รายงานการศึกษาส่วนบุคคล
(Individual Study)

เรื่อง แนวทางการเพิ่มประสิทธิภาพในการตัดวงจรอาชญากรรมออนไลน์

จัดทำโดย นายสัจจะ โชคบุญส่งสวัสดิ์

รหัส 9844

รายงานนี้เป็นส่วนหนึ่งของการฝึกอบรม

หลักสูตรนักบริหารระดับสูง : ผู้นำที่มีวิสัยทัศน์และคุณธรรม รุ่นที่ 98

วิทยาลัยนักบริหาร สถาบันพัฒนาข้าราชการพลเรือน สำนักงาน ก.พ.

ประจำปี 2566

รายงานการศึกษาส่วนบุคคล

(Individual Study)

เรื่อง แนวทางการเพิ่มประสิทธิภาพในการตัดวงจรอาชญากรรมออนไลน์

จัดทำโดย นายสัจจะ โชคบุญส่งสวัสดิ์

รหัส 9844

หลักสูตรนักบริหารระดับสูง : ผู้นำที่มีวิสัยทัศน์และคุณธรรม รุ่นที่ 98

วิทยาลัยนักบริหาร สถาบันพัฒนาข้าราชการพลเรือน สำนักงาน ก.พ.

ประจำปี 2566

รายงานนี้เป็นความคิดเห็นเฉพาะบุคคลของผู้ศึกษา

สำนักงาน ก.พ.

เอกสารรายงานการศึกษาส่วนบุคคลนี้ อนุมัติให้เป็นส่วนหนึ่งของการฝึกอบรมหลักสูตรนักบริหารระดับสูง : ผู้นำที่มีวิสัยทัศน์และคุณธรรม ของสำนักงาน ก.พ.

ลงชื่อ .....

(นางปัทมา เธียรวิศิษฎ์สกุล)

อาจารย์ที่ปรึกษา

ลงชื่อ.....

(นางระรินทร์ทิพย์ ศิโรรัตน์)

อาจารย์ที่ปรึกษา

ลงชื่อ.....

(นางสาวสุชาดา ไทยบรรเทา)

อาจารย์ที่ปรึกษา

บทสรุปสำหรับผู้บริหาร

รายงานการศึกษาส่วนบุคคล เรื่อง แนวทางการเพิ่มประสิทธิภาพในการตัดวงจรอาชญากรรมออนไลน์ฉบับนี้ การพัฒนาเทคโนโลยีดิจิทัลมีความสำคัญ ทั้งในด้านเศรษฐกิจ และสังคม จากการที่ภาครัฐมีแนวนโยบายส่งเสริมและสนับสนุนการใช้เทคโนโลยีดิจิทัลและอินเทอร์เน็ตในการพัฒนาประเทศในการยกระดับคุณภาพชีวิตของประชาชน และเพิ่มขีดความสามารถในการแข่งขันของประเทศ ในทางกลับกันอาชญากรรมทางออนไลน์ที่เกิดขึ้นเป็นจำนวนมาก เป็นผลจากจำนวนผู้ใช้งานอินเทอร์เน็ตที่เพิ่มมากขึ้นเป็นอย่างมาก เช่นกัน อาชญากรรมทางออนไลน์มีวงจรความสัมฤทธิผลไม่ต่างจากอาชญากรรมอื่น กล่าวคือองค์ประกอบการเกิดอาชญากรรมประกอบด้วย 1. คนร้าย (Offender) 2. โอกาส (Opportunity) (เวลา + สถานที่) และ 3.เหยื่อ (Victim) อาชญากรรมไม่สามารถเกิดขึ้นได้ หากขาดองค์ประกอบใดองค์ประกอบหนึ่งไป จากการศึกษาพบว่า การดำเนินการการระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์หรือการปิดเว็บไซต์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติมเป็นกระบวนการที่กำหนดไว้ตามกฎหมายซึ่งมีระยะเวลาการดำเนินการจนเสร็จสิ้นประมาณ 14 วัน อีกทั้งการดำเนินการยังเป็นในลักษณะเชิงรับ โดยการรับแจ้งเรื่องจากหน่วยงานต่างๆ พนักงานเจ้าหน้าที่ต้องขอความเห็นชอบจากรัฐมนตรีในการยื่นคำร้องต่อศาลในการเว็บกั้นเว็บไซต์ เมื่อพิจารณาจากปริมาณการกระทำความผิดจากอาชญากรรมทางออนไลน์ที่เพิ่มขึ้นอย่างเป็นทวีคูณ จำเป็นต้องพิจารณาปรับปรุงกระบวนการทำงานให้สอดคล้องกับสถานการณ์ ให้เกิดความรวดเร็ว ทันท่วงที เพื่อระงับยับยั้งความเสียหายที่อาจเกิดขึ้นและลดโอกาสการเกิดอาชญากรรมที่ส่งผลกระทบต่อชีวิต และทรัพย์สินของประชาชน

ผู้ศึกษาจึงมีข้อเสนอเชิงนโยบายแนวทางการเพิ่มประสิทธิภาพในการตัดวงจรอาชญากรรมออนไลน์แบ่งเป็น 2 แนวทางคือ 1.แนวทางการจัดทำระบบการเฝ้าระวัง ตรวจสอบ วิเคราะห์ และปิดกั้นเว็บไซต์หลอกลวง (Phishing) และ 2.แนวทางการรณรงค์ สร้างการรับรู้ และแจ้งเตือนภัยออนไลน์ แนวทางทั้งสองนี้เป็นการตัดวงจรการเกิดอาชญากรรมออนไลน์ทั้งในส่วนขององค์ประกอบด้านโอกาสและเหยื่อ ทำให้ขาดความสัมฤทธิผลหรืออาชญากรรมไม่เกิดขึ้น โดยนำเทคโนโลยีปัญญาประดิษฐ์สมัยใหม่ (Artificial Intelligence: AI) เช่น ML (Machine Learning) และ NLP (Natural Language Processing) ในการตรวจจับลักษณะรูปแบบเว็บไซต์หลอกลวงหรือเว็บไซต์ปลอม พร้อมทั้งประสานการปิดกั้นเว็บไซต์ต่อผู้ให้บริการจดชื่อเว็บไซต์ (Domain Name Registrar) โดยอัตโนมัติ สามารถลดระยะเวลาของกระบวนการปิดกั้นเว็บไซต์จากรูปแบบเดิมลงเหลือเพียง 2 วัน รวมถึงการประชาสัมพันธ์สร้างความตระหนักรู้ให้กับประชาชนเกี่ยวกับรูปแบบภัยออนไลน์ต่างๆ การจัดเวทีการแข่งขันของเยาวชน เพื่อกระตุ้นการเรียนรู้และจัดทำคู่มือประชาชนแนวทางการป้องกันและแก้ไขปัญหาที่เกี่ยวกับเว็บไซต์ และสื่อสังคมออนไลน์ (Social Media)

กิตติกรรมประกาศ

รายงานการศึกษาส่วนบุคคล เรื่อง แนวทางการเพิ่มประสิทธิภาพในการตัดวงจรอาชญากรรมออนไลน์ ฉบับนี้ สำเร็จลุล่วงได้ด้วยดี จากความกรุณาเป็นอย่างสูงของท่านอาจารย์ปัทมา เธียรวิศิษฎ์สกุล ซึ่งเป็นท่านอาจารย์ที่ปรึกษาที่ให้การแนะนำ ให้การปรึกษา และชี้แนะแนวทางการจัดทำรายงาน ตลอดจนข้อเสนอแนะการแก้ไข ให้แนวทางเทคนิควิธีการนำเสนอรายงาน ด้วยความเมตตาเอาใจใส่เป็นอย่างยิ่ง ทำให้รายงานฉบับนี้มีความสมบูรณ์ เป็นประโยชน์ต่อการนำไปในการการศึกษาต่อยอดในการทำงานต่อไป และผู้ศึกษาของกราบขอบพระคุณ ท่านอาจารย์ ระรินทิพย์ ศิโรรัตน์ และท่านอาจารย์สุชาดา ไทยบรรเทา ซึ่งกรุณาให้ข้อแนะนำ ข้อเสนอแนะต่างๆ ที่เป็นประโยชน์ ทั้งความรู้ทางวิชาการ ในการวิเคราะห์ทฤษฎี และมุมมองต่างๆ จากประสบการณ์อันมีค่า ในการจัดทำรายงานฉบับนี้

ผู้ศึกษาหวังเป็นอย่างยิ่งว่ารายงานฉบับนี้ จะเป็นประโยชน์ต่อสำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ในการพัฒนาการทำงานให้มีประสิทธิภาพมากยิ่งขึ้น และสามารถนำความรู้และประสบการณ์ที่ได้รับจากการฝึกอบรม นำไปประยุกต์ใช้ในการพัฒนางานในความรับผิดชอบ เพื่อให้เกิดประโยชน์แก่หน่วยงาน และประชาชนผู้เกี่ยวข้องต่อไป

นายสัจจะ โชคบุญส่งสวัสดิ์

29 สิงหาคม 2566

สารบัญ

สารบัญตาราง

สารบัญภาพ

คำอธิบายสัญลักษณ์และคำย่อ

ดศ.	กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
สตช.	สำนักงานตำรวจแห่งชาติ
ธปท.	ธนาคารแห่งประเทศไทย
สำนักงาน กสทช.	สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ
สำนักงาน ปปง.	สำนักงานคณะกรรมการป้องกันและปราบปรามการฟอกเงิน
กลต.	สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
ดีเอสไอ	กรมสอบสวนคดีพิเศษ
สคบ.	สำนักงานคณะกรรมการคุ้มครองผู้บริโภค
ICANN	Internet Corporation for Assigned Names and Numbers
AI	Artificial Intelligence
ML	Machine Learning
NLP	Natural Language Processing
API	Application Programming Interface

1. วิสัยทัศน์ของตำแหน่งเป้าหมาย

(ข้อมูลส่วนบุคคลไม่เผยแพร่)

2. ข้อเสนอเพื่อขับเคลื่อนนโยบายสู่การปฏิบัติ

"แนวทางการเพิ่มประสิทธิภาพในการตัดวงจรอาชญากรรมออนไลน์"

2.1 การกำหนดประเด็นการศึกษา

การดำเนินการทางกฎหมายกับผู้กระทำความผิดหรือการแก้ไขปัญหาการกระทำความผิดของอาชญากรรมทางออนไลน์ ในปัจจุบันผู้บังคับใช้กฎหมายเกี่ยวข้องมีแนวทางการดำเนินงานในลักษณะแบบเชิงรับ คือ ต้องเกิดการกระทำความผิดเกิดขึ้นมาก่อน ประชาชนผู้เสียหายต้องร้องทุกข์กล่าวโทษ เจ้าหน้าที่จึงดำเนินการตามกระบวนการกฎหมาย ในการจัดการแก้ไขปัญหาได้ การดำเนินการตามขั้นตอนของกฎหมายใช้เวลาในการดำเนินการเป็นอย่างมาก ไม่ทันต่อสถานการณ์ที่เปลี่ยนแปลงตามยุคสมัย การศึกษานี้ มีความคิดในการปรับเปลี่ยนแนวทางการดำเนินงานเพื่อให้สามารถป้องกันหรือระงับยับยั้งก่อนเกิดการกระทำความผิด ลดโอกาสในการเกิดความเสียหายที่อาจเกิดขึ้นกับประชาชน มุ่งใช้แนวทางการดำเนินงานแบบเชิงรุกไม่จำเป็นต้องให้เกิดการกระทำความผิด ความเสียหายหรือการแจ้งความ ร้องทุกข์ จากประชาชน โดยเสนอแนวทางการเพิ่มประสิทธิภาพในการตัดวงจรอาชญากรรมออนไลน์ 2 ด้าน คือ 1. แนวทางการจัดทำระบบการเฝ้าระวัง ตรวจสอบ วิเคราะห์ และปิดกั้นเว็บไซต์หลอกลวง (Phishing) และ 2. แนวทางการรณรงค์ สร้างการรับรู้และแจ้งเตือนภัยออนไลน์

2.1.1 สภาพปัญหา ความท้าทาย

จากการขับเคลื่อนนโยบายเศรษฐกิจและสังคมดิจิทัลของรัฐบาลทำให้ประชาชนชาวไทยสามารถเข้าถึงและใช้งานเทคโนโลยีดิจิทัลเพื่อเพิ่มประสิทธิภาพในการทำงานและอำนวยความสะดวกในการใช้ชีวิตประจำวันได้โดยง่าย ปัจจุบันจากจำนวนประชากร 71 ล้านคน คนไทยใช้โทรศัพท์เคลื่อนที่ จำนวน 101.2 ล้านเครื่อง (คิดเป็นร้อยละ 141 ของจำนวนประชากร) เข้าถึงอินเทอร์เน็ต 61.21 ล้านคน (คิดเป็นร้อยละ 85.3 ของจำนวนประชากร) และการใช้งานสื่อสังคมออนไลน์ (Social Media) 52.25 ล้านคน (คิดเป็นร้อยละ 72.8 ของจำนวนประชากร)[1] อย่างไรก็ตาม จากการเข้าถึงและใช้งานเทคโนโลยีดิจิทัลได้อย่างสะดวกรวดเร็วย่อมนำมาซึ่งปัญหาภัยออนไลน์หรืออาชญากรรมในรูปแบบต่าง ๆ ด้วยเช่นกัน โดยเฉพาะปัญหาการฉ้อโกงและหลอกลวงประชาชนผ่านสื่อสังคมออนไลน์ซึ่งทวีความรุนแรงมากขึ้นเป็นอย่างมาก อาทิ การหลอกลวงผ่านแก๊งคอลเซ็นเตอร์ (Call Center) การหลอกลวงลงทุน - ระดมทุนออนไลน์ ประชาชนได้รับความเดือดร้อนจากการสูญเสียทรัพย์สินเป็นจำนวนมาก ส่งผลกระทบต่อเศรษฐกิจ ความเชื่อมั่นและความมั่นคงทางระบบเทคโนโลยีของประเทศ ทั้งนี้ ปัญหาการฉ้อโกงและหลอกลวงออนไลน์ เกิดจากสาเหตุหลายประการ

[1] DIGITAL 2023: THAILAND, https://datareportal.com/reports/digital-2023-thailand

เช่น ประชาชนขาดความตระหนักรู้เกี่ยวกับภัยออนไลน์ทำให้ตกเป็นเหยื่อของมิจฉาชีพ, การรับจ้างเปิดบัญชีธนาคาร และการซื้อ-ขาย บัญชีธนาคาร (บัญชีม้า) เป็นฐานให้มิจฉาชีพใช้ในการกระทำความผิดในอาชญากรรมออนไลน์, การหลอกลวงประชาชนโดยใช้ซิมโทรศัพท์โดยไม่ลงทะเบียนในชื่อของตน, กฎหมายกฎ ระเบียบ ยังไม่ครอบคลุมหรือให้อำนาจในการดำเนินงานของธนาคารในการส่งต่อหรือแลกเปลี่ยนข้อมูลบัญชีต้องสงสัยหรือข้อมูลผู้กระทำความผิดระหว่างธนาคาร ในการระบุหรือยืนยันผู้กระทำความผิด ยับยั้งธุรกรรมทางการเงินของผู้กระทำความผิดให้ทันต่อสถานการณ์ หรือผู้ให้บริการโทรศัพท์เคลื่อนที่สามารถตรวจสอบข้อความ (SMS) หรือการส่งลิงก์และเว็บไซต์หลอกลวงประชาชน และการระงับยับยั้งข้อความที่ต้องสงสัยก่อนเกิดความเสียหาย เป็นต้น

เนื่องจาก ปัญหาการฉ้อโกงและหลอกลวงประชาชนผ่านทางสื่อสังคมออนไลน์เกิดขึ้นอย่างต่อเนื่องและเป็นจำนวนมาก ทำให้ประชาชนได้รับความเดือดร้อนและสูญเสียทรัพย์สินเป็นอย่างมาก คณะรัฐมนตรีจึงมีมติเมื่อวันที่ 18 ตุลาคม 2565 ให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ ธนาคารแห่งประเทศไทยร่วมกับหน่วยงานที่เกี่ยวข้องดำเนินการแก้ไขปัญหาดังกล่าว

จากสถิติการรับแจ้งความทางออนไลน์ของสำนักงานตำรวจแห่งชาติ ตั้งแต่วันที่ 1 มีนาคม 2565 – 30 มิถุนายน 2566 (https://thaipoliceonline.com) มีจำนวนคดีอาชญากรรมออนไลน์กว่า 287,122 คดี คิดเป็นมูลค่าความเสียหายกว่า 39,847 ล้านบาท ซึ่งปัญหาดังกล่าวจำเป็นต้องศึกษาแนวทางทางการเพิ่มประสิทธิภาพในการตัดวงจรอาชญากรรมออนไลน์ เพื่อแก้ไขปัญหาและบรรเทาความเดือดร้อนของประชาชนอย่างเร่งด่วน จากสถิติการแจ้งความออนไลน์ สำนักงานตำรวจแห่งชาติได้รวบรวมประเภทภัยออนไลน์ทั้งหมดจำนวน 22 ประเภท และพบมากที่สุด 5 อันดับแรก (ข้อมูลช่วง 17 มี.ค. – 8 ก.ค. 66) ได้แก่

1. หลอกลวงซื้อขายสินค้าหรือบริการ จำนวน 297 คดี/วัน ความเสียหาย 4.3 ล้านบาท/วัน
2. หลอกให้โอนเงินเพื่อทำงาน จำนวน 78 คดี/วัน ความเสียหาย 9.6 ล้านบาท/วัน
3. หลอกให้กู้เงิน จำนวน 64 คดี/วัน ความเสียหาย 3 ล้านบาท/วัน
4. คดี Call Center จำนวน 37 คดี/วัน ความเสียหาย 8.1 ล้านบาท/วัน
5. หลอกให้ลงทุนผ่านระบบคอมพิวเตอร์ จำนวน 37 คดี/วัน ความเสียหาย 16.4 ล้านบาท/วัน

รูปภาพที่ 2 ประเภทคดีที่เกิดมาก (17 มี.ค. 66 – 8 ก.ค. 66)

ที่มา: สำนักงานตำรวจแห่งชาติ

จากการดำเนินงานที่ผ่านมา การป้องกันและปราบปรามอาชญากรรมทางออนไลน์ในประเทศไทย พบปัญหาการป้องกันและปราบปรามอาชญากรรมทางออนไลน์ ขาดกฎหมายโดยเฉพาะเรื่องเพื่อบังคับใช้ในการป้องกันและปราบปรามอาชญากรรมทางออนไลน์ เนื่องจากรูปแบบพฤติกรรมของอาชญากรรมทางออนไลน์มีหลากหลายประเภท จะใช้กฎหมายแต่ละฉบับมาปรับใช้กับการกระทำความผิดและลงโทษในการกระทำความผิดนั้น เช่น การนำประมวลกฎหมายอาญาว่าด้วยการฉ้อโกงประชาชนหรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ มาปรับใช้ส่งผลทำให้ในการบังคับใช้กฎหมาย อาจจะไม่ตรงต่อรูปแบบของการกระทำความผิดที่มีการพัฒนาหรือเปลี่ยนแปลงรูปแบบของการกระทำความผิดตลอดเวลา ทำให้ปัจจุบันยิ่งเกิดการกระทำความผิดมากยิ่งขึ้น เพราะอาชญากรเห็นถึงช่องว่างทางกฎหมายที่เกิดขึ้นและภาครัฐยังขาดกฎหมายที่มีความทันสมัยหรือครอบคลุม ต่อรูปแบบการกระทำความผิดที่เป็นอาชญากรรมทางออนไลน์ได้อย่างครบถ้วน ประกอบกับแนวทางการแก้ไขปัญหาหรือดำเนินการตามกฎหมายจำเป็นต้องมีการร้องเรียนหรือร้องทุกข์กล่าวโทษในท้องที่เกิดเหตุ ทำให้ประชาชนไม่ได้รับความสะดวกเท่าที่ควร

<u>ปัญหาอื่นๆ ที่เกี่ยวข้อง</u>

จากการดำเนินงานที่ผ่านมาพบปัญหา/อุปสรรค ที่เกิดขึ้นสรุปพอสังเขปได้ดังนี้

- อำนาจหน้าที่ของหน่วยงาน ไม่สอดคล้องกับสถานการณ์ในปัจจุบัน กล่าวคือกฎหมายไม่ได้ให้อำนาจในการดำเนินการ ทำให้เจ้าที่ไม่สามารถดำเนินการต่อผู้กระทำความผิดได้ เช่น การประกาศขายบัญชีธนาคารให้แก่ผู้กระทำความผิดใช้เป็นเครื่องมือในการกระทำความผิด

- ประชาชนขาดแหล่งข้อมูลหรือแหล่งตรวจสอบ ประชาชนไม่ทราบเบอร์ติดต่อสอบถามหรือเว็บไซต์ หรือแอพพลิเคชั่นในการตรวจสอบความถูกต้อง เช่น ผู้ได้รับการอนุญาตให้บริการด้านการลงทุนอย่างถูกกฎหมาย การตรวจสอบข่าวปลอมที่เกี่ยวกับการหลอกลงทุน
- การบังคับใช้กฎหมายหรือการดำเนินคดีของเจ้าหน้าที่ความล่าช้าในการดำเนินงานของหน่วยงานหรือเจ้าหน้าที่ เจ้าหน้าที่มีจำนวนน้อยมากเมื่อเทียบกับปริมาณงานหรือคดีที่เกิดขึ้น ทำให้การปฏิบัติเป็นไปด้วยความล่าช้า
- ช่องทางในการร้องเรียน ช่วยเหลือ หรือแก้ไขหากเกิดเหตุ ประชาชนไม่ทราบขั้นตอนว่าขณะเกิดเหตควรทำอย่างไรบ้าง แจ้งความที่ไหน ระงับการใช้บัญชีอย่างไร ติอต่อประสานงานอย่างไร
- รูปแบบการกระทำความผิดบางรูปแบบไม่เข้าองค์ประกอบของกฎหมาย เนื่องจากมีพฤติกรรมหรือรูปแบบการกระทำความผิดในรูปแบบใหม่ที่ผู้ร้ายใช้ในแผนแผนประทุษกรรม
- การให้ความรู้ ประชาสัมพันธ์แจ้งเตือนประชาชนอย่างทั่วถึง และเท่าทันต่อรูปแบบการโกงหรือหลอกลวงที่เปลี่ยนแปลงไป หมั่นศึกษาหาความรู้ที่ทันสมัยเพื่อเป็นภูมิต้านทานการป้องกันภัยออนไลน์ได้ด้วย

<u>บทบาทหน้าที่ของหน่วยงาน</u>

ปัจจุบันการดำเนินการแก้ไขปัญหาอาชญากรรมทางออนไลน์แต่ละหน่วยงานแก้ไขตามบทบาท หน้าที่อำนาจตามกฎหมายที่กำหนดไว้ตามกฎหมายของแต่ละหน่วยงาน ยังไม่ได้มุ่งสู่การแก้ปัญหาในลักษณะบูรณาการอย่างเต็มที่ ทำให้เมื่อประชาชนเกิดปัญหาขึ้นต้องติดต่อหน่วยงานหลายหน่วยงาน ทำงานหลายครั้งเกิดความไม่สะดวก และใช้เวลาการดำเนินการค่อนข้างมากในการแก้ไขปัญหาที่มีความซับซ้อนเกี่ยวข้องกับหน่วยงานหลายหน่วยงาน บทบาท หน้าที่ หน่วยงานที่เกี่ยวข้องในการป้องกันและปราบปรามปัญหาอาชญากรรมออนไลน์ มีดังนี้

<u>กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ดศ.)</u> มีอำนาจหน้าที่ปิดกั้นเว็บไซต์ และเรียกพยานหลักฐานเกี่ยวกับข้อมูลจราจรทางคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม บูรณาการและขับเคลื่อนการแก้ไขปัญหาการฉ้อโกงออนไลน์ในรูปแบบของคณะกรรมการระดับชาติร่วมกับภาคีหน่วยงานที่เกี่ยวข้อง

<u>สำนักงานตำรวจแห่งชาติ (สตช.)</u> ป้องกันและปราบปรามการกระทำความผิดอาญาตามประมวลกฎหมายวิธีพิจารณาความอาญา และเป็นพนักงานเจ้าหน้าที่ตามกฎหมายอื่นตามที่ได้รับแต่งตั้ง ดำเนินคดีต่อผู้กระทำความผิดตามกระบวนการยุติธรรม

<u>ธนาคารแห่งประเทศไทย (ธปท.)</u> กำกับและตรวจสอบสถาบันการเงินตามพระราชบัญญัติธนาคารแห่งประเทศไทย พ.ศ. 2485 ที่แก้ไขเพิ่มเติม กำหนดมาตรการเกี่ยวข้อง เช่น มาตรการจัดการภัยทุจริตทางการเงิน

เป็นแนวปฏิบัติขั้นต่ำให้สถาบันการเงินทุกแห่งปฏิบัติตามเป็นมาตรฐานเดียวกันในการบริหารจัดการความเสี่ยงจากการทำธุรกรรมทางการเงิน ทั้งการป้องกัน การตรวจจับ และการรับมือ ซึ่งจะช่วยแก้ปัญหาให้ประชาชนได้รวดเร็ว

สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (สำนักงาน กสทช.) กำกับดูแลการประกอบกิจการโทรคมนาคมให้เป็นไปตามหลักเกณฑ์และเงื่อนไขการอนุญาตที่กำหนด กำหนดแนวทางการตรวจสอบ และดำเนินคดีผู้กระทำความผิดเกี่ยวกับการประกอบกิจการโทรคมนาคมตามกฎหมายว่าด้วยวิทยุคมนาคม และกฎหมายว่าด้วยการประกอบกิจการโทรคมนาคม พ.ร.บ. องค์กรจัดสรรคลื่นความถี่และกำกับการประกอบกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์ และกิจการโทรคมนาคม พ.ศ. 2553 และที่แก้ไขเพิ่มเติม ปิดเบอร์โทรศัพท์ที่ผิดกฎหมายที่ไม่สามารถแสดงตัวตนได้

สำนักงานคณะกรรมการป้องกันและปราบปรามการฟอกเงิน (สำนักงาน ปปง.) ตรวจสอบวิเคราะห์ข้อมูลทางการเงินที่เกี่ยวข้องกับการฟอกเงิน พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2552 พิจารณากำหนดหรือทบทวนรายชื่อบุคคลที่มีความเสี่ยงสูงซึ่งควรได้รับการเฝ้าระวังอย่างใกล้ชิดตามกฎกระทรวงการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้าบัญชีธนาคารที่มีความเสี่ยง

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (กลต.) กำกับดูแลตลาดทุน พระราชบัญญัติหลักทรัพย์และตลาดหลักทรัพย์ พ.ศ. 2535 และที่แก้ไขเพิ่มเติม ออกใบอนุญาต/จดทะเบียน/ให้ความเห็นชอบผู้ให้บริการในตลาดทุนที่อยู่ภายใต้การกำกับดูแลของ ก.ล.ต.

กรมสอบสวนคดีพิเศษ (ดีเอสไอ) ป้องกัน ปราบปราม และควบคุมอาชญากรรมที่มีผลกระทบอย่างร้ายแรงต่อเศรษฐกิจ สังคม ความมั่นคงและความสัมพันธ์ระหว่างประเทศ พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 ดำเนินคดี สืบสวน สอบสวน คดีพิเศษ

สำนักงานคณะกรรมการคุ้มครองผู้บริโภค (สคบ.) กำกับดูแลการซื้อสินค้าออนไลน์ตามพระราชบัญญัติขายตรงและตลาดแบบตรง พ.ศ. 2545 ผู้บริโภคมีสิทธิเลิกสัญญาหรือขอคืนสินค้าได้ภายใน 7 วัน หลังจากการรับสินค้า โดยผู้บริโภคต้องทำหนังสือแจ้งและส่งทางไปรษณีย์ลงทะเบียนตอบรับไปยังผู้ประกอบธุรกิจ พร้อมเก็บเอกสารการซื้อ-ขาย และสินค้าไว้ก่อน (ภายใน 21 วัน) นับแต่วันที่ใช้สิทธิขอคืนสินค้า

ตารางที่ 1 ผลการดำเนินงานที่เกี่ยวข้องกับการป้องกันและปราบปรามอาชญากรรมทางออนไลน์[2]

ผลการดำเนินงานที่ผ่านมา
1. ปิดกั้น SMS / เบอร์โทร หลอกลวง
- ปิดกั้น 71,243 SMS / 144,144 เบอร์โทร รวม 215,387 รายการ (ก.ย. 64 – มิ.ย. 66) (สำนักงาน กสทช.)
2. ปิดกั้นสื่อออนไลน์ที่หลอกลวงประชาชน
- ปิดกลุ่ม Facebook ซื้อขายบัญชีม้า 19 กลุ่ม (ต.ค. 65 - มี.ค. 66) (ดศ.)
- ปิดกั้นโฆษณา Facebook 2,526 รายการ (พ.ค. – มิ.ย. 66) (ดศ.)
- ปิดกั้นเว็บไซต์พนันออนไลน์ 1,894 รายการ (ก.ค. 65 – มิ.ย. 66) (ดศ.)
3. จับกุมซื้อขายบัญชีม้า / ซิมม้า
- ดำเนินคดี บัญชีม้า ซิมม้า 219 คดี ผู้ต้องหา 216 คน (15 - 31 พ.ค. 66) (สตช.)
4. แจ้งรายชื่อผู้มีความเสี่ยงสูงทางการเงิน
- แจ้งรายชื่อบุคคล /เจ้าของบัญชีธนาคาร ที่ใช้กระทำความผิด 2,394 รายชื่อ (มิ.ย. 66) (สำนักงาน ปปง.)
5. จับกุมดำเนินคดี เรื่องหลอกลวงทางการเงิน
- ดำเนินคดี 740 คดี / ผู้ต้องหา 762 ราย (ม.ค. 65 – พ.ค. 66) (สตช.)
- ดำเนินคดีแก๊ง Call Center ในต่างประเทศ (กัมพูชา) 8 ครั้ง จับกุม 166 ราย (ธ.ค. 64–ต.ค. 65) (สตช.)

2.2 การกำหนดข้อเสนอเชิงนโยบาย

อาชญากรรมทางออนไลน์มีวงจรความสัมฤทธิผลไม่ต่างจากอาชญากรรมอื่นกล่าวคือ องค์ประกอบการเกิดอาชญากรรมประกอบด้วย 1. คนร้าย (Offender) 2. โอกาส (Opportunity) (เวลา + สถานที่) และ 3.เหยื่อ (Victim) อาชญากรรมไม่สามารถเกิดขึ้นได้ หากขาดองค์ประกอบใดองค์ประกอบหนึ่งไป

[2] รายงานการประชุมคณะกรรมการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ครั้งที่ 1/2566, กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

รูปภาพที่ 3 สามเหลี่ยมสัมฤทธิผลของอาชญากรรม[3]

2.2.1 การวิเคราะห์ข้อมูลที่เกี่ยวข้องเพื่อประกอบการจัดทำข้อเสนอ

การวิเคราะห์สภาวะแวดล้อม (SWOT Analysis) การจัดทำระบบการเฝ้าระวัง ตรวจสอบ วิเคราะห์ และปิดกั้นเว็บไซต์หลอกลวง (Phishing) โดยหาจุดแข็ง และจุดอ่อน หรือสิ่งที่อาจเป็นประเด็นปัญหาสำคัญที่สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมพบในกระบวนงานที่เกี่ยวกับการปิดกั้นเว็บไซต์ และการวิเคราะห์ปัจจัยภายนอก เพื่อประเมินโอกาส และอุปสรรค วิเคราะห์ได้ ดังนี้

ตารางที่ 2 การวิเคราะห์ GAP Analysis ด้วยเครื่องมือ SWOT Analysis ในการหาจุดแข็งจุดอ่อนต่อประเด็นศึกษา

จุดแข็ง (Strengths)	จุดอ่อน (Weaknesses)
1. สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นหน่วยงานหลักที่รับผิดชอบในการปิดกั้นเว็บไซต์ผิดกฎหมาย 2. สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมมีฐานข้อมูลเกี่ยวกับชื่อเว็บไซต์ที่เว็บไซต์ผิดกฎหมาย 3. พนักงานเจ้าหน้าที่มีความรู้ ประสบการณ์เกี่ยวกับเว็บไซต์ผิดกฎหมาย	1. สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมมีบุคคลากรที่ปฏิบัติหน้าที่ในการปิดกั้นไซต์ผิดกฎหมายเป็นจำนวนน้อยเมื่อเทียบกับปริมาณงานที่เกิดขึ้น 2. สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมดำเนินงานเชิงรับตามกรอบกระบวนการที่ระบุไว้ในกฎหมายในลักษณะรับเรื่องจากผู้ร้องเรียนหรือหน่วยงานประสานส่งเรื่องมา

[3] สามเหลี่ยมสัมฤทธิผลของอาชญากรรม พันตำรวจตรี ชวลิต น้ำใจสัตย์, 2562

โอกาส (Opportunities)	อุปสรรค (Threats)
1. Internet Corporation for Assigned Names and Numbers หรือ ICANN เป็นองค์กรสากลที่ทำหน้าที่ในการบริหารงานและพัฒนาระบบชื่อโดเมนโลกได้กำหนดให้ผู้ใช้งานสามารถรายงานเว็บไซต์ที่มีการละเมิด (abuse)[4] นำไปใช้งานในทางที่ผิด เช่น เว็บไซต์หลอกลวง (Phishing) สามารถปิดกั้นได้หากมีการละเมิดเกิดขึ้น 2. สื่อสังคมออนไลน์ (social media) ในแต่ละแพลตฟอร์มมีช่องทางรายงานเพจหรือบัญชีปลอม[5] 3. เทคโนโลยีสมัยใหม่ เช่น Artificial Intelligence (AI), Machine Learning (ML) และ Natural Language Processing (NLP) สามารถจดจำ เรียนรู้ และทำงานในการตัดสินใจแทนมนุษย์ได้	1. การปิดกั้นเป็นการดำเนินการโดยการรายงาน (Report) ต่อผู้ให้บริการจดทะเบียนชื่อเว็บไซต์หรือผู้ให้บริการสื่อสังคมออนไลน์ ซึ่งเป็นผู้ให้บริการอยู่ต่างประเทศ และเป็นการปฏิบัติตามกฎของผู้กำกับดูแลในต่างประเทศอาจมีการปฏิเสธหรือไม่ดำเนินการหากมีความเห็นไม่ตรงกัน หรือข้อมูลสนับสนุนการตัดสินใจไม่เพียงพอ 2. รูปแบบที่ต้องการให้ระบบเรียนรู้เพื่อเลือกเว็บไซต์ที่เข้าข่ายเกณฑ์หลอกลวงผู้ร้ายมีการเปลี่ยนรูปแบบตลอดเวลา

แนวทางการเพิ่มประสิทธิภาพในการตัดวงจรอาชญากรรมออนไลน์ เป็นแนวทางที่แปลงจากแผนนโยบายสู่การปฏิบัติ เน้นการดำเนินการตามกลยุทธ์ด้านการป้องกัน (Prevention) และกลยุทธ์ด้านการยับยั้ง (Interception) ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยมีแนวทางการดำเนินงานดังนี้

(1) ระบบการเฝ้าระวัง ตรวจสอบ วิเคราะห์ และปิดกั้นเว็บไซต์หลอกลวง (Phishing)

การปิดกั้นเว็บไซต์หรือข้อมูลคอมพิวเตอร์ที่ผิดกฎหมายจากแนวทางเดิม ดศ. ดำเนินการในลักษณะตามกระบวนการของกฎหมาย (ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง ขั้นตอนการแจ้งเตือน) กล่าวคือ รับข้อมูลจากหน่วยงานที่เกี่ยวข้องจัดเตรียมเรื่องเสนอให้รัฐมนตรีเห็นชอบให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลใน

[4] Registrar Abuse Reports, https://www.icann.org/resources/pages/abuse-2014-01-29-en

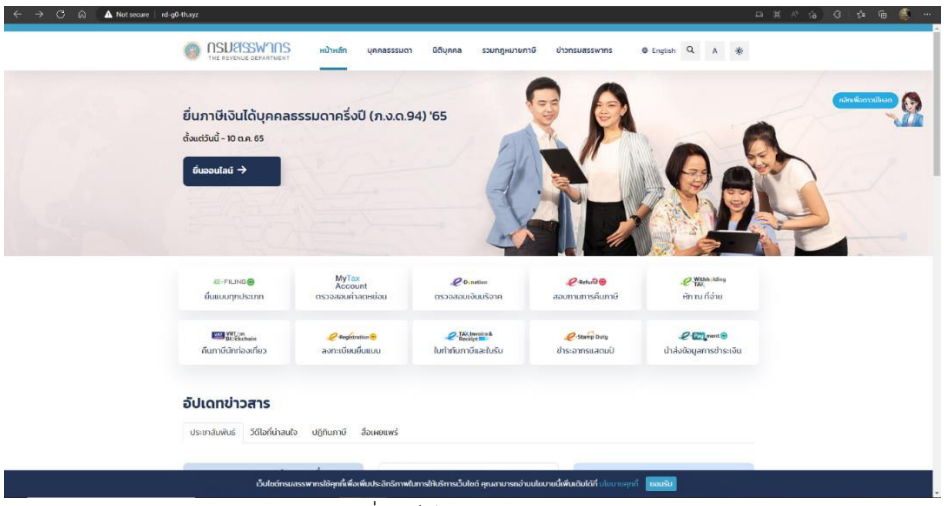
[5] Introduction to the Advertising Standards, https://transparency.fb.com/policies/ad-standards/

การปิดกั้นข้อมูลที่ผิดกฎหมายจนศาลมีคำสั่ง จากนั้นพนักงานเจ้าหน้าที่แจ้งคำสั่งศาลไปยังผู้ให้บริการอินเทอร์เน็ต เพื่อดำเนินการปิดกั้นหรือลบข้อมูลที่ผิดกฎหมายออก ซึ่งกระบวนการนี้ใช้ระยะเวลาประมาณ 14 วัน[6]

รูปภาพที่ 4 ขั้นตอนการปิดเว็บไซต์ที่ผิดกฎหมาย

และจากการวิเคราะห์ข้อมูลของ สตช. พบว่าภัยทางออนไลน์ที่พบมากสูงสุด 5 อันดับแรกที่ได้กล่าวไว้แล้วข้างต้นนั้น มักมีสาเหตุจากการที่มิจฉาชีพใช้เว็บไซต์ (Website) เครือข่ายสังคมออนไลน์ (Social Network) ตลอดจนระบบข้อความโต้ตอบ (Instant Messaging) เป็นเครื่องมือในการหลอกลวงประชาชน และรูปแบบการหลอกลวงที่พบบ่อยๆ ก็คือเว็บไซต์หลอกลวง (Phishing Website) หรือการปลอมแปลงเป็นบุคคลหรือหน่วยงานต่างๆ (impersonation) ซึ่งเว็บไซต์เหล่านี้ถูกสร้างขึ้นโดยมีเจตนาอันไม่สุจริต เป็นเครื่องมือที่ช่วยให้มิจฉาชีพสามารถเข้าถึงข้อมูลส่วนบุคคลต่างๆ และนำข้อมูลนั้นไปแอบอ้างทำธุรกรรมต่างๆ รวมไปถึงก่ออาชญากรรมทางออนไลน์หรืออินเทอร์เน็ตจากประชาชนได้โดยง่าย โดยเฉพาะประเทศไทยที่มีคดีออนไลน์ด้านการฉ้อโกงออนไลน์ซึ่งทวีความรุนแรงมากขึ้นอย่างต่อเนื่อง ประชาชนถูกมิจฉาชีพหลอกลวงโดยการส่งข้อความหลอกลวงต่างๆ ผ่านทาง SMS หรือเครือข่ายสังคมออนไลน์ และใช้เว็บไซต์ปลอมของหน่วยงานภาครัฐและบริษัทเอกชนที่มีชื่อเสียง หลอกลวงในลักษณะ Hybrid Scam เพื่อให้ผู้เสียหายกรอกข้อมูลส่วนบุคคลและนำไปใช้ในทางมิชอบ เช่น หลอกให้กลัวโดยแอบอ้างเป็นเจ้าหน้าที่ภาครัฐ หลอกให้ทำงานออนไลน์ หลอกให้กู้เงินแต่ไม่ได้เงิน และหลอกให้ลงทุนในรูปแบบต่างๆ เป็นต้น จากรูปภาพที่ 5 แสดงตัวอย่างเว็บไซต์ปลอม (Phishing) ที่ใช้หลอกประชาชนโดยปลอมจากเว็บไซต์ของกรมสรรพากร https://www.rd.go.th ชื่อของเว็บปลอม คือ http://rd-g0-th.xyz และรูปภาพที่ 6 แสดงเพจหรือบัญชีเฟซบุ๊กปลอมที่แอบอ้างหน่วยงานภาครัฐ เอกชน และบุคคลที่มีชื่อเสียง

[6] กองป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

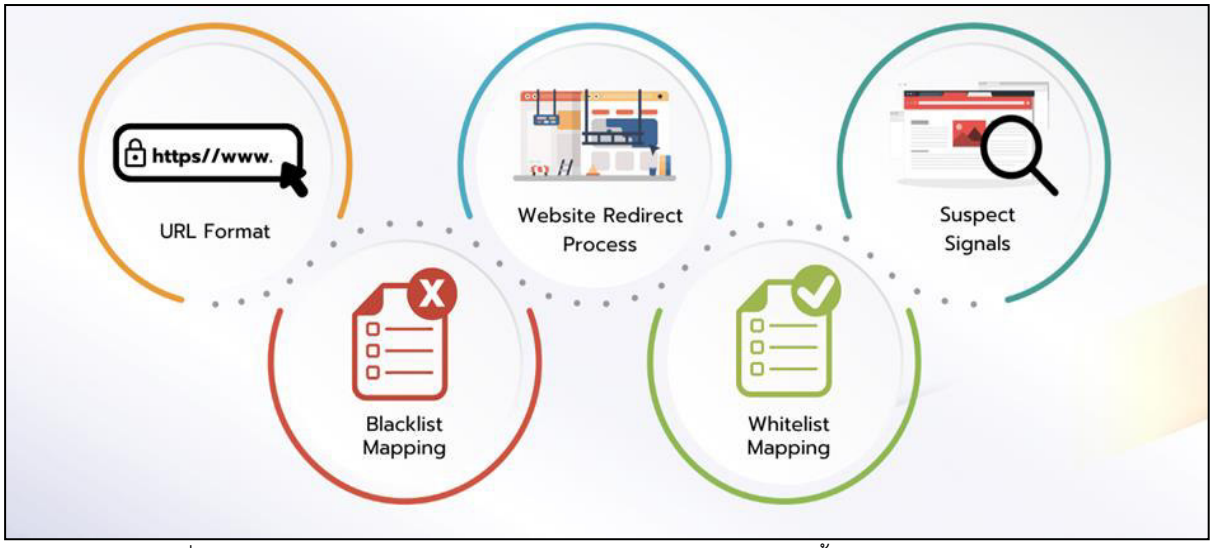


รูปภาพที่ 5 เว็บไซต์กรมสรรพากรปลอม

รูปภาพที่ 6 แสดงเพจหรือเฟซบุ๊กปลอมที่แอบอ้างหน่วยงานภาครัฐ เอกชน และบุคคลที่มีชื่อเสียง

การตัดวงจรอาชญากรรมออนไลน์โดยใช้เทคโนโลยี Social Listening, Natural Language Processing (NLP), Machine Learning (ML) เข้าช่วยในการตรวจสอบเว็บไซต์ปลอม หรือ ข้อความในเครือข่ายสังคมออนไลน์ที่เข้าข่ายหลอกลวงและอาจทำให้เกิดความเสียหายแก่ประชาชน และให้เจ้าหน้าที่ใช้ประกอบการพิจารณาในการแจ้งให้เครือข่ายสื่อสังคมออนไลน์ (Social Media) หรือผู้ให้บริการจดทะเบียนโดเมนเนม (Domain Name Registrar) ดำเนินการปิดกั้นการเข้าถึงเว็บไซต์หรือข้อความในเครือข่ายสังคมออนไลน์ดังกล่าว ก่อนจะทำให้เกิดความเสียหายในวงกว้างต่อไป การดำเนินการในแนวทางนี้ไม่จำเป็นต้องมีคำสั่งศาลแต่อย่างใด เนื่องจากการหลอกลวงในลักษณะ (Phishing) เป็นข้อตกลงเกี่ยวกับการใช้งาน (Terms of Use) ที่ผู้ใช้งานต้องปฏิบัติตาม

การตรวจสอบ ค้นหา และจัดการกับเว็บไซต์หลอกลวงในแบบเชิงรุก (Pro Active) มีหลักคิดในการทำงานในการสืบค้นหาต้นเว็บไซต์หลอกลวงในลักษณะ (Phishing Website) โดยใช้เทคโนโลยีตรวจสอบรูปแบบของ Uniform Resource Locator (URL) ปลอม จัดเก็บในฐานข้อมูลเว็บไซต์หลอกลวง การตรวจสอบเปรียบเทียบกับฐานข้อมูลของเว็บไซต์จริง รวมถึงการใช้เทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) เช่น ML (Machine Learning) และ NLP (Natural Language Processing) ในการเรียนรู้ วิเคราะห์ เปรียบเทียบรูปแบบการหลอกลวง และนำส่งข้อมูลแจ้งเจ้าหน้าที่หรือประสานงานผ่านระบบ API (Application Programming Interface) ได้อย่างอัตโนมัติ โดยระบบดังกล่าวจะช่วยลดกำลังคนของผู้ปฏิบัติงาน และระยะเวลาในการจัดการปิดกั้นเว็บไซต์หลอกลวง (Phishing Website) ได้อย่างมีประสิทธิภาพ ลดความเสียหายก่อนที่ประชาชนหลงเข้าไปดำเนินการธุรกรรมต่างๆ จากเว็บไซต์ปลอมเหล่านั้นได้ ลดโอกาสการเกิดอาชญากรรมเนื่องจากถูกยับยั้งก่อนเกิดเหตุ ซึ่งการดำเนินงานโดยวิธีดังกล่าวนี้สามารถลดระยะเวลาการปิดกั้นเว็บไซต์ลงได้เหลือระยะเวลาไม่เกิน 2 วัน



รูปภาพที่ 7 แสดงแนวความคิดระบบการเฝ้าระวัง ตรวจสอบ วิเคราะห์ และปิดกั้นเว็บไซต์หลอกลวง (Phishing)

การทำงานในส่วนของระบบเฝ้าระวังตรวจสอบเว็บไซต์หลอกลวง มีดังนี้

1) จัดเตรียมทีมงานในการจัดทำฐานข้อมูลเว็บไซต์หรือบัญชีสื่อสังคมออนไลน์ที่ต้องการเฝ้าระวัง ได้แก่ เว็บไซต์และบัญชีสื่อหน่วยงานราชการทั้งหมด 270 กรม 20 กระทรวง และหน่วยงานหรือบุคคลที่มักจะเป็นเป้าหมายในการหลอกลวง เช่น บริษัทหรือบุคคลที่มีชื่อเสียงและมีความน่าเชื่อถือ (Whitelist) และฐานข้อมูลของเว็บไซต์และบัญชีสื่อสังคมออนไลน์ปลอมต่างๆ (Blacklist)

2) ดำเนินการสร้างการเรียนรู้ (Training) ให้แก่ระบบ AI โดยใช้เทคนิค Machine Learning เพื่อให้ระบบสามารถจดจำพฤติกรรมการปลอมแปลงไม่ว่าจะเป็นภาพที่ถูกดัดแปลงหรือโลโก้หน่วยงานต่างๆ ที่ถูกผู้ร้ายนำไปใช้

อีกส่วนหนึ่งระบบสามารถเข้าใจภาษาไทยได้โดยใช้เทคนิค Natural Language Processing มีฐานข้อมูลที่รู้จักภาษาไทยทำให้ระบบสามารถสืบค้นเว็บไซต์ที่เข้าข่ายการปลอมแปลงตามกฎเกณฑ์ (criteria) ที่เรากำหนดไว้

3) เมื่อระบบทำการสืบค้นหรือกวาดต้อนข้อมูล (Scan) และทำการประมวลผลคัดเลือกแสดงผลการแยกแยะเว็บไซต์ที่เข้าข่ายการหลอกลวง (Phishing Website) ระบบจะทำการแยกออกมาแสดงผลและจัดเก็บข้อมูล หากข้อมูลดังกล่าวเข้าเกณฑ์ตามที่กำหนดไว้เกินร้อยละ 90 ขึ้นไป ระบบจะทำการส่งข้อมูลโดยอัตโนมัติไปสู่ผู้ให้บริการจดทะเบียนโดเมนเนม (Domain Name Registrar) ดำเนินการปิดกั้นเว็บไซต์ดังกล่าวต่อไป หากข้อมูลที่ได้มาเข้าเกณฑ์ที่ตั้งไว้น้อยกว่าร้อยละ 90 ระบบจะส่งข้อมูลให้เจ้าหน้าที่ตัดสินใจว่าจะดำเนินการประสานให้ผู้ให้บริการจดทะเบียนฯ ดำเนินการปิดกั้นต่อไป

4) เมื่อระบบมีการเรียนรู้และปิดกั้นซ้ำๆ ตามทั้งสองหลักเกณฑ์ที่กล่าวไว้ข้างต้นแล้ว ระบบจะจดจำและมีการเรียนรู้มากยิ่งขึ้น มีความแม่นยำมากยิ่งขึ้น นำไปสู่การปิดกั้นแบบอัตโนมัติได้ในอนาคตต่อไป เมื่อสามารถปิดกั้นได้แบบอัตโนมัติแล้ว การปิดกั้นเว็บไซต์ที่เข้าข่ายการหลอกลวง (Phishing Website) จะลดลงอย่างมีนัยยะสำคัญ มีความรวดเร็วทันต่อสถานการณ์ ประชาชนมีความปลอดภัยและเชื่อมั่นในการใช้งานเว็บไซต์ในการทำธุรกรรมต่างๆ ได้อย่างมั่นใจ

(2) การรณรงค์ สร้างการรับรู้ และการแจ้งเตือนภัยออนไลน์แก่ประชาชน

นอกจากจัดทำระบบเพื่อการแก้ไขปัญหาการหลอกลวงผ่านช่องทางเว็บไซต์ (Phishing Website) หรือสื่อสังคมออนไลน์ในลักษณะปลอมเป็นบุคคลอื่น (impersonation) แล้ว การป้องกั้นที่ดีที่สุดคือการส่งเสริมให้ประชาชนสามารถใช้เทคโนโลยีเป็น อย่างรู้เท่าทัน (digital literacy) โดยเฉพาะในกลุ่มเสี่ยงที่อาจถูกคุกคามหรือถูกหลอกลวงทางออนไลน์ได้ง่าย เช่น เยาวชนหรือกลุ่มผู้สูงอายุ เนื่องจากยังขาดประสบการณ์และมักเปิดรับสื่อสารสนเทศที่เสี่ยงต่อการถูกหลอก การใช้งานอินเทอร์เน็ต การทำธุรกรรมทางการเงินผ่านทางออนไลน์มากขึ้นตามยุคสมัย แต่หากผู้ใช้งานขาดความตระหนักรู้ถึงภัยออนไลน์ที่ใกล้ตัว รวมไปถึงการแชร์หรือแบ่งปันข้อมูลข่าวสารที่ไม่ถูกต้อง ปลอม หลอกลวง หรือบิดเบือน (Fake news) ย่อมก่อให้เกิดความเสียหายต่อชีวิตหรือทรัพย์สินของประชาชนได้ การรณรงค์ สร้างการรับรู้ และแจ้งเตือนภัยออนไลน์แก่ประชาชนจึงเป็นสิ่งที่สำคัญที่จะช่วยป้องกันไม่ให้ถูกหลอก ไม่ตกเป็นเหยื่อ หรือรับทราบแนวทางการแก้ไข แนวทางการป้องกัน หากพบปัญหาเพื่อที่ประชาชนช่วยเหลือตัวเองได้อย่างทันท่วงที สามารถป้องกันหรือลดการเกิดอาชญากรรมออนไลน์ได้

แนวทางการสร้างการรับรู้อย่างเป็นระบบผ่านช่องทางการสื่อสารทั้งเว็บไซต์ สื่อสังคมออนไลน์ และการรณรงค์ สร้างการรับรู้ โดยการจัดกิจกรรม จัดเวทีการประกวดสื่อสร้างสรรค์ เพื่อกระตุ้นในการสร้างการรับรู้แก่เยาวชน และจัดทำคู่มือประชาชนเพื่อเป็นแนวทางในการรับทราบรูปแบบการกระทำความผิด และแนวทางการป้องกันและการแก้ไขที่สามารถดำเนินได้ด้วยตนเอง เพื่อเป็นความรู้พื้นฐานในการป้องกันตัวในการใช้ชีวิตเนื่องจากสื่อออนไลน์ต่างๆ หรือการทำธุรกรรมในชีวิตประจำวันใช้เครื่องมือดิจิทัลกันอย่างมาก

การทำงานในส่วนของการรณรงค์ สร้างการรับรู้ และการแจ้งเตือนภัยออนไลน์แก่ประชาชน มีดังนี้

(1) ศึกษาลักษณะการให้บริการและจำนวนผู้ใช้บริการเว็บไซต์/โซเชียลเน็ตเวิร์กต่าง ๆ รวบรวมและวิเคราะห์ข้อมูลรูปแบบการกระทำความผิด แนวทางป้องกันและแก้ไขปัญหาที่เกี่ยวกับเว็บไซต์/โซเชียลมีเดียต่างๆ

(2) จัดทำคู่มือแนวทางการป้องกัน/แก้ไขปัญหาที่เกี่ยวกับเว็บไซต์/โซเชียลมีเดีย (Social Media) ต่างๆ ซึ่งมีเนื้อหาในการไขปัญหาสื่อโซเชียลมีเดียหลักที่กำลังเป็นที่นิยมของประชาชน เช่น Facebook Line Instagram Twitter และรูปแบบการกระทำความผิดต่างๆ ที่ประชาชนสามารถป้องกันและแก้ไขได้ด้วยตนเอง เช่น การป้องกันการถูกฉ้อโกงจากการซื้อขายสินค้า การถูกเข้าถึงบัญชีโดยมิชอบ (Hacked) ปลอมแปลงแอบอ้างตัวบุคคลหรือองค์กร การถูกข่มขู่/กลั่นแกล้ง/ส่งภาพลามกอนาจาร เป็นต้น เนื้อจะเกี่ยวข้องกับวิธีการกู้คืนบัญชี การดาวน์โหลดข้อมูลบัญชี การแจ้งรายงานบัญชีปลอมหรือแอบอ้าง การแจ้งรายงานเนื้อหาที่ทำให้เกิดความเสียหาย การรักษาความปลอดภัยของบัญชี และช่องทางการติดต่อประสานงานกับผู้ให้บริการโซเชียลมีเดีย เป็นต้น

(3) จากคู่มือประชาชนที่ดำเนินการแล้ว นำไปสู่การประชาสัมพันธ์ในรูปแบบต่างๆ นอกจากตัวคู่มือแล้ว จัดทำสื่อต่าง ๆ ในรูปแบบ Infographic หรือวีดีโอสั้น ให้เข้าใจง่ายเพื่อกระตุ้นการตระหนักรู้แก่ประชาชน จัดกิจกรรมเพื่อกระตุ้นการเรียนรู้ เช่น การจัดการแข่งขันในการตอบคำถามหรือชิงรางวัลเกี่ยวกับการป้องกันภัยทางอาชญากรรมทางออนไลน์ จัดอบรมสัมมนากับหน่วยงานผู้เกี่ยวข้องหรืออาสาสมัครต่างๆ เพื่อเป็นผู้ถ่ายทอดความรู้ให้แก่ประชาชนต่อไปให้มากที่สุดเพื่อ ที่ประชาชนมีความรู้พื้นฐานในการป้องกันตนเองจากภัยทางออนไลน์ ลดโอกาสการตกเป็นเหยื่อและลดจำนวนคดีที่อาจเกิดขึ้นได้

(4) ติดตามประเมินผล เพื่อปรับปรุงข้อมูลให้มีความทันสมัยต่อสถานกาณ์ที่เกิดขึ้นในปัจจุบัน ประเมินผลช่องทางการสื่อสารประชาสัมพันธ์ว่ามีประสิทธิภาพหรือไม่ การรับรู้ของประชาชนเป็นอย่างไร เพื่อนำผลลัพธ์มาปรับปรุงช่องทางหรือรูปแบบในการประชาสัมพันธ์ต่อไป

แนวทางในการบริหารจัดการภายใต้ข้อเสนอแนะทั้ง 2 ด้าน

จากข้อเสนอเชิงนโยบาย “แนวทางการเพิ่มประสิทธิภาพในการตัดวงจรอาชญากรรมออนไลน์” ผู้ศึกษาขอเสนอแนวทางการบริหารจัดการในระดับปฏิบัติการ ดังนี้

1) แต่งตั้งคณะทำงานในการจัดระบบเฝ้าระวังตรวจสอบเว็บไซต์หลอกลวงและการรณรงค์ สร้างการรับรู้และการแจ้งเตือนภัยออนไลน์แก่ประชาชน โดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นฝ่ายเลขานุการ โดยมีองค์ประกอบ คือ ปลัดกระทรวงหรือรองปลัดกระทรวงที่ได้รับมอบหมายเป็นประธานคณะทำงาน คณะทำงานโดยตำแหน่ง มาจากหน่วยงานที่เกี่ยวข้อง คือ ผู้แทนสำนักงานตำรวจแห่งชาติ ผู้แทนธนาคารแห่งประเทศไทย

ผู้แทนสำนักงาน กสทช. ผู้แทนสำนักงาน ปปง. ผู้แทนสำนักงาน กลต. ผู้แทนกรมสอบสวนคดีพิเศษ ผู้แทนสำนักงานคณะกรรมการคุ้มครองผู้บริโภค

2) คณะทำงานฯ มีหน้าที่และอำนาจ คือ กำหนดรูปแบบเว็บไซต์ปลอมที่ถูกแอบอ้างและหลอกหลวงประชาชน และวางแผนแนวทางการประชาสัมพันธ์ในการสร้างการรับรู้ในด้านภัยออนไลน์ให้แก่ประชาชนร่วมกัน โดยแต่ละหน่วยมีการตั้งผู้ประสานงานประสานโดยเมื่อพบภัยออนไลน์ในรูปแบบที่ส่งผลกระทบต่อประชาชน หรือต้องการสื่อสารให้เป็นไปในแนวเดียวกันเพื่อให้การประชาสัมพันธ์มีพลังสามารถสื่อสารไปสู่ประชาชนได้อย่างมีประสิทธิภาพ

3) คณะทำงานฯ มีการหารือทบทวนถึงการทำงานเป็นระยะๆ เพื่อตรวจสอบประสิทธิภาพในการปิดกั้นของทั้งระบบและผลลัพธ์ของการประชาสัมพันธ์ไม่ว่ารูปแบบการหลอกลวงที่เปลี่ยนแปลงจำเป็นต้องกำหนดหรือป้อนข้อมูลให้กับระบบเฝ้าระวังให้เกิดการเรียนรู้รูปแบบการหลอกลวงใหม่ที่เกิดขึ้น และคณะทำงานฯ สามารถนำรูปแบบที่เกิดขึ้นใหม่นำไปประชาสัมพันธ์สร้างการรับรู้ให้แก่ประชาชนเพื่อไม่ให้ตกเป็นเหยื่อต่อไป

ปัจจัยที่มีผลกระทบต่อความสำเร็จและแนวทางบริหารจัดการ

1) บุคลากรจำนวนบุคลากรของสำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมที่มีทักษะในการวิเคราะห์ แยกแยะเว็บไซต์หลอกลวง และสามารถประสานงานกับผู้ให้บริการ จดทะเบียนโดเมนเนม (Domain Name Registrar) หรือผู้ให้บริการสื่อสังคมออนไลน์ มีจำนวนไม่มากพอในการรองรับภารกิจที่จะเพิ่มขึ้น อย่างไรก็ตาม ระบบการเฝ้าระวัง ตรวจสอบ วิเคราะห์ และปิดกั้นเว็บไซต์หลอกลวง (Phishing) ที่พัฒนาขึ้นมีความแม่นยำสามารถทำงานแทนเจ้าหน้าที่และสามารถประสานงานผ่านระบบในรูปแบบอัตโนมัติได้ ก็ไม่จำเป็นที่ต้องมีการหาบุคลากรเพิ่มแต่อย่างใด เพียงแต่ต้องวางแผนในการเพิ่มทักษะบุคคลากรที่มีอยู่ในปัจจุบันหรือสลับสับเปลี่ยนหมุนเวียนเข้ามาใหม่ให้มีความสามารถด้านทักษะด้านการวิเคราะห์ข้อมูลเว็บไซต์หลอกลวง การประสานงานกับหน่วยงานต่างๆ ได้

2) งบประมาณ ต้องมีงบประมาณสนับสนุนจากแหล่งงบประมาณงบประมาณประจำปีหรือกองทุนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมในการจัดทำระบบจัดทำระบบการเฝ้าระวัง ตรวจสอบ วิเคราะห์ และปิดกั้นเว็บไซต์หลอกลวง (Phishing) และงบประมาณในการรณรงค์ สร้างการรับรู้ และแจ้งเตือนภัยออนไลน์ให้แก่ประชาชนอย่างต่อเนื่อง เนื่องจากรูปแบบการหลอกลวงมีการเปลี่ยนแปลงอยู่ตลอดเวลา หากมีการหยุดการพัฒนาระบบงานหรือการประชาสัมพันธ์ในการสร้างการรับรู้ต่างๆ อาญากรรมทางออนไลน์ไม่ได้หยุดมีการเกิดขึ้นตลอดเวลา ปัญหาหรือความเดือดร้อนของประชาชนก็ยังคงอยู่ต่อไป

3) ความร่วมมือกับหน่วยงานต่างๆ ระหว่างประเทศ เนื่องจากปัจจุบันเทคโนโลยีดิจิทัล การสื่อสารต่างๆ มีการติดต่อสื่อสารกันอย่างค่อนข้างอิสระ รวดเร็ว และไร้พรมแดน ในส่วนนี้จำเป็นต้องสร้างกฎกติกาในการอยู่ร่วมกัน อาชญากรรมทางออนไลน์ส่วนใหญ่คนร้ายมักใช้ต่างประเทศเป็นฐานในการก่ออาชญากรรม

เช่น การสื่อสังคมออนไลน์จากประเทศเพื่อนบ้าน และในทำนองเดียวกันต่างประเทศมีการประสานหน่วยงานความมั่นคงแจ้งว่ามีการใช้ประเทศไทยเป็นฐานในการก่ออาชญากรรมทางออนไลน์กับประเทศอื่นเช่นกัน จึงจำเป็นต้องมีความร่วมมือกันในระดับประเทศในการติดต่อประสานงาน แลกเปลี่ยนข้อมูล ในการป้องกันยับยั้ง และปราบปรามอาชญากรรมทางออนไลน์ ไม่ว่าจะเป็นระดับเจ้าหน้าที่ องค์กร หรือระดับนโยบาย เพื่อมีกลไกในความร่วมมือที่มีประสิทธิภาพยิ่งขึ้นต่อไป

2.3 ภาวะผู้นำเพื่อการขับเคลื่อนข้อเสนอ

คุณลักษณะที่สำคัญของผู้นำในการขับเคลื่อนข้อเสนอ “แนวทางการเพิ่มประสิทธิภาพในการตัดวงจรอาชญากรรมออนไลน์” เพื่อให้เกิดเป็นรูปธรรม มีดังนี้

1) การมีวิสัยทัศน์ เนื่องจากสิ่งที่ต้องการผลักดันเป็นเรื่องที่ปรับกระบวนการทางความคิดของผู้ปฏิบัติงาน ดังนั้นผู้นำจะต้องมีวิสัยทัศน์ในการมองเห็นโอกาสในการแก้ปัญหามากกว่าอุปสรรค สามารถวิเคราะห์สภาพแวดล้อมที่เปลี่ยนแปลงไปได้ ทว่าการมีวิสัยทัศน์จะต้องอยู่บนพื้นฐานของความเป็นไปได้ เข้าใจกฎระเบียบต่างๆ ธรรมชาติขององค์กร และบุคลากรภายในหน่วยงานได้เป็นอย่างดี

2) การสร้างและส่งเสริมให้เกิดการทำงานบูรณาการและความร่วมมืออย่างเต็มที่ ต้องใช้ทักษะความสามารถในการสร้างความร่วมมือและการทำงานบูรณาการกับภาคส่วนต่าง ๆ ไม่ว่าจะเป็นภายในองค์กร ระหว่าง องค์กร และการทำงานร่วมกับประชาชนผู้เสียหาย โดยการแบ่งปันข้อมูลอย่างเหมาะสม การสร้างความสัมพันธ์ เพื่อการขับเคลื่อนงานที่มีคุณค่าและเป็นประโยชน์ต่อประชาชนและส่วนรวม

3) การสื่อสารโน้มน้าวใจ การประสานงานจำเป็นอย่างยิ่งในขับเคลื่อนในลักษณะนี้เกี่ยวข้องกับสร้างเครือพันธมิตร ความร่วมมือในลักษณะการทำงานร่วมกัน ไม่เพียงแต่ผู้บังคับบัญชา ผู้ใต้บังคับบัญชา เท่านั้น ดังนั้น ผู้นำจะต้องสามารถสื่อสารภารกิจจากนโยบายและแนวทางการปฏิบัติต่อพันธมิตรหรือผู้มีส่วนเกี่ยวข้องเพื่อขับเคลื่อนงานให้ได้ประโยชน์กันในลักษณะทุกภาคส่วนด้วยเช่นเดียวกัน

3. แผนพัฒนาตนเอง

(ข้อมูลส่วนบุคคลไม่เผยแพร่)

บรรณานุกรม

KEMP, S. (2023, Feb 13). *DIGITAL 2023: THAILAND*. Retrieved from datareportal.com: https://datareportal.com/reports/digital-2023-thailand

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (2566). คณะกรรมการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ครั้งที่ 1/2566.

พันตำรวจตรี ชวลิต น้ำใจสัตย์. (2562). สามเหลี่ยมสัมฤทธิผลของอาชญากรรม

Registrar Abuse Reports, https://www.icann.org/resources/pages/abuse-2014-01-29-en

Introduction to the Advertising Standards, https://transparency.fb.com/policies/ad-standards/

กองป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ภาคผนวก

ประวัติผู้เขียนเอกสารรายงานการศึกษาส่วนบุคคล

นายสัจจะ โชคบุญส่งสวัสดิ์

ประวัติการศึกษา

ปริญญาตรี	วิทยาศาสตรบัณฑิต (ฟิสิกส์ประยุกต์)
	สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง (พ.ศ. 2543)
ปริญญาโท	วิทยาศาสตรมหาบัณฑิต (เทคโนโลยีสารสนเทศ)
	มหาวิทยาลัยพระจอมเกล้าธนบุรี (พ.ศ. 2547)

ประสบการณ์การรับราชการ

6 ตุลาคม 2564 – ปัจจุบัน	ผู้อำนวยการกองป้องกันและปราบปรามการกระความผิดทางเทคโนโลยีสารสนเทศ
12 ตุลาคม 2559 – 5 ตุลาคม 2564	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ
4 กุมภาพันธ์ 2553 - 1 ตุลาคม 2559	นักวิชาการคอมพิวเตอร์ชำนาญการ

รางวัลหรือทุนการศึกษา (เฉพาะที่สำคัญ)

ทุนรัฐบาลญี่ปุ่น Project Management for e-Government Promotion, 2009
ณ JICA Okinawa ประเทศญี่ปุ่น
หลักสูตรการบริหารจัดการความมั่นคงแหงชาติ (บมช.) รุนที่ 14 (สำนักขาวกรองแหงชาติ)

ตำแหน่งหน้าที่ปัจจุบันและสถานที่ทำงาน

ผู้อำนวยการกองป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ
สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม