการกับภัยคุกคามเหล่านั้น
5) ศูนย์การเรียนรู้เสมือนบนเว็บไซต์และมีการเชื่อมต่อกับสังคมออนไลน์

1.4 ประโยชน์ที่คาดว่าจะได้รับ

กลุ่มเป้าหมายของโครงการนี้มุ่งเน้นผู้บริโภคที่เป็นประชาชนทั่วไปใช้อินเทอร์เน็ต โดยที่ประโยชน์ที่คาดว่าจะได้รับจากโครงการมีดังนี้

1) ทำให้ประชาชนทั่วไปและสังคมมีความตระหนักถึง มีความรู้เกี่ยวกับวิธีป้องกัน และวิธีจัดการภัยอันตรายที่เกิดขึ้นเมื่อเข้าใช้งานระบบคอมพิวเตอร์และการสื่อสาร
2) ใช้เป็นแนวทางเชิงปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ให้กับหน่วยงานรัฐ ภาคเอกชน ผู้ประกอบกิจการและสถานศึกษา
3) ลดปัญหาภัยคุกคามทางไซเบอร์อันนำไปสู่การรักษาผลประโยชน์ด้านเศรษฐกิจ ความปลอดภัยของสังคม และความมั่นคงของประเทศไทยทั้งในปัจจุบันและอนาคตอย่างยั่งยืน

1.5 ตัวชี้วัดผลผลิตและตัวชี้วัดผลลัพธ์

ผลลัพธ์จากโครงการนี้ที่เป็นรูปธรรมคือ การจัดตั้งศูนย์การเรียนรู้เสมือนให้กับประชาชนทั่วไปในการตระหนักถึงความเสี่ยงของการใช้งานบนโลกไซเบอร์ ซึ่งผู้ใช้ที่สามารถเชื่อมต่ออินเตอร์เน็ตก็สามารถเข้าถึงได้ โดยในศูนย์ประกอบด้วย สื่อความรู้ในการสร้างความตระหนักรู้ทั้ง 6 หมวด ระบบฝึกอบรมเชิงอิเล็กทรอนิกส์ ระบบเกมฝึกอบรมสำหรับเด็กและเยาวชน และสืบค้นข้อมูลข่าวเกี่ยวกับอาชญากรรมทางไซเบอร์ รวมทั้งการเชื่อมต่อกับสังคมออนไลน์

สำหรับตัวชี้วัดความสำเร็จ

1) การพัฒนาศูนย์การเรียนรู้และองค์ประกอบในศูนย์เสร็จสมบูรณ์ภายในเวลาที่กำหนด
2) การได้ประเมินผลความพึงพอใจผู้ใช้ต่อศูนย์การเรียนรู้ในระดับดีมาก

ทำให้ประชาชนทั่วไปตระหนักถึง มีความรู้เกี่ยวกับวิธีป้องกันและวิธีจัดการกับภัยอันตรายที่เกิดขึ้นเมื่อเข้าใช้งานระบบคอมพิวเตอร์และการสื่อสาร หน่วยงานรัฐ ภาคเอกชน ผู้ประกอบกิจการ และสถานศึกษาสามารถใช้เป็นแนวทางเชิงปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ ลดปัญหาภัยคุกคามทางไซเบอร์อันนำไปสู่การรักษาผลประโยชน์ด้านเศรษฐกิจ ความปลอดภัยของสังคม และความมั่นคงของประเทศไทยทั้งในปัจจุบันและอนาคตอย่างยั่งยืน

1.6 บุคลากรในโครงการ

บุคลากรในโครงการมีดังนี้

1) หัวหน้าผู้รับผิดชอบโครงการ ผู้ช่วยศาสตราจารย์ ดร. วรวัฒน์ เชิญสวัสดิ์ (มหาวิทยาลัยกรุงเทพ)
2) คณะนักวิจัย
    ก) รองศาสตรจารย์ ดร.ประสงค์ ปราณีตพลกรัง (มหาวิทยาลัยศรีปทุม)
    ข) ผู้ช่วยศาสตราจารย์ ดร.กิ่งกาญจน์ สุขคณาภิบาล (มหาวิทยาลัยกรุงเทพ)

บรรณานุกรม

Richard, Robert. (2011). 2010/2011 CSI Computer Crime and Security Survey. http://reports.informationseek. com/abstract/21/7377/Security/research-2010-2011-csi-survey.html

บทที่ 2
กรอบแนวคิดในการดำเนินงาน รูปแบบหรือวิธีการ และแผนการดำเนินงาน

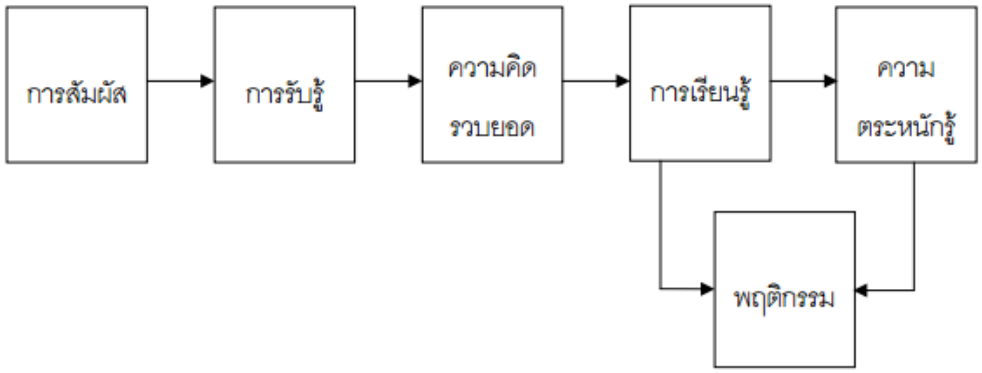
3.1 กรอบแนวคิดในการดำเนินงาน

กลุ่มเป้าหมายของโครงการเป็นประชาชนทั่วไป โดยเน้นไปที่ประชาชนที่ไม่ได้อยู่ในองค์กร เนื่องจากผู้ใช้ระดับองค์กรย่อมมีความตระหนักรู้ถึงความเสี่ยงจากการใช้งานบนโลกไซเบอร์ ภัยคุกคามและอาชญากรรมไซเบอร์ เพราะองค์กรจำเป็นต้องบังคับคนในองค์กรให้ปฏิบัติตามนโยบาย เรียนรู้ขั้นตอนการปฏิบัติ แนวทางการใช้งาน และแนวปฏิบัติที่ดี

ประเด็นสำคัญของการสร้างความตระหนักรู้แก่ประชาชน คือ (1) ช่องทางและวิธีการในการให้ความรู้และสร้างความตระหนักรู้ และ (2) สื่อซึ่งสามารถสื่อสารกับประชาชนทั่วไปให้เกิดความเข้าใจได้ง่ายในแนวปฏิบัติที่ที่เป็นมาตรฐานเพื่อป้องกันภัยคุกคามและอาชญากรรมทางไซเบอร์

ช่องทางในการให้ความรู้ คือศูนย์การเรียนรู้เสมือนซึ่งประกอบด้วย (1) สื่อความรู้ในการสร้างความตระหนักรู้ในรูปแบบอินโฟกราฟิกและแอนิเมชัน (2) ระบบฝึกอบรมเชิงอิเล็กทรอนิกส์ (3) ระบบเกมฝึกอบรมสำหรับเด็กและเยาวชน (4) ระบบสืบค้นข้อมูลข่าวเกี่ยวกับอาชญากรรมทางไซเบอร์ และ (5) การเชื่อมต่อกับสังคมออนไลน์

วิธีการให้ความรู้และการสร้างความตระหนักรู้ ประกอบด้วย การเรียนรู้ผ่านสื่อดิจิทัลในรูปแบบอินโฟกราฟิกและแอนิเมชันซึ่งสามารถสื่อสารกับประชาชนทั่วไปให้เกิดความเข้าใจได้ง่าย จากภาพที่ 1 ความตระหนักรู้เป็นผลมาจากกระบวนการทางปัญญาที่ผู้เรียนได้รับการกระตุ้นจากสิ่งเร้าหรือได้รับการสัมผัสจากสิ่งเร้าแล้วเกิดการรับรู้ และเมื่อรับรู้แล้วได้ความคิดรวบยอดซึ่งนำไปสู่การเรียนรู้ เมื่อมีความรู้แล้วเกิดความตระหนักรู้ในที่สุด



ภาพที่ 1: ขั้นตอนและกระบวนการเกิดความตระหนักรู้

การพัฒนาสื่อดิจิทัล (อินโฟกราฟิกและแอนิเมชัน) ซึ่งสามารถสื่อสารกับประชาชนทั่วไปให้เกิดความเข้าใจได้ง่ายในแนวปฏิบัติที่ที่เป็นมาตรฐาน (ThaiCERT) เพื่อป้องกันภัยคุกคาม โดยที่เนื้อหาของสื่อต้องครอบคลุม 6 หมวด ดังต่อไปนี้

1) การใช้งานสื่อสังคมออนไลน์ (Social Media) อย่างปลอดภัย มีเนื้อหาดังนี้ ประโยชน์ของการใช้สื่อสังคมออนไลน์ วิธีป้องกันภัยจากสื่อสังคมออนไลน์ และการใช้สื่อสังคมออนไลน์อย่างสร้างสรรค์
2) การใช้และจัดตั้งเครือข่ายไร้สายบ้านให้ปลอดภัย มีเนื้อหาดังนี้ ประเภทเครือข่ายไร้สาย ภัยคุกคามที่เกิดขึ้นกับการจัดตั้งบริการเครือข่ายไร้สาย และการจัดตั้งบริการเครือข่ายไร้สายอย่างไรให้ปลอดภัย
3) ไวรัสและมัลแวร์คอมพิวเตอร์ มีเนื้อหาดังนี้ ความหมายและประเภทของไวรัสและมัลแวร์ การตระหนักรู้และป้องกันภัยเบื้องต้น การตรวจสอบ และการกำจัดมัลแวร์ด้วยโปรแกรมแอนติไวรัส
4) การใช้งานโทรศัพท์มือถือให้ปลอดภัยจากภัยคุกคาม มีเนื้อหาดังนี้ ภัยคุกคามบนโทรศัพท์มือถือ ภัยคุกคามที่เกิดจากการใช้งานเว็บไซต์บนโทรศัพท์มือถือ (Web-based Threats) ภัยคุกคามจากการใช้งานเครือข่าย (Network Threats) ภัยคุกคามจากการดูแลรักษาโทรศัพท์ (Physical Threats) ภัยคุกคามจากการใช้ติดตั้งแอปพลิเคชัน แนวทางการปฏิบัติ สำหรับผู้ใช้งานโทรศัพท์มือถือและข้อมูลให้มีความมั่นคงปลอดภัย
5) เล่นอินเทอร์เน็ตอย่างไรให้ปลอดภัยมีเนื้อหาดังนี้ ความหมายและความสำคัญของ HTTP (Hypertext Transfer Protocol) HTTPS (Hypertext Transfer Protocol Secure) การรู้เท่าทันเว็บปลอม (phishing site) และการตั้งรหัสผ่าน
6) ผู้ปกครองเพื่อสอนบุตรหลาน มีเนื้อหาดังนี้ การใช้งานอินเทอร์เน็ตและประโยชน์ ภัยจากการพูดคุยกับคนไม่รู้จักบนโลก ออนไลน์ ภัยจากการให้ข้อมูลส่วนตัว การป้องกันบุตรหลานจากการถูกรังแกทางอินเตอร์เน็ต (Cyber-bullying) แนวทางอย่างง่ายในการป้องกันบุตรหลานจากความเสี่ยง

3.2 วิธีการดำเนินงาน

การดำเนินงานเป็นการผลิตและเผยแพร่สื่อความรู้ที่เข้าใจง่ายให้กับประชาชนผ่านสังคมออนไลน์ ออกแบบและพัฒนาระบบสืบค้นข่าวอาชญากรรมทางไซเบอร์ และรวบรวมข่าวอาชญากรรมทางไซเบอร์และข่าวที่เกี่ยวกับให้ประชาชนได้ตระหนักรู้และระวังภัยที่ผ่านมาล่าสุด 10 ปีที่ผ่านมา พร้อมทั้งเสนอแนะแนวทางป้องกันและจัดการกับภัยคุกคามเหล่านั้น ออกแบบและพัฒนาระบบฝึกอบรมเชิงอิเล็กทรอนิกส์เพื่อสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามและอาชญากรรมทางไซเบอร์ ออกแบบและพัฒนาเกมซึ่งสร้างความเพลิดเพลินพร้อมกับสอนความรู้ในเรื่องภัยคุกคามทางไซเบอร์ที่ใกล้ตัวสำหรับเด็กและเยาวชน

การสร้างศูนย์การเรียนรู้ซึ่งประกอบด้วย (1) สื่อความรู้ในการสร้างความตระหนักรู้ทั้ง 6 หมวด (2) ระบบฝึกอบรมเชิงอิเล็กทรอนิกส์ (3) ระบบเกมฝึกอบรมสำหรับเด็กและเยาวชน (4) ระบบสืบค้นข้อมูลข่าวเกี่ยวกับอาชญากรรมทางไซเบอร์ และ (5) การเชื่อมต่อกับสังคมออนไลน์
ในด้านการผลิตเนื้อหาและสื่อที่เหมาะสมกับประชาชนทั่วไปนั้น โครงการได้จัดตั้งคณะกรรมการผลิตเนื้อหาสื่อ และชุดข้อสอบ ที่ครอบคลุมทั้ง 6 หมวด ศูนย์การเรียนรู้จะแล้วเสร็จภายใน 9 เดือน หลังจากนั้นเป็นการทดสอบการใช้งานและประเมินความพึงพอใจของผู้ใช้

ระเบียบวิธีการวิจัยและปฏิบัติทดลองเพื่อสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ให้กับประชาชน มีวิธีการและขั้นตอนดังนี้ (ตัวเลขในวงเล็บด้านหลังใช้อ้างอิงในแผนดำเนินงาน)

3.2.1การผลิต สื่อดิจิทัล และชุดข้อสอบการสร้างความตระหนักรู้ทางด้านความมั่นคงปลอดภัยทางไซเบอร์

(1) คัดสรรผู้ทรงคุณวุฒิและแต่งตั้งคณะกรรมการผู้ทรงคุณวุฒิ ในการพิจารณาเนื้อหาเพื่อผลิตสื่อดิจิทัล โดยคณะกรรมการผู้ทรงคุณวุฒิประกอบด้วย
- ผู้ทรงคุณวุฒิด้านคอมพิวเตอร์และเทคโนโลยีการสื่อสารจากหน่วยงานภาครัฐและภาคเอกชน
- ผู้ทรงคุณวุฒิด้านความมั่นคงปลอดภัยทางไซเบอร์
- ผู้ทรงคุณวุฒิด้านประชากรและสังคมศาสตร์
- ผู้ทรงคุณวุฒิด้านการผลิตสื่อดิจิทัล

(2) คัดสรรผู้ทรงคุณวุฒิในการเขียนชุดข้อสอบเรื่องความมั่นคงปลอดภัยด้านไซเบอร์ให้กับประชาชนทั่วไป ทั้ง 6 หมวด ดังนี้
- การใช้งานสื่อสังคมออนไลน์ (Social Media) อย่างปลอดภัย
- การใช้และจัดตั้งเครือข่ายไร้สายบ้านให้ปลอดภัย
- ไวรัสและมัลแวร์คอมพิวเตอร์
- การใช้งานโทรศัพท์มือถือให้ปลอดภัยจากภัยคุกคาม
- HTTP (Hypertext Transfer Protocol)
- ผู้ปกครองเพื่อสอนบุตรหลานเกี่ยวกับการใช้อินเทอร์เน็ตอย่างปลอดภัย

(3) พัฒนาสื่อทั้ง 6 หมวด และส่งร่างที่ 1 ต่อคณะกรรมการผู้ทรงคุณวุฒิ

(4) แก้ไขสื่อทั้ง 6 หมวด และส่งร่างที่ 2 ต่อคณะกรรมการผู้ทรงคุณวุฒิ

(5) แก้ไขสื่อทั้ง 6 หมวด และส่งร่างที่ 3 (สุดท้าย) ต่อคณะกรรมการผู้ทรงคุณวุฒิ

(6) เผยแพร่สื่อดิจิทัลผ่านศูนย์การเรียนรู้เสมือน และสังคมออนไลน์

3.2.2 ระบบฝึกอบรมอิเล็คทรอนิกส์

(7) พัฒนาชุดข้อสอบทั้ง 6 หมวด และส่งร่างที่ 1 ต่อคณะกรรมการผู้ทรงคุณวุฒิ

(8) แก้ไขชุดข้อสอบทั้ง 6 หมวด และส่งร่างที่ 2 ต่อคณะกรรมการผู้ทรงคุณวุฒิ

(9) แก้ไขชุดข้อสอบทั้ง 6 หมวด และส่งร่างสุดท้าย ต่อคณะกรรมการผู้ทรงคุณวุฒิ

(10) ตรวจสอบความถูกต้องของภาษา

(11) ประเมินคุณภาพข้อสอบด้วยวิธี Index of Item Objective of Congruence (IOC) และนำไป try out เพื่อหาค่าความเที่ยงและความตรงของข้อสอบ

(12) เปิดให้ใช้งานระบบฝึกอบรมอิเล็คทรอนิกส์ในศูนย์การเรียนรู้เสมือน

3.2.3 การสร้างระบบเกมฝึกอบรมสำหรับเด็กและเยาวชน

(13) พัฒนาเกมทั้ง 5 เกม และส่งร่างที่ 1 ต่อคณะกรรมการผู้ทรงคุณวุฒิ

(14) แก้ไขเกม และส่งร่างที่ 2 ต่อคณะกรรมการผู้ทรงคุณวุฒิ

(15) แก้ไขเกม และส่งร่างสุดท้าย ต่อคณะกรรมการผู้ทรงคุณวุฒิ

(16) ตรวจสอบความถูกต้องของภาษา

(17) ติดตั้งและทดสอบระบบในห้องปฏิบัติการ

(18) เปิดให้ใช้งานระบบเกมฝึกอบรมในศูนย์การเรียนรู้เสมือน

3.2.4 การสร้างระบบสืบค้นข่าวอาชญากรรมทางไซเบอร์

(19) ออกแบบและพัฒนาระบบสืบค้นข่าวอาญชญากรรมทางไซเบอร์

(20) รวบรวมและวิเคราะห์แยกประเภทข่าว

(21) เรียบเรียงเขียนสรุปและป้อนข้อมูลข่าว

(22) ติดตั้งและทดสอบระบบในห้องปฏิบัติการ

(23) เปิดให้ใช้งานระบบสืบค้นข่าวในศูนย์การเรียนรู้เสมือน

3.2.5การออกแบบและพัฒนาเว็บไซต์เพื่อเป็นศูนย์การเรียนรู้เสมือน

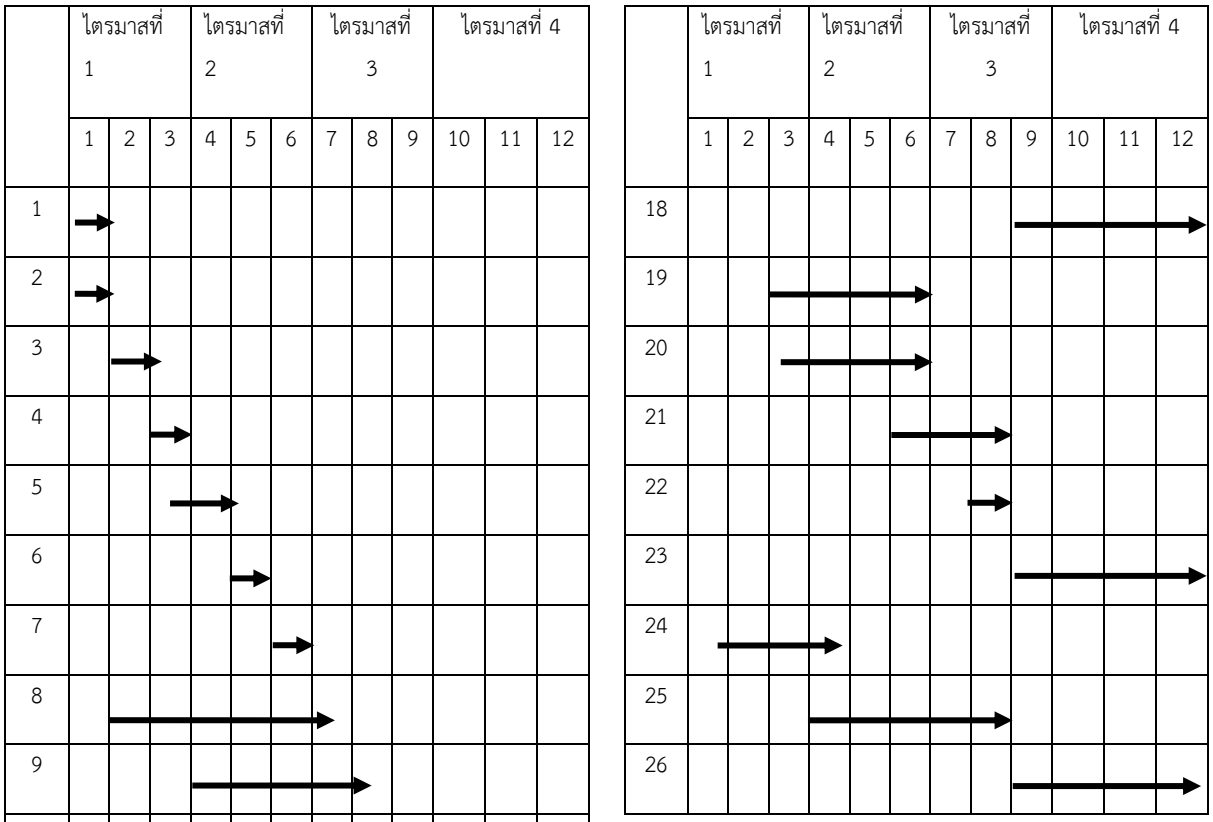
(24) ออกแบบและพัฒนาเว็บไซต์เพื่อเป็นศูนย์การเรียนรู้เสมือน

(25) ออกแบบและพัฒนาแฟนเพจของศูนย์การเรียนรู้เสมือน

3.2.6 เผยแพร่และประชาสัมพันธ์

(26) เผยแพร่และประชาสัมพันธ์กับโรงเรียนมัธยมและมหาวิทยาลัย

ระยะเวลาทำวิจัย 1 ปี (12 เดือน) และแผนดำเนินงานตลอดโครงการมีการปฏิบัติตามขั้นตอนที่ระบุไว้ในรายละเอียดของหัวข้อที่ 14 ดังนี้



3.3 รายงานที่ส่งมอบและแผนการดำเนินงาน

3.3.1 รายงานที่ส่งมอบ

ผลงานที่ส่งมอบภายใต้โครงการการสร้างความตระหนักรู้ให้กับประชาชนเกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์ ตามวัตถุประสงค์ ขอบเขตของงาน และกรอบเวลาที่กำหนด คือ รายงานเบื้องต้น และรายงานประจำงวดอีกจำนวน 4 ฉบับ

1) รายงานเบื้องต้น (ภายใน 30 วัน) ประกอบด้วย รายงานแผนการดำเนินงาน ประกอบด้วย รูปแบบหรือวิธีดำเนินงาน ขั้นตอนและระยะเวลาการดำเนินงาน
2) รายงานความก้าวหน้าฉบับที่ 1 (ภายใน 180 วัน) ประกอบด้วยเนื้อหาของรายงานเบื้องต้น และรายละเอียดผลการศึกษาเพิ่มเติมดังนี้
    - รายงานผลการศึกษา รวบรวมพร้อมจัดทำข้อมูลเนื้อหาในการสร้างความตระหนักรู้
    - สื่อการเรียนรู้ในรูปแบบสื่ออินโฟกราฟฟิค จำนวน ๑๕ คลิป
    - เกมส์ออนไลน์สำหรับฝึกอบรมแก่เด็กและเยาวชน จำนวน ๓ เกมส์
    - ระบบสืบค้นข้อมูลข่าวเกี่ยวกับอาชญากรรมทางไซเบอร์ (เวอร์ชั่นเบต้า)
    - ชุดข้อสอบในการสร้างความตระหนักรู้ และสร้างคอร์สเรียนใน Thaimooc หรือแพลตฟอร์ม e-learning อื่นๆ
3) รายงานความก้าวหน้าฉบับที่ 2 (ภายใน 300 วัน) ประกอบด้วยเนื้อหาของรายงานความก้าวหน้าที่ 1 และรายละเอียดผลการศึกษาเพิ่มเติมดังนี้
    - สื่อการเรียนรู้ในรูปแบบสื่ออินโฟกราฟฟิค จำนวน ๗ คลิป
    - เกมส์ออนไลน์สำหรับฝึกอบรมแก่เด็กและเยาวชน จำนวน ๒ เกมส์
    - สรุปผลการรวบรวมข่าวสารเกี่ยวกับอาชญากรรมทางไซเบอร์สำหรับเป็นฐานข้อมูลระบบสืบค้นข้อมูลข่าวเกี่ยวกับอาชญากรรมทางไซเบอร์
    - ศูนย์การเรียนรู้เสมือนในรูปแบบเว็บไซต์เพื่อการสร้างความตระหนักรู้ให้กับประชาชนเกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์
4) รายงานฉบับสมบูรณ์ (ภายใน 365 วัน) ประกอบด้วยเนื้อหาของร่างรายงานฉบับสมบูรณ์ และรายละเอียดผลการศึกษาเพิ่มเติมดังนี้
    - สรุปผลการทดสอบและประเมินการใช้งานศูนย์การเรียนรู้เสมือนในรูปแบบเว็บไซต์เพื่อการสร้างความตระหนักรู้ให้กับประชาชนเกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์
    - เอกสารรับรองความถูกต้องครบถ้วนของค่าใช้จ่ายทั้งหมดของโครงการโดยผู้สอบบัญชีรับอนุญาต
    - รายงานผลการดำเนินงานฉบับย่อสำหรับลงตีพิมพ์ในวารสารสำนักงาน กสทช.

3.3.2 แผนการดำเนินงาน

สรุปกิจกรรมและงบประมาณในแต่ละงวด

กิจกรรม	น้ำหนักของงาน (%)	ระยะเวลา (Duration)	แผนปฏิบัติการ (Schedule)		แผนงบประมาณ (Budget)				
			เริ่มต้น	สิ้นสุด	งวดที่ 1	งวดที่ 2	งวดที่ 3	งวดที่ 4	รวม
1. จัดทำรายงานแผนการดำเนินงาน (Project Plan)	5	30 วัน			20%				20%
2. ศึกษา รวบรวมพร้อมจัดทำข้อมูลเนื้อหาในการสร้างความตระหนักรู้	10	150 วัน				30%			50%
3. จัดทำสื่อการเรียนรู้ในรูปแบบสื่ออินโฟกราฟฟิค จำนวน 15 คลิป (จากทั้งหมด 22 คลิป)	10								
4. จัดทำเกมส์ออนไลน์สำหรับฝึกอบรมแก่เด็กและเยาวชน จำนวน 3 เกมส์ (จากทั้งหมด 5 เกม)	5								
5. จัดทำระบบสืบค้นข้อมูลข่าวเกี่ยวกับอาชญากรรมทางไซเบอร์ (เวอร์ชั่นเบต้า)	15								
6. จัดทำชุดข้อสอบในการสร้างความตระหนักรู้ และสร้างคอร์สเรียนใน Thaimooc หรือแพลตฟอร์ม e-learning อื่นๆ	15								
7. จัดทำสื่อการเรียนรู้ในรูปแบบสื่ออินโฟกราฟฟิค จำนวน 7 คลิป (จากทั้งหมด 22 คลิป)	5	120 วัน					30%		80%

กิจกรรม	น้ำหนักของงาน (%)	ระยะเวลา (Duration)	แผนปฏิบัติการ (Schedule)		แผนงบประมาณ (Budget)				
			เริ่มต้น	สิ้นสุด	งวดที่ 1	งวดที่ 2	งวดที่ 3	งวดที่ 4	รวม
8. จัดทำเกมส์ออนไลน์สำหรับฝึกอบรมแก่เด็กและเยาวชน จำนวน 2 เกมส์ (จากทั้งหมด 5 เกม)	5								
9. รวบรวมข่าวสารเกี่ยวกับอาชญากรรมทางไซเบอร์สำหรับเป็นฐานข้อมูลระบบสืบค้นข้อมูลข่าวเกี่ยวกับอาชญากรรมทางไซเบอร์	5								
10. จัดทำศูนย์การเรียนรู้เสมือนในรูปแบบเว็บไซต์เพื่อการสร้างความตระหนักรู้ให้กับประชาชนเกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์	15								
11. ทดสอบและประเมินการใช้งานศูนย์การเรียนรู้เสมือน	5	65 วัน						20%	100%
12. จัดทำรายงานฉบับสมบูรณ์	5								
รวมทั้งสิ้น	100	365 วัน			20%	30%	30%	20%	100%