การรับมือกับกลโกงในโลกไซเบอร์
Dealing with Cyber Scams

สุปราณี วงษ์แสงจันทร์[1] ประภาพร กุลลิ้มรัตน์ชัย[1] และพิมล จงวรนนท์[2]
Supranee Vongsaengjun[1], Prapaporn Kullimratchai[1] and Phimol Chongvoranond[2]
[1]คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยอีสเทิร์นเอเชีย
[1]School of Information Technology, Eastern Asia University
[2]อาจารย์ประจำ มหาวิทยาลัยอีสเทิร์นเอเชีย
[2]Instructor Eastern Asia University
Received: November 26, 2024
Revised: February 27, 2025
Accepted: March 5, 2025

บทคัดย่อ

ปัจจุบันภัยออนไลน์และกลโกงในโลกไซเบอร์เกิดขึ้นอย่างต่อเนื่อง มีการปรับเปลี่ยนรูปแบบกลโกงอย่างสม่ำเสมอ ทำให้เกิดความเสียหายต่อทรัพย์สินของบุคคลในวงกว้างและมีมูลค่าความเสียหายสูง บทความนี้มีวัตถุประสงค์เพื่อนำเสนอข้อมูลเกี่ยวกับกลโกงในโลกไซเบอร์ โดยสามารถแบ่งออกเป็น 4 ประเภท ได้แก่ (1) การหลอกลวงโดยใช้รูปแบบของ Social Engineering (2) การข่มขู่ (3) การควบคุมโดยใช้ระบบคอมพิวเตอร์ และ (4) กลโกงในรูปแบบอื่น ๆ รวมถึงกรณีตัวอย่าง แนวทางป้องกัน การรับมือจากกลโกงและภัยออนไลน์ เพื่อส่งเสริมให้บุคคลมีความรู้และความตระหนักในการป้องกันและสามารถจัดการกับสถานการณ์ที่อาจเกิดขึ้นได้อย่างทันท่วงที

คำสำคัญ: การหลอกลวงทางไซเบอร์ อาชญากรรมทางไซเบอร์ ภัยออนไลน์

Abstract

Nowadays, online threats and cyber scams are continuously occurring, with scam patterns being regularly modified. This causes widespread damage to individuals' property and results in high-value losses. This article aims to present information about cyber scams, which can be categorized into four types: (1) Scams using social engineering techniques, (2) Threatening, (3) Remote access scams, and (4) Other forms of scams, including case studies. It also provides prevention guidelines and response methods to scams and online threats to promote awareness and understanding among individuals so they can immediately manage potential situations.

Keywords: cyber scam, cybercrime, online threats

บทนำ

กลโกงและภัยคุกคามที่เกิดขึ้นในโลกออนไลน์มีแนวโน้มเพิ่มสูงขึ้นอย่างต่อเนื่อง ส่งผลให้เกิดคดีความและมูลค่าความเสียหายที่เกิดจากภัยออนไลน์อย่างมหาศาล การขาดความตระหนักรู้และความเข้าใจต่ออันตรายเหล่านี้อาจนำไปสู่ผลกระทบที่ร้ายแรงต่อบุคคลและองค์กร จึงเป็นสิ่งจำเป็นที่ต้องมีการศึกษาและพัฒนามาตรการป้องกันอย่างเข้มงวดเพื่อลดความเสี่ยงและสร้างความปลอดภัยในสังคมดิจิทัล จากรายงานของสำนักงานตำรวจแห่งชาติ พบสถิติการแจ้งความออนไลน์ ตั้งแต่วันที่ 1 มีนาคม 2565–วันที่ 10 กุมภาพันธ์ 2567 ในประเทศไทยมีการแจ้งความผ่านเว็บไซต์ของศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติ โดยขออายัดบัญชี 148,585 เคส จำนวน 236,038 บัญชี ยอดเงิน 15,025,476,040 บาท สามารถอายัดเงินได้ทัน 2,243,617,705 บาท คิดเป็นร้อยละ 14.93 มีสถิติการแจ้งความออนไลน์ทั้งสิ้น 427,979 เรื่อง มีมูลค่าความเสียหายรวม 59,138,627,839 บาท โดยสรุปจำนวนคดีความออนไลน์ 15 อันดับ ดังภาพ 1

จากสถิติการแจ้งความออนไลน์ตั้งแต่ ปี พ.ศ. 2565–2567 มีมูลค่าความเสียหายรวม 74,893,134,395 บาท เฉลี่ย 77 ล้านบาทต่อวัน ซึ่งประเภทคดีออนไลน์ที่มีการแจ้งความมากที่สุด 5 อันดับแรก มีมูลค่าความเสียหายถึง 56,452,637,652 บาท ซึ่งส่งผลกระทบทั้งภาครัฐ ภาคธุรกิจ สถาบันการเงิน และภาคประชาชนที่ได้รับความเสียหายในวงกว้าง มีรายละเอียดดังภาพ 2

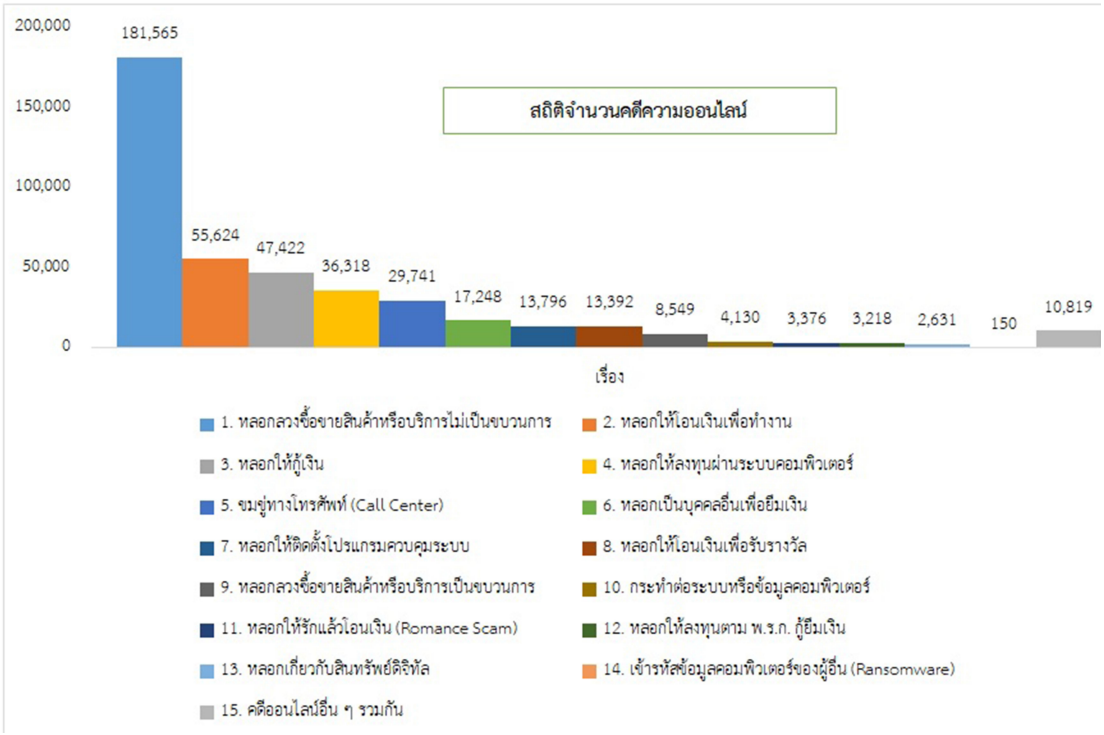
จากการศึกษาปัญหาอาชญากรรมทางเทคโนโลยีที่เกิดขึ้นในชุมชนจังหวัดราชบุรี (Wingworn, 2023) พบปัญหาการถูกหลอกลวงซึ่งแบ่งได้เป็น 5 ลักษณะ คือ (1) ปัญหาการหลอกลวงโดยแก๊งคอลเซ็นเตอร์ (2) ปัญหาการหลอกลวงโดยการขายสินค้าออนไลน์ (3) ปัญหาการถูกแฮกบัญชีโซเชียล (4) ปัญหาการถูกหลอกลวงเพื่อนำเอาเอกสารและข้อมูลส่วนบุคคลไปใช้เพื่ออำนวยความสะดวกต่อการกระทำความผิด และ (5) ปัญหาการชักชวนให้เปิดบัญชีเงินฝากและมีค่าตอบแทนให้ โดยสามารถแบ่งปัญหาอาชญากรรมทางเทคโนโลยีออกเป็น 3 ประเด็น ได้แก่ (1) ปัญหาความไม่รู้เท่าทันต่อกลอุบายของอาชญากรทางเทคโนโลยีที่เข้ามาหลอกลวงให้มีการโอนไปซึ่งทรัพย์สิน/ข้อมูล/เอกสารสำคัญ (2) ปัญหาการไม่รู้กฎหมายเกี่ยวกับสิทธิในกระบวนการยุติธรรม เนื่องจากอาชญากรมักจะอ้างตัวเป็นตำรวจ หรือผู้ที่มีอำนาจในการดำเนินการทางกฎหมาย และข่มขู่ให้เหยื่อกลัวว่าจะถูกดำเนินคดีหากไม่ทำตาม และ (3) ปัญหาขาดความรู้ในการป้องกันตนเองจากอาชญากรรมทางเทคโนโลยีและแนวทางในการดำเนินการเมื่อตกเป็นเหยื่อ

อีกทั้งผู้สูงอายุยังตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ในหลายรูปแบบ (Sarmart & Lerdtomornsakul, 2023) อาทิ (1) การหลอกลวงให้ลงทุนโดยมีผลตอบแทนสูงเป็นสิ่งจูงใจ (2) การหลอกลวงทางโทรศัพท์แบบเป็นกระบวนการหรือแก๊งคอลเซ็นเตอร์ โดยทำให้ตกใจกลัวหรือทำให้เกิดความโลภ หรือหลอกว่าเป็นคนรู้จัก (3) การหลอกซื้อสินค้าออนไลน์ โดยสร้างโปรไฟล์ให้ดูมีความน่าเชื่อถือเป็นสินค้ามีราคาไม่สูงหรือราคาต่ำกว่าท้องตลาด และ (4) การหลอกให้รักทางออนไลน์ โดยใช้จิตวิทยาเพื่อให้หลงรักที่นำไปสู่การหลอกลวงทรัพย์สินเงินทอง

นอกจากนี้ ในต่างประเทศยังพบภัยคุกคามจากอาชญากรรมทางไซเบอร์และการหลอกลวงที่เกิดขึ้นอย่างต่อเนื่อง มีรูปแบบกลโกงประเภทใหม่ ๆ ที่พยายามเจาะจงเป้าหมายให้ถึงเหยื่อโดยตรง (Zhu et al., 2023) ทั้งภาครัฐ ภาคธุรกิจและภาคประชาชน มีผู้ตกเป็นเหยื่อและหลงเชื่อ

เป็นจำนวนมาก ซึ่งแต่ละประเทศยังคงพยายามหาวิธีการป้องกันและการรับมือกับปัญหาดังกล่าวอย่างต่อเนื่อง เช่น การพัฒนาโมเดลการแจ้งเตือนการหลอกลวงด้วยการจำแนกประเภทข้อความ การใช้ข้อมูลและอัลกอริทึมการเรียนรู้เพื่อให้ได้ข้อมูลเชิงลึกนำมาใช้ในการป้องกันภัยออนไลน์ที่เกิดขึ้น การสร้างแพลตฟอร์มและการนำปัญญาประดิษฐ์ (AI) เข้าช่วยวิเคราะห์และป้องกันภัยออนไลน์ในอนาคต เป็นต้น

ดังนั้น บทความนี้จึงมีวัตถุประสงค์เพื่อนำเสนอกรณีตัวอย่างของกลโกงในโลกไซเบอร์ วิธีการรับมือ และแนวทางในการป้องกัน เพื่อให้มีภูมิคุ้มกันและรู้เท่าทันภัยออนไลน์ที่อาจเกิดขึ้นได้



ภาพ 1 สถิติคดีความออนไลน์ ข้อมูล ณ วันที่ 3 มีนาคม 2567

Note. From “Revealing online crime report statistics: Thais lost a total of over 59 billion baht,” by Prachachat Online, 2024, retrieved from https://www.prachachat.net/ict/news-1514260

ภาพ 2 มูลค่าความเสียหายที่เกิดจากคดีออนไลน์ 5 ประเภทที่มีความแจ้งความมากที่สุด ตั้งแต่ปี พ.ศ. 2565 – 2567

Note. From “The government reveals online crime report statistics, showing damages exceeding 70 billion baht from 2022 to 2024,” by Radio Station for Safety and Traffic, 2024, retrieved from https://today.line.me/th/v2/article/3NW25jv

กลโกงในโลกไซเบอร์

จากการรวบรวมข้อมูลภัยกลโกงในโลกไซเบอร์ที่เกิดขึ้นและมีการแจ้งความในประเทศไทย ในที่นี้ ผู้เขียนขอกล่าวถึงภัยคุกคามที่เกิดจากการหลอกลวงที่เป็นส่วนหนึ่งของกลวิธีทางวิศวกรรมสังคม (social engineering influence tactics) (Boonmee, 2023) ซึ่งเป็นรูปแบบของการปฏิบัติการทางจิตวิทยาผ่านการหลอกลวงให้เหยื่อหลงเชื่อเพื่อให้ได้ผลประโยชน์ตามที่ผู้โจมตีต้องการ และแรนซัมแวร์ (ransomware) หรือมัลแวร์เรียกค่าไถ่ (Boonmee & Chavanich, 2021) ซึ่งใช้เทคนิคขั้นสูงขึ้นในการสร้างความเสียหายตั้งแต่ระดับบุคคลไปจนถึงองค์กรขนาดใหญ่ เพื่อสร้างผลตอบแทนให้แฮกเกอร์ ดังนี้

การหลอกลวง เช่น การหลอกลวงทางอินเทอร์เน็ต (phishing) (Immigration Bureau, 2024) หลอกให้ซื้อขายสินค้าหรือบริการทั้งเป็นขบวนการและไม่เป็นขบวนการ หลอกเรียกเก็บเงินค่าสินค้าปลายทางโดยไม่มีการสั่งสินค้า การลงโพสต์ขายสินค้าทางออนไลน์เพื่อหลอกเงินแต่ไม่จัดส่งสินค้า การส่ง QR Code เพื่อหลอกให้โอนเงิน การหลอกว่าได้รับรางวัล หลอกให้โอนเงินเพื่อรับรางวัล/ทำงาน/หารายได้จากการทำกิจกรรมพิเศษ หลอกลวงเกี่ยวกับการจ้างงานที่ไม่จริง (job scam) หลอกให้ไปทำงานต่างประเทศ/โฆษณาชวนไปทำงานต่างประเทศ หลอกให้ลงทุน/หลอกให้เงินกู้ในรูปแบบต่าง ๆ หลอกเกี่ยวกับสินทรัพย์ดิจิทัล หลอกด้วย SMS ปลอม/เฟซบุ๊กปลอม/เว็บไซต์ปลอม (AIS AUNJAI CYBER, 2024) การแอบอ้างว่าเป็นเพื่อนหรือคนรู้จักเพื่อขอยืมเงินผ่านเครือข่ายสังคมออนไลน์ หลอกให้ทำบุญ หลอกด้วยเสน่หา (romance scam) (Aborisade, Ocheja & Okuneye, 2024) หลอกให้รักแล้วลงทุน หลอกให้รักแล้วโอนเงิน/ยืมเงิน หลอกลวงให้ถ่ายภาพโป๊เปลือย หลอกลวงเพื่อเอาข้อมูลส่วนตัว (phishing scam) (Drew & Webster, 2024) หลอกลวงและข่มขู่ให้เกิดความกลัว การหลอกลวงทางโทรศัพท์เป็นขบวนการ (แก๊งคอลเซ็นเตอร์)

การควบคุมโดยใช้ระบบคอมพิวเตอร์ อาทิ การหลอกให้ติดตั้งโปรแกรมควบคุมบนคอมพิวเตอร์หรืออุปกรณ์สื่อสาร โดยกดลิงก์หรือดาวน์โหลดโปรแกรม/แอปพลิเคชันเพื่อควบคุมอุปกรณ์จากระยะไกล (remote access scam) เพื่อกระทำต่อระบบหรือข้อมูล คอมพิวเตอร์ การเข้ารหัสข้อมูลคอมพิวเตอร์ของผู้อื่น การเรียกค่าไถ่ทางคอมพิวเตอร์ (Ransomware)

การฉ้อโกงในรูปแบบอื่น ๆ อาทิ แชร์ลูกโซ่ การพนันออนไลน์ การยินยอมให้ผู้อื่นใช้บัญชีธนาคาร (บัญชีม้า) ข่าวปลอม (fake news) เป็นต้น

การจัดกลุ่มประเภทของกลโกงในโลกไซเบอร์

จากการศึกษากลโกงในโลกไซเบอร์ที่ส่งผลกระทบกับประชนในวงกว้างทั้งในและต่างประเทศ เพื่อสะท้อนให้ตระหนักถึงกลโกงและภัยคุกคามที่ใกล้ตัว ผู้เขียนจึงขอสรุปประเด็นรูปแบบกลโกงในโลกไซเบอร์ ออกเป็น 4 ประเภท ดังนี้ (1) การหลอกลวงโดยใช้รูปแบบของ Social Engineering (2) การข่มขู่เพื่อให้เกิดความกลัว (3) การควบคุมโดยใช้ระบบคอมพิวเตอร์ และ (4) การฉ้อโกงในรูปแบบอื่น ๆ ดังแสดงรายละเอียดในตาราง 1 พร้อมยกตัวอย่างกลโกงและแนวทางป้องกัน จากคดีความและปัญหาที่เกิดขึ้นอย่างต่อเนื่อง โดยมีรายละเอียดดังต่อไปนี้

1. การหลอกลวงโดยใช้รูปแบบของ Social Engineering

1.1 หลอกลวงซื้อ/ขายสินค้าหรือบริการออนไลน์

ในบริบทของผู้บริโภค: มิจฉาชีพทำการเปิดเพจขายสินค้าและใช้ชื่อที่ใกล้เคียงกับเพจจริง รวมถึงใช้ชื่อเพจอื่น ๆ ที่มีการชี้นำไปในลักษณะแอบอ้างเป็นตัวแทนจำหน่ายผลิตภัณฑ์นั้น ๆ ในราคาถูก โดยหลอกขายผลิตภัณฑ์ภายใต้แบรนด์ดังแต่ไม่มีการจัดส่งสินค้าจริง (Royal Thai Police Office, 2023)

มีแนวทางป้องกัน ดังนี้ (1) ตรวจสอบเพจ Facebook ให้แน่ใจก่อนซื้อ โดยดูที่ตัวเลือก “เกี่ยวกับ” “ความโปร่งใส” เพื่อดูว่าเพจเปิดมานานเท่าใด ผู้จัดการเพจอยู่ประเทศไทยหรือไม่ (2) สังเกตช่องกดไลก์มีเครื่องหมาย “โกรธ” จำนวนมากหรือไม่ (3) นำชื่อเพจนั้นไปค้นหาใน Facebook ว่ามีเพจอื่นอีกหรือไม่ เพื่อเปรียบเทียบดูว่าเพจใดจริงหรือปลอม (4) สินค้าที่มีราคาถูกกว่าราคาตลาดมาก ๆ ให้ตั้งข้อสังเกตไว้ว่าอาจหลอกลวง และ (5) บัญชีรับโอนเงินควรเป็นบัญชีชื่อร้าน หากเป็นบัญชีบุคคลธรรมดาให้สงสัยว่าหลอกลวง

ในบริบทของผู้ประกอบการ: เหตุการณ์มิจฉาชีพติดต่อร้านอาหารผ่านแอปพลิเคชันไลน์ หลอกสั่งข้าวกล่องจำนวนมากเพื่อนำไปจัดเลี้ยงและโอนเงินค่ามัดจำให้จำนวนหนึ่ง จากนั้นมิจฉาชีพโทรศัพท์แจ้งว่าต้องการสั่งอาหารเพิ่มและจะจ่ายเงินเพิ่มให้ภายหลัง และส่ง QR Code มาให้ โดยอ้างว่าเพื่อเป็นการแอดไลน์เท่านั้น เมื่อร้านสแกน QR Code แล้ว จะได้รับการแฝงลิงก์ดาวน์โหลดมัลแวร์แบบอัตโนมัติ เพื่อมิจฉาชีพจะควบคุมเครื่องโทรศัพท์เพื่อถอนเงินหรือติดตามการทำงาน (Royal Thai Police Office, 2023)

มีแนวทางป้องกัน ดังนี้ (1) ตรวจสอบให้แน่ใจว่าคู่บัญชีที่ทำธุรกรรมนั้นได้ทำการซื้อขายสินค้ากันจริงหรือไม่ (2) ติดตั้งโปรแกรมหรือแอปพลิเคชันที่สามารถระบุได้ว่าเป็นลิงก์ปลอม (3) หากสแกนแล้วปรากฏลิงก์แปลก

ปลอมหรือไม่น่าเชื่อถือ ไม่ควรกดเข้าไป (4) หลังจากสแกนแล้วหากเข้าเว็บแปลกปลอมให้รีบออกทันที และ (5) หากมีการติดตั้งแอปพลิเคชันที่เป็นอันตรายลงไป ให้มีสติ ปิดเครื่อง ตัดสัญญาณอินเทอร์เน็ตและมือถือทันที

ตาราง 1

การสังเคราะห์ข้อมูลกลโกงในโลกไซเบอร์

ประเภทภัยออนไลน์	Royal Thai Police Office (2024)	Bank of Thailand (2023)	Radio Station for Safety and Traffic (2024)	Thairath Online (2023)	Thaipost (2023)	Prachachat Online (2024)	Matichon Online (2023)	AIS Aunjai Cyber (2024)	Aborisade & Ocheja & Okuneye (2024)	Drew & Webster (2024)	Wang & Topalli (2024)	Zhu et al. (2023)
1. การหลอกลวงโดยใช้รูปแบบของ Social Engineering	✓	✓	✓	✓	✓	✓	✓	✓				✓
1.1 หลอกลวงซื้อ/ขายสินค้าหรือบริการออนไลน์ เช่น การหลอกเรียกเก็บเงิน เช่น เก็บค่าสินค้าปลายทางทั้งที่ไม่ได้มีการสั่งสินค้า หรือการลงโพสต์ขายสินค้าออนไลน์เพื่อหลอกเอาเงินแต่ไม่จัดส่งสินค้า เป็นต้น	✓	✓	✓	✓	✓	✓						
1.2 การหลอกลวงเกี่ยวกับการจ้าง เช่น หลอกจ้างงานที่ไม่มีอยู่จริง (job scam) หลอกให้โอนเงินเพื่อทำงาน หลอกให้ทำงานเสริมออนไลน์ โฆษณาชวนไปทำงานต่างประเทศ เป็นต้น	✓	✓					✓	✓				✓
1.3 การหลอกให้ลงทุน/ หลอกให้กู้เงิน เช่น เงินกู้ออนไลน์ หลอกให้กู้เงินแต่ไม่ได้เงิน หลอกลงทุนในรูปแบบต่าง ๆ เป็นต้น	✓	✓	✓				✓	✓				✓
1.4 การหลอกให้โอนเงินด้วยวิธีต่าง ๆ เช่น การส่ง QR Code การปลอม SMS การปลอมบัญชีเครือข่ายสังคมออนไลน์แล้วหลอกยืมเงิน การแอบอ้างเป็นคนรู้จัก หลอกว่าได้รับรางวัล หลอกให้ทำบุญ เป็นต้น							✓	✓				✓
1.5 การหลอกด้วยเสน่หา (romance scam) เช่น หลอกให้รักแล้วลงทุน หลอกให้รักแล้วโอนเงิน/ยืมเงิน หลอกลวงให้ถ่ายภาพโป๊เปลือย เป็นต้น								✓	✓	✓	✓	✓
2. การข่มขู่เพื่อให้เกิดความกลัว เช่น การข่มขู่ทางโทรศัพท์ (คอลเซ็นเตอร์) ในรูปแบบต่าง ๆ เป็นต้น	✓	✓	✓	✓	✓	✓	✓	✓				
3. การควบคุมโดยใช้ระบบคอมพิวเตอร์ เช่น การหลอกให้กดลิงก์หรือดาวน์โหลดโปรแกรม/แอปพลิเคชัน เพื่อควบคุมคอมพิวเตอร์หรืออุปกรณ์สื่อสารจากระยะไกล (remote access scam) การเรียกค่าไถ่ทางคอมพิวเตอร์ (Ransomware) เพื่อกระทำต่อระบบหรือข้อมูลในคอมพิวเตอร์ เป็นต้น	✓	✓				✓		✓				
4. กลโกงในรูปแบบอื่น ๆ เช่น แชร์ลูกโซ่ การพนันออนไลน์ บัญชีม้า (ยินยอมให้ผู้อื่นใช้บัญชีธนาคาร) ข่าวปลอม (Fake News) เป็นต้น	✓	✓						✓				

1.2 การหลอกด้วยเสน่หา (romance scam) มิจฉาชีพติดต่อพูดคุยกับผู้เสียหายทาง Facebook และเว็บไซต์หาคู่ (Royal Thai Police Office, 2023) จากนั้นอ้างว่า อยากจะมาอยู่ประเทศไทย มาใช้ชีวิตคู่กับผู้เสียหาย จะส่งทรัพย์สินมีค่ามาให้โดยให้ผู้เสียหายโอนเงินเพื่อชำระภาษีและได้เงินจากผู้เสียหายรอบแรก เมื่อมิจฉาชีพสามารถสร้างความเชื่อถือให้กับผู้เสียหายได้แล้วจะหลอกให้ผู้เสียหายเปิดบัญชีเพื่อลงทุนทำธุรกิจร่วมกัน (Anesa, 2020) จากนั้นมิจฉาชีพจะไปหลอกผู้เสียหายคนที่สองและให้โอนเงินเข้าบัญชีผู้เสียหายคนแรก สุดท้ายมิจฉาชีพให้ผู้เสียหายคนแรกซื้อเหรียญคริปโตให้ บัญชีผู้เสียหายคนแรกจึงกลายเป็นบัญชีม้า (ใช้บัญชีผู้อื่นรับโอนเงินจากผู้กระทำผิด) (The Thai Bankers Association, 2024) โดยมิจฉาชีพมักใช้รูปโปรไฟล์ชาวต่างชาติหน้าตาดีหรือมีประวัติการทำงานที่ดีและมั่นคง ซึ่งข้อมูลและรูปเหล่านี้ได้มาจากหลายแหล่งในอินเทอร์เน็ต มิจฉาชีพที่ใช้กลโกงลักษณะนี้มักมีการหลอกให้โอนเงินโดยใช้ข้ออ้างต่าง ๆ

มีแนวทางป้องกัน ดังนี้ (1) ตรวจสอบตัวตนของคนในโลกโซเชียลโดยการโทรพูดคุยผ่าน messenger หรือโทรศัพท์ปกติ เพื่อสังเกตสำเนียงการใช้ภาษาพูดว่าเป็นบุคคลที่กล่าวอ้างหรือไม่ (2) ถ้ามีการชักชวนให้เปิดบัญชีเพื่อลงทุนหรือเทรดเงินคริปโต หลังจากสร้างความเชื่อมั่นในระยะเวลาไม่นาน ให้ปฏิเสธและปิดกั้นการสนทนา (3) ควรเรียนรู้และกระทำการลงทุนหรือเทรดเงินคริปโตด้วยตนเอง และ (4) ควรมีสติทุกครั้งเมื่อมีการทำธุรกรรมใด ๆ กับบุคคลที่ไม่รู้จัก

2. การข่มขู่เพื่อให้เกิดความกลัว

2.1 คอลเซ็นเตอร์หลอกดูดเงินในบัญชี มิจฉาชีพจะใช้หลักจิตวิทยาในการโน้มน้าวให้เชื่อ โดยแอบอ้างเป็นเจ้าหน้าที่ของหน่วยงานรัฐหรือองค์กรต่าง ๆ (Tuncharoen & Assawaboonmee 2023) เพื่อให้ผู้รับสารทำตามอุบายที่วางไว้ภายในเวลาที่จำกัด หรือล่อด้วยผลตอบแทนที่ต้องรีบตัดสินใจ เพื่อกระตุ้นให้เหยื่อรีบทำตาม โดยขาดการคิดให้รอบคอบ หนึ่งในวิธีการที่มิจฉาชีพนิยมใช้คือการหลอกขอข้อมูลและให้ติดตั้งแอปพลิเคชันปลอม จากนั้นจะเข้าควบคุมโทรศัพท์มือถือของเหยื่อจากระยะไกล แล้วทำการโอนเงินของเหยื่อออกมาอย่างรวดเร็วโดยไม่ต้องเห็นหน้าหรือเจอตัวกัน รูปแบบการหลอกดูดเงินในบัญชีมีขั้นตอนหลัก ๆ ดังนี้ (1) ติดต่อเข้ามาหาเหยื่อโดยอ้างเป็นหน่วยงานรัฐหรือองค์กรต่าง ๆ เช่น กรมสรรพากร กรมที่ดิน กรมบัญชีกลาง กรมบังคับคดี การไฟฟ้า การประปา สถาบันการเงิน สำนักงานตำรวจ สายการบิน ศูนย์บัตรเครดิต เป็นต้น (2) มิจฉาชีพมักจะบอก ชื่อ หรือข้อมูลเบื้องต้นของเหยื่อได้ถูกต้อง เพื่อสร้างความน่าเชื่อถือและทำให้เกิดการหลงเชื่อ (3) จากนั้นมิจฉาชีพจะหลอกขอข้อมูลที่จำเป็นอื่น ๆ เพิ่มเติม โดยให้เหยื่อเพิ่มเพื่อนใน LINE เพื่อแชตคุยส่วนตัว (4) อาจจะมีการส่งลิงก์ให้คลิกหรือส่งไฟล์ให้เหยื่อดาวน์โหลด เพื่อติดตั้งแอปพลิเคชันที่มิจฉาชีพเตรียมไว้สำหรับการเข้าควบคุมอุปกรณ์มือถือ โดยแอปพลิเคชันที่ให้ติดตั้งจะเป็นแอปพลิเคชันปลอมที่ใช้ชื่อตามหน่วยงานที่นำมาแอบอ้าง (5) หลังจากเหยื่อติดตั้งแอปพลิเคชันตามคำกล่าวอ้างแล้ว มิจฉาชีพจะหลอกให้กรอกข้อมูลต่าง ๆ เพิ่มเติม รวมถึงสแกนใบหน้าเพื่อยืนยันตัวตน ซึ่งข้อมูลที่ให้ไปหรือกดส่งไปในขั้นตอนนี้จะเป็นเหมือนการอนุญาตให้มิจฉาชีพสวมรอยเข้ามาทำธุรกรรมในนามเหยื่อได้ทันที (6) โทรศัพท์มือถือของเหยื่อจะถูกล็อก มิจฉาชีพจะโอนเงินในบัญชีของเหยื่อออกไปยังบัญชีม้าทันที และ (7) มิจฉาชีพจะนำข้อมูลส่วนตัวของเหยื่อมาเก็บไว้เพื่อหลอกลวงในรูปแบบอื่น ๆ ต่อไป

มีแนวทางป้องกัน ดังนี้ หากไม่มั่นใจว่าเป็นหน่วยงานจริงติดต่อมาหรือไม่ ให้สอบถามไปที่เบอร์สายด่วนของหน่วยงานนั้นโดยตรง ซึ่งโดยปกติแล้วหน่วยงานหรือองค์กรต่าง ๆ หากมีเรื่องสำคัญที่เกี่ยวข้องกับลูกค้า ประชาชน จะมีการประกาศแจ้งเป็นทางการบนเว็บไซต์หรือโซเชียลมีเดียของหน่วยงานนั้น ๆ ล่วงหน้า (Siam Commercial Bank, 2023) และจะมีระยะเวลาให้เตรียมตัวหรือดำเนินการอย่างน้อยเป็นหลักเดือนขึ้นไป จะไม่มีบริการติดต่อเข้ามาเสนอให้บริการโดยแชตคุยเป็นการส่วนตัวเด็ดขาด ในกรณีที่ตกเป็นเหยื่อของมิจฉาชีพ ให้รีบติดต่อธนาคารเจ้าของบัญชีเพื่ออายัดบัญชีให้เร็วที่สุด และดำเนินการแจ้งความออนไลน์ผ่าน https://thaipoliceonline.go.th/ ตามขั้นตอน

2.2 การข่มขู่ทางโทรศัพท์ เหตุการณ์หลอกลวงนักศึกษาเกิดขึ้นในพื้นที่จังหวัดนครราชสีมา (Thaipbs,

2024) โดยแก๊งคอลเซ็นเตอร์อ้างตัวเป็นเจ้าหน้าที่ตำรวจ และพบหมายเลขบัตรประชาชนของผู้เสียหายเกี่ยวข้องกับคดีต่าง ๆ เช่น การติดตั้งอินเทอร์เน็ตบ้านแล้วไม่จ่ายเงิน พัวพันกับเว็บพนันออนไลน์ เป็นต้น จากนั้นมิจฉาชีพเหล่านี้จะใช้กลวิธีทางจิตวิทยาในการสื่อสารและเจรจากับผู้เสียหาย เพื่อล่อลวงให้ไปยังสถานที่เงียบ ๆ ตามลำพัง โดยอ้างว่ามีการดำเนินคดีที่เกี่ยวข้องกับผู้เสียหาย และต้องการพูดคุยเพื่อแก้ไขปัญหา เมื่อผู้เสียหายตกเป็นเหยื่อและไปยังสถานที่ที่ถูกนัดหมาย มิจฉาชีพจะเริ่มบอกให้ผู้เสียหายโอนเงินเพื่อเป็นค่าดำเนินคดี หรือขอให้ผู้เสียหายไปหลอกลวงผู้ปกครองด้วยการอ้างว่าถูกทำร้ายร่างกายหรือถูกจับตัว เพื่อให้ผู้ปกครองโอนเงินให้ โดยโอนเงินเข้าบัญชีของผู้เสียหายก่อนแล้วจึงโอนเงินไปยังบัญชีม้าอีกทอดหนึ่งเพื่อป้องกันการติดตามตัว

มีแนวทางป้องกัน ดังนี้ ในกรณีที่มีสายโทรเข้าในลักษณะที่น่าสงสัย ควรเดินทางไปยังสถานีตำรวจที่ใกล้ที่สุด เนื่องจากเจ้าหน้าที่ตำรวจในทุกสถานีสามารถตรวจสอบได้ว่าท่านมีหมายจับหรือมีคดีจริงหรือไม่ และควรระมัดระวังในการกรอกข้อมูลบนสื่อสังคมออนไลน์ การให้ข้อมูลส่วนบุคคลทางออนไลน์ที่ต้องส่งสำเนาบัตรประชาชนทั้งด้านหน้าและด้านหลัง เบอร์ติดต่อ รวมทั้งการสแกนใบหน้า

3. การควบคุมโดยใช้ระบบคอมพิวเตอร์ กรณีการแฮกข้อมูลโรงพยาบาลเพชรบูรณ์ที่ถูกโจมตีในลักษณะของแรนซัมแวร์หรือมัลแวร์เรียกค่าไถ่ในปี 2564 ทำให้ข้อมูลผู้ป่วยจำนวน 16 ล้านคนถูกขโมยและมีการขายในตลาดมืด (Thaipbs, 2024) โดยสาเหตุของการถูกแฮกอาจมาจากช่องโหว่ในระบบคอมพิวเตอร์ หรือเกิดจากความผิดพลาดของบุคลากรที่เผลอกดลิงก์ที่เป็นอันตราย เหตุการณ์นี้ไม่ใช่ครั้งแรกที่กระทรวงสาธารณสุขถูกโจมตี เนื่องจากใน ปี 2563 โรงพยาบาลสระบุรีเคยถูกแฮกข้อมูลด้วยวิธีเดียวกัน โดยถูกเรียกค่าไถ่เป็นเงินจำนวน 200,000 บิตคอยน์ (63,000 ล้านบาทไทย) ข้อมูลที่ถูกแฮกในกรณีนี้ไม่ได้เป็นข้อมูลทุกอย่างจากระบบเซิร์ฟเวอร์ แต่เป็นข้อมูลบางส่วนในนระบบการรักษาที่ถูกดึงออกมาเพื่อการวิเคราะห์

มีแนวทางป้องกัน ดังนี้ (1) ไม่กดลิงก์ที่ไม่น่าเชื่อถือ (2) ไม่ควรกรอกข้อมูลส่วนตัวทางออนไลน์ในเว็บไซต์ที่ไม่รู้จัก รวมถึงเว็บไซต์ที่ไม่มีความน่าเชื่อถือ (3) ในการใช้คอมพิวเตอร์สาธารณะ ไม่ควรใช้เว็บไซต์ที่ต้องล็อกอินโดยใช้ข้อมูลส่วนตัว เช่น การล็อกอินเข้าเครือข่ายสังคมออนไลน์หรือเว็บไซต์ของธนาคารเพื่อทำธุรกรรมทางการเงิน (4) ควรตั้งค่าการแจ้งเตือนกับบัญชีธนาคารและบัตรเครดิต เพื่อให้ทราบการเคลื่อนไหวหากมีการทำธุรกรรม และ (5) ไม่เข้าเว็บไซต์หรือดาวน์โหลดแอปพลิเคชันแปลกหรือถูกแนะนำจากคนที่ไม่รู้จัก

4. กลโกงในรูปแบบอื่น ๆ เช่น แชร์ลูกโซ่ เป็นกลโกงที่มีการพัฒนาให้ซับซ้อนยิ่งขึ้นตามยุคสมัย โดยการระดมทุนจากสมาชิกที่ตกเป็นเหยื่อ จูงใจด้วยผลตอบแทนที่สูง และมักอ้างว่าจะนำไปลงทุนในธุรกิจที่มีกำไรดีแต่ไม่นำเงินไปลงทุนจริง เพียงต้องการหาสมาชิกใหม่ให้ได้จำนวนมากเพื่อนำเงินจากเหยื่อรายใหม่มาจ่ายให้รายเก่า ซึ่งจะทำแบบนี้เป็นทอด ๆ กันเป็นลูกโซ่ เมื่อถึงจุดที่ธุรกิจหมุนเงินไม่ทันจะเริ่มเลื่อนการจ่ายผลตอบแทน สุดท้ายวงแชร์ลูกโซ่นี้ก็จะถึงจุดจบ ตัวอย่างเช่น แชร์แม่ชม้อย แชร์ชาร์เตอร์ แชร์เสมาฟ้าคราม แชร์บลิสเซอร์ แชร์ลูกโซ่ยูฟัน แชร์แม่มณี คดี Forex-3D (PPTV Online, 2024) คดีบิ๊กบอสและบอสดาราเครือข่ายดิไอคอน โครงการสุขภาพเครือข่ายหมอบุญ เป็นต้น

มีแนวทางป้องกัน ดังนี้ เมื่อตัดสินใจลงทุนควรดูข้อมูลจากบริษัทที่มีการรับรองอย่างถูกต้อง ภายใต้การกำกับของตลาดหลักทรัพย์ฯ ธนาคารแห่งประเทศไทย (ธปท.) สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) หรือ สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) ซึ่งเป็นหน่วยงานกำกับดูแลอย่างเป็นทางการจะมีความปลอดภัยในระดับหนึ่ง หากมีการแนะนำการลงทุนที่ไม่ถูกต้องนักลงทุนสามารถร้องเรียนไปยังหน่วยงานที่กำกับดูแลได้ หากได้รับการชักชวนลงทุนโดยมีข้อเสนอที่ดีเกินความเป็นจริง ให้ตั้งข้อสังเกตว่าอาจเป็นการหลอกลวง นอกจากนี้หากมีข้อสงสัยว่าการลงทุนนั้น ๆ เข้าข่ายว่าจะเป็นแชร์ลูกโซ่หรือผิดกฎหมายหรือไม่ สามารถสอบถามข้อมูลเพิ่มเติมกับหน่วยงานที่เกี่ยวข้อง ดังนี้ (1) สำนักงานคณะกรรมการคุ้มครองผู้บริโภค โทร. 1166 (2) กรมสอบสวนคดีพิเศษ (DSI) โทร. 1202 (3) กรมพัฒนาธุรกิจการค้า โทร.1570

(4) ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย โทร. 1213 (5) ศูนย์รับแจ้งการเงินนอกระบบ สำนักงานเศรษฐกิจการคลัง กระทรวงการคลัง โทร. 1359 และ (6) สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) โทร. 1207

การรับมือจากกลโกงและภัยออนไลน์

การลดโอกาสการเกิดปัญหาอาชญากรรมทางคอมพิวเตอร์มีมาตรการที่หลากหลาย แนวทางหนึ่งที่สามารถดำเนินการเพื่อทำให้ตนเองปลอดภัยจากการหลอกลวงทางไซเบอร์ จากการใช้คอมพิวเตอร์ สมาร์ตโฟน รวมถึง Mobile Banking Application (Krungsri GURU, 2024; Northern Trust, 2024) ควรยึดแนวปฏิบัติดังต่อไปนี้ (1) ไม่เก็บข้อมูลส่วนตัวในสมาร์ตโฟน เพราะหากสูญหายข้อมูลอาจตกไปอยู่ในมือมิจฉาชีพได้ (2) ไม่ใช้รหัสล็อกหน้าจอโทรศัพท์เดียวกับรหัสเข้า Mobile Banking Application เพื่อให้มิจฉาชีพเข้าถึงข้อมูลได้ยากขึ้น (3) จำกัดวงเงินในการใช้งาน Mobile Banking Application เพื่อลดมูลค่าความเสียหายหากถูกโอนเงินออกจากบัญชี (4) ควรลงชื่อออกจากบัญชีหรือปิดแอปพลิเคชันทุกครั้งเมื่อทำธุรกรรมเสร็จ เพื่อป้องกันการเข้าถึงจากบุคคลอื่น (5) เปิดรับการแจ้งเตือนผ่าน SMS และ e-mail เสมอ (6) ตรวจสอบข้อมูลธุรกรรมเป็นประจำว่าเป็นของตนเองหรือไม่ (7) ตรวจสอบข้อมูลการขอใช้สิทธิ์การเข้าถึงข้อมูลแอปพลิเคชันต่าง ๆ ในสมาร์ตโฟนไม่ให้เกินขอบเขตการใช้งาน (8) ควรตรวจสอบแอปพลิเคชันที่น่าเชื่อถือก่อนการติดตั้ง (9) อัปเดตอุปกรณ์คอมพิวเตอร์และสมาร์ตโฟนอย่างต่อเนื่อง (10) ใช้ซอฟต์แวร์ป้องกันไวรัสและมัลแวร์บนคอมพิวเตอร์และสมาร์ตโฟน (11) เคร่งครัดกับการตั้งรหัสผ่านที่ดี (12) สร้างระบบเครือข่ายภายในบ้านให้รัดกุม (13) สำรองข้อมูลบนคอมพิวเตอร์และสมาร์ตโฟนอย่างสม่ำเสมอ (14) พูดคุยและแลกเปลี่ยนในเรื่องของความปลอดภัยทางอินเทอร์เน็ตภายในครอบครัว (15) เข้าใจและป้องกันการถูกขโมยข้อมูลประจำตัว (16) รู้ว่าควรทำอย่างไรหากตกเป็นเหยื่อจากภัยออนไลน์ และ (17) ตั้งสติและดูแลรักษาข้อมูลส่วนตัวของตนเองตลอดเวลา

นอกจากนี้ คณะทำงานสร้างเสริมภูมิคุ้มกันภัยอาชญากรรมทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ จัดทำแอปพลิเคชันไซเบอร์วัคซีน (Cyber vaccinated) ซึ่งเป็นระบบประเมินภูมิคุ้มกันภัยทางไซเบอร์ รวบรวมสื่อความรู้เพื่อป้องกันตนเองจากภัยออนไลน์ โดยมีการแบ่งหมวดหมู่ตามประเภทกลโกงออนไลน์ ระบุเรื่องที่พบบ่อย วิธีการของคนร้าย วิธีการสังเกต รวมถึงวิธีการป้องกัน (Royal Thai Police Office, 2024) การติดตั้งแอปพลิเคชัน Whoscall ซึ่งเป็นแอปพลิเคชันที่มีฟังก์ชัน Caller ID & Blocker ช่วยระบุเบอร์โทรศัพท์ที่ไม่รู้จัก เพื่อช่วยตัดสินใจในการรับสายหรือเลือกที่จะบล็อกสายมิจฉาชีพ

หากได้รับการชักชวนเพื่อลงทุน ควรตรวจสอบความน่าเชื่อถือในเบื้องต้นของผู้ชักชวนลงทุน ผ่านช่องทางของสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) ดังนี้ (1) เว็บไซต์ market.sec.or.th/LicenseCheck เพื่อค้นหารายชื่อผู้ให้บริการในตลาดทุนที่อยู่ภายใต้การกำกับดูแลของ ก.ล.ต. รวมถึงผลิตภัณฑ์ที่ได้รับอนุญาต (2) แอปพลิเคชัน SEC Check First ช่วยในการกรองข้อมูลผู้ที่ได้รับหรือไม่ได้รับอนุญาตจาก ก.ล.ต. โดยใส่ชื่อหลักทรัพย์ ผลิตภัณฑ์การลงทุน หรือผู้ให้บริการ และ (3) โทรตรวจสอบเรื่องหลอกลงทุนในตลาดทุนกับสายด่วน ก.ล.ต. (SEC Help Center) โทร. 1207 กด 22 อย่างไรก็ตาม หากเกิดปัญหาขึ้นแล้ว สามารถแจ้งความผ่านระบบบนเว็บไซต์ www.thaipoliceonline.com หรือสายด่วน 1441

ในต่างประเทศตระหนักถึงภัยออนไลน์ที่เกิดขึ้น โดยกำหนดมาตรการรับมือ (Bank of Thailand, 2023) ดังต่อไปนี้ อาทิ ประเทศอังกฤษมีการนำเทคโนโลยีปัญญาประดิษฐ์ (AI) ที่ทันสมัยมาช่วยธนาคารเพิ่มประสิทธิภาพเพื่อยับยั้งการโจรกรรมได้อย่างทันท่วงที โดย AI จะทำการวิเคราะห์พฤติกรรมการเงินของลูกค้า เพื่อตรวจจับการเคลื่อนไหวที่เข้าข่ายผิดปกติ เช่น โอนเงินไปยังบัญชีที่อาจเป็นธุรกิจหรือบุคคลปลอมหรือผิดกฎหมาย AI จะตรวจสอบข้อมูลการทำธุรกรรมแบบบัญชีต่อบัญชี (account-to-account) และช่วยวิเคราะห์ข้อมูลสำคัญ เช่น ชื่อบัญชี จำนวนเงิน ประวัติการทำธุรกรรมของผู้โอนและผู้รับ รวมถึง

ความเป็นไปได้ที่บัญชีผู้รับเงินอาจเกี่ยวข้องกับการโจรกรรม อีกทั้ง ยังสามารถสืบค้นข้อมูลการกระทำความผิดของเจ้าของบัญชี ช่วยทำให้หลายธนาคารสามารถระงับธุรกรรมต้องสงสัยได้แบบเรียลไทม์ (real-time) ก่อนเกิดความเสียหาย ประเทศออสเตรเลียจัดทำแพลตฟอร์ม Fraud Reporting Exchange ช่วยธนาคารรับเรื่องร้องเรียน สื่อสาร ติดตาม และระงับการทำธุรกรรมที่เป็นการฉ้อโกงระหว่างธนาคารสมาชิกแบบเรียลไทม์ เพื่อช่วยลดขั้นตอนระหว่างธนาคาร ผู้รับโทรศัพท์ และตอบอีเมล รวมทั้งมีการจัดตั้งศูนย์ต่อต้านการหลอกลวงแห่งชาติ (National Anti-Scam Centre) เพื่อประสานงานกับรัฐบาล หน่วยงานผู้บังคับใช้กฎหมาย และภาคเอกชน เพื่อแก้ปัญหาอย่างรอบด้าน ครอบคลุมการปรับแก้กฎหมายและเกณฑ์ต่าง ๆ ให้เหมาะสมกับสถานการณ์ใหม่ ๆ ที่เปลี่ยนแปลงไป

อย่างไรก็ตาม ในประเทศไทยโดยคณะกรรมการป้องกันและปราบปรามอาชญากรรมออนไลน์ทางเทคโนโลยี ได้มีการหารือกับหน่วยงานที่เกี่ยวข้อง ได้แก่ กระทรวงการต่างประเทศ กระทรวงมหาดไทย กระทรวงกลาโหม ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) สำนักงานตำรวจแห่งชาติ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และโทรคมนาคมแห่งชาติ (กสทช.) ธนาคารแห่งประเทศไทย (ธปท.) สมาคมธนาคารไทย สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) กรมสอบสวนคดีพิเศษ (DSI) สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) และคณะกรรมการคุ้มครองผู้บริโภค (สคบ.) โดยกำหนดมาตรการในการแก้ปัญหาอาชญากรรมออนไลน์ ดังนี้

1. บูรณาการข้อมูล โดยใช้ศูนย์ปฏิบัติการแก้ไขปัญหาอาชญากรรมออนไลน์ (Anti Online Scam Operation Center: AOC) ในการเชื่อมโยงข้อมูลของทุกหน่วยงาน ซึ่งทุกหน่วยงานจะต้องส่งข้อมูลที่เกี่ยวข้อง เช่น ข้อมูลบัญชีม้า ซิมม้า ข้อมูล URL/Line ของเว็บพนัน หรือข้อมูลอื่น ๆ ที่ศูนย์ AOC ร้องขอ รวมทั้งพัฒนาระบบบูรณาการข้อมูลให้มีความมั่นคงปลอดภัย และไม่ขัดต่อกฎหมายคุ้มครองข้อมูลส่วนบุคคล

2. กำหนดมาตรการแก้ไขปัญหาบัญชีม้า โดยนำบัญชีม้าออกจากระบบอย่างเร่งด่วน และป้องกันการเกิดบัญชีม้าเข้าสู่ระบบ โดยกำกับการเปิดบัญชีออนไลน์ การเปิดบัญชีหลายบัญชี และต้องมีมาตรการตรวจสอบก่อนอนุมัติเปิดบัญชี

3. จัดการเสาโทรคมนาคม สายสัญญาณอินเทอร์เน็ต และสายโทรศัพท์ ที่ผิดกฎหมายตามแนวชายแดนประเทศเพื่อนบ้าน โดยร่วมกับหน่วยงานภาครัฐเพื่อปิดกั้น และจับกุมผู้กระทำความผิด

4. จับกุมปราบปรามชาวต่างชาติที่อยู่ในประเทศไทยที่มีพฤติกรรมผิดกฎหมาย โดยเฉพาะการชักชวนหลอกลวงคนไทยไปทำงานเป็นแก๊งคอลเซ็นเตอร์ในประเทศเพื่อนบ้าน ทั้งนี้ ให้ความสำคัญกับจังหวัดที่มีพรมแดนติดกับประเทศเพื่อนบ้าน

5. จับกุมปราบปรามอาชญากรรมออนไลน์ โดยดำเนินการจัดทำแผนปฏิบัติการปราบปรามแก๊งคอลเซ็นเตอร์และอาชญากรรมออนไลน์ บูรณาการแผนร่วมกับหน่วยงานที่เกี่ยวข้อง และดำเนินการสืบสวน สอบสวน และขยายผลการเอาผิดกับเจ้าหน้าที่ที่ร่วมการกระทำความผิดอาชญากรรมออนไลน์

6. การแก้ไขกฎหมาย กฎระเบียบ เกี่ยวกับการแก้ปัญหาภัยออนไลน์ อาทิ (1) กฎหมายหรือกฎระเบียบที่เกี่ยวกับการบริการเก็บเงินปลายทางสำหรับพาณิชย์อิเล็กทรอนิกส์ (COD) เพื่อขจัดปัญหาการหลอกขายสินค้าออนไลน์ (2) ระเบียบการกำกับดูแลสินทรัพย์ดิจิทัลของผู้ประกอบธุรกิจ P2P และประกาศใช้เพื่อตัดช่องทางการโอนเงินไปเป็นสกุลเงินดิจิทัลออกจากบัญชีม้า (3) กฎระเบียบเกี่ยวกับการใช้บริการข้อความสั้น (SMS) ในการส่งข้อความหรือส่งลิงก์หลอกลวง (4) กฎหมายเกี่ยวกับการแก้ไขปัญหาการคืนเงินให้แก่ผู้เสียหาย และ (5) ปรับปรุงแก้ไขกฎหมาย กฎระเบียบ ที่เกี่ยวข้องกับการซื้อขายข้อมูลส่วนบุคคล

7. จัดตั้งห้องปฏิบัติการปัญญาประดิษฐ์เพื่อวิเคราะห์ข้อมูลสำหรับ AOC (AOC Data Lab) เพื่อใช้ในการวิเคราะห์ตรวจสอบข้อมูล รวมทั้งกำหนดนโยบายการแก้ไขและป้องกันอาชญากรรมออนไลน์

มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 (Royal Thai Police Office, 2023; Pokudom, 2020) ระบุมาตรการและบทลงโทษในการรับมืออาชญากรรมทางเทคโนโลยี ดังนี้

1. กำหนดให้ผู้เสียหายสามารถติดต่อธนาคารเพื่อระงับธุรกรรมของบัญชีต้องสงสัยชั่วคราวได้โดยตรงทันที จากนั้นจึงไปร้องทุกข์ต่อพนักงานสอบสวน

2. กรณีธนาคารพบธุรกรรมต้องสงสัย สามารถระงับธุรกรรมชั่วคราว แล้วส่งให้เจ้าหน้าที่ตำรวจตรวจสอบ

3. ผู้เสียหายสามารถร้องทุกข์ที่สถานีตำรวจ หรือที่กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี และพนักงานสอบสวนผู้รับคำร้องทุกข์เป็นพนักงานสอบสวนผู้รับผิดชอบ โดยผู้เสียหายต้องแจ้งความร้องทุกข์ภายใน 72 ชั่วโมง และพนักงานสอบสวนจะรวบรวมพยานหลักฐานแจ้งกลับไปยังธนาคารของบัญชีนั้นภายใน 7 วัน เพื่อยืนยันการระงับธุรกรรมของบัญชีนั้น

4. ให้อำนาจเจ้าหน้าที่ตำรวจกรมสอบสวนคดีพิเศษ (DSI) และ สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) มีอำนาจนำข้อมูลต้องสงสัยไปใช้ประโยชน์ได้โดยไม่เป็นความผิดตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

การกำหนดฐานความผิดและบทลงโทษสำหรับอาชญากรรมทางเทคโนโลยี ดังตาราง 2

ตาราง 2

ฐานความผิดและบทลงโทษตามมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566

ฐานความผิด	อัตราโทษ
เปิดหรือยินยอมให้บุคคลอื่นใช้บัญชีเงินฝาก (บัญชีม้าหรือซิมม้า) โดยรู้หรือควรรู้ว่าจะนำไปใช้ในการกระทำความผิด	จำคุกไม่เกิน 3 ปี ปรับไม่เกิน 300,000 บาท หรือทั้งจำทั้งปรับ
เป็นธุระ จัดหา โฆษณา หรือกระทำเพื่อให้มีการซื้อ ขายบัญชี (บัญชีม้าหรือซิมม้า) เพื่อใช้ในการกระทำความผิด	จำคุกตั้งแต่ 2 ถึง 5 ปี ปรับตั้งแต่ 200,000 ถึง 500,000 บาท หรือทั้งจำทั้งปรับ
เป็นธุระ จัดหา โฆษณา หรือกระทำเพื่อให้มีการซื้อ ขายหมายเลขโทรศัพท์ซึ่งลงทะเบียนในนามบุคคลอื่นแล้ว แต่ไม่สามารถระบุตัวผู้ใช้จริงได้ (คนจัดหาบัญชีม้า)	จำคุกตั้งแต่ 2 ถึง 5 ปี ปรับตั้งแต่ 200,000 ถึง 500,000 บาท หรือทั้งจำทั้งปรับ

สรุป

ภัยคุกคามในโลกไซเบอร์จากอดีตจนถึงปัจจุบันทั้งในและต่างประเทศยังคงเกิดขึ้นและทวีจำนวนเพิ่มขึ้นอย่างต่อเนื่อง อีกทั้งมิจฉาชีพหรือแฮกเกอร์ยังพยายามพัฒนารูปแบบกลโกงใหม่ ๆ และสร้างความเดือดร้อนแก่ประชาชน แม้แต่ผู้ที่มีความรู้และองค์กรขนาดใหญ่ก็ยังคงตกเป็นเหยื่อจากภัยออนไลน์ ซึ่งในบทความนี้ได้จัดกลุ่มกลโกงในโลกไซเบอร์ออกเป็น 4 กลุ่ม ได้แก่ (1) การหลอกลวงโดยใช้รูปแบบของ Social Engineering (2) การข่มขู่เพื่อให้เกิดความกลัว (3) การควบคุมโดยใช้ระบบคอมพิวเตอร์ และ (4) การฉ้อโกงอื่น ๆ ซึ่งทุกคนควรศึกษาทำความเข้าใจในแต่ละประเด็น เพื่อช่วยลดปัญหาที่อาจเกิดขึ้นและสามารถให้คำแนะนำกับผู้ที่ตกเป็นเหยื่อจากภัยออนไลน์ในแต่ละประเภทได้

ทุกหน่วยงาน/องค์การมีความจำเป็นต้องจัดทำนโยบายจัดทำระบบ และการดำเนินงานตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล โดยการกำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคล การให้สิทธิแก่เจ้าของข้อมูลเพื่อตรวจสอบ แก้ไข หรือลบข้อมูลที่ร้องขอได้ การจัดทำระบบการรักษาความปลอดภัยและการโอนย้ายข้อมูล การตรวจประเมินมาตรฐานการรักษาข้อมูล เป็นต้น อีกทั้งยังต้องติดตามภัยออนไลน์ที่มีการพัฒนารูปแบบการหลอกลวงใหม่ ๆ ตลอดเวลา อาทิ ภัยคุกคามจากปัญญาประดิษฐ์ (Artificial Intelligence: AI) และเทคโนโลยีใหม่ ๆ อาทิ Deepfake Scams AI-Generated Phishing และ Voice Cloning Fraud เป็นต้น

รวมทั้งการส่งเสริมให้ภาคประชาชนมีความรู้เท่าทันการหลอกลวงทางไซเบอร์และตระหนักถึงภัยออนไลน์ที่อาจเกิดขึ้น โดยมีแนวทางการดำเนินการ ดังนี้

1. ประเมินตนเองเพื่อให้รู้ว่ามีความเสี่ยงต่อการถูกหลอกลวงในโลกไซเบอร์มากน้อยเพียงใด

2. สร้างภูมิคุ้มกันโดยการติดตามข่าวสารจากสื่อความรู้ในการเสริมสร้างภูมิคุ้มกันป้องกันภัยอาชญากรรมทางเทคโนโลยีที่ผู้เขียนได้รวบรวมไว้

3. การรับมือ/แก้ปัญหาในกรณีที่ตกเป็นเหยื่อจากภัยออนไลน์ให้ดำเนินการตามประเด็นที่ได้นำเสนอไว้ในบทความข้างต้น

อย่างไรก็ตาม หากยึดถือแนวปฏิบัติและข้อแนะนำจากบทความนี้อาจช่วยบรรเทาปัญหาและลดความเสี่ยงจากการตกเป็นเหยื่อของมิจฉาชีพในรูปแบบต่าง ๆ พร้อมสามารถรับมือกับภัยออนไลน์ที่อาจเกิดขึ้นได้อย่างมีสติ

References

Aborisade, R. A., Ocheja, A., & Okuneye, B. A. (2024). Emotional and financial costs of online dating scam: A phenomenological narrative of the experiences of victims of Nigerian romance fraudsters. *Journal of Economic Criminology, 3*, 100044. https://doi.org/10.1016/j.jeconc.2023.100044

AIS Aunjai Cyber. (2024). *A compilation of 22 scams used by fraudsters to deceive victims online, along with ways to handle them*. Retrieved from https://sustainability.ais.co.th/th/update/aunjai-cyber/795/ (in Thai)

Anesa, P. (2020). Lovextortion: Persuasion strategies in romance cybercrime. *Discourse, Context & Media, 35*, 100398. https://doi.org/10.1016/j.dcm.2020.100398

Bank of Thailand. (2023). *Gathering criminals: Global online financial threats*. Retrieved from https://www.bot.or.th/th/ research-and-publications/articles-and-publications/bot-magazine/Phrasiam-66-3/globaltrend_financialfraud.html (in Thai)

Boonmee, S. (2023). The threat of call center gangs evolving from economic crime to cybercrime. *EAU Heritage Journal Science and Technology, 17*(2), 19-26. Retrieved from https://he01.tci-thaijo.org/index.php/EAUHJSci/article/view/261423/178478 (in Thai)

Boonmee, S., & Chavanich, S. (2021). Ransomware from individual threats to corporate disasters. *EAU Heritage Journal Science and Technology, 15*(1), 1–10. Retrieved from https://he01.tci-thaijo.org/index.php/EAUHJSci/article/view/245408/168485 (in Thai)

Drew, J. M., & Webster, J. (2024). The victimology of online fraud: A focus on romance fraud victimisation. *Journal of Economic Criminology, 3*, 100053. https://doi.org/10.1016/j.jeconc.2024.100053

Immigration Bureau. (2024). *18 scams used by fraudsters to deceive victims online*. Retrieved from https://www.immigration.go.th/?avada_portfolio=18-กลโกงมิจฉาชีพ-ใช้หลอกล (in Thai)

Krungsri GURU. (2024). *It's time to get back at scammers and protect yourself! With 3 super cool methods*. Retrieved from https://www.krungsri.com/th/plearn-plearn/revenge-criminal-scammer-lost-money. (in Thai)

Matichon Online. (2023). *Revealing one year of online fraud statistics: Complaints surge! 250,000 cases, losing over 32 billion baht*. Retrieved from https://www.matichon.co.th/economy/news_3906313 (in Thai)

Northern Trust. (2024). *Reduce your risk significantly by adopting some basic best practices*. Retrieved from https://www.northerntrust.com/united-states/institute/articles/10-steps-to-reduce-your-risk-of-cyber-fraud

Pokudom, N. (2020). Data privacy in the digital age. *EAU Heritage Journal Science and Technology, 14*(2), 59–69. Retrieved from https://he01.tci-thaijo.org/index.php/EAUHJSci/article/view/240997/166063 (in Thai)

PPTV Online. (2024). *Revisiting the famous "fraud" case! In Thailand, losses amounting to tens of billions - sentences totaling hundreds of years!*. Retrieved from https://www.pptvhd36.com/news/สังคม/234851 (in Thai)

Prachachat Online. (2024). *Revealing online crime report statistics: Thais lost a total of over 59 billion baht*. Retrieved from https://www.prachachat.net/ict/news-1514260 (in Thai)

Radio Station for Safety and Traffic. (2024). *The government reveals online crime report statistics, showing damages exceeding 70 billion baht from 2022 to 2024*. Retrieved from https://today.line.me/th/v2/article/3NW25jv (in Thai)

Royal Thai Police Office. (2024). *Knowledge media database for enhancing immunity against technology-related crimes*. Retrieved from https://24hicarecenter.com/cybervaccinated (in Thai)

Royal Thai Police Office. (2023). *Press release document*. Retrieved from https://pctpr.police.go.th/blog/?p=21 (in Thai)

Sarmart, T., & Lerdtomornsakul, U. (2023). Cyber victimization of the elderly. *Thai Interdisciplinary and Sustainability Review, 12*(2), 1-13. Retrieved from https://so03.tci-thaijo.org/index.php/JIRGS/article/view/268349/180646 (in Thai)

Siam Commercial Bank. (2023). *Siam Commercial Bank launched the website "Game Over Scammers" a hub for content on preventing modern-day fraudsters, along with the "Nong Aeh The Series" to raise financial awareness among Thais*. Retrieved from https://www.scb.co.th/th/about-us/news/nov-2566/fraud-fighter.html (in Thai)

Thaipbs. (2024). *Scammers' trick: Using children to deceive parents into transferring money as "ransom" resulting in millions lost*. Retrieved from https://www.thaipbs.or.th/news/content/ 345203 (in Thai)

Thaipbs. (2021). *Revisiting the case of the hospital - the Permanent Secretary's office has previously been "hacked"*. Retrieved from https://www.thaipbs.or.th/news/content/307681 (in Thai)

Thaipost. (2023). *Summary of online crime statistics: nearly 400,000 cases, losses in the tens of billions, with the highest number of scams involving product sales*. Retrieved from https://www.thaipost.net/criminality-news/510188/ (in Thai)

Thairath Online. (2023). *Thailand ranks 6th in money transfer scams, according to the Bank of Thailand. Statistics show that 1 in 5 people worldwide have fallen victim*. Retrieved from https://thairath.co.th/money/personal_finance/banking_bond/2745867 (in Thai)

The Thai Bankers Association. (2024). *Get to know "mule accounts" the dangerous accounts with extraordinary penalties*. Retrieved from https://www.tba.or.th/ (in Thai)

Tuncharoen, T., & Assawaboonmee, S. (2023). *Call Center Scammer Problems. Journal of Digital Communications, 7(1), 131–150*. Retrieved from https://so04.tci-thaijo.org/index.php/NBTC_Journal/article/view/259898/179645 (in Thai)

Wang, F., & Topalli, V. (2024). The cyber-industrialization of catfishing and romance fraud. *Computers in Human Behavior, 154*, 108133. https://doi.org/10.1016/j.chb.2023.108133

Wingworn, Y. (2023). Preventing cybercrime in communities in order to develop the communities into digital citizens. *Journal of MCU Nakhondhat, 10*(10), 1–11. Retrieved from https://so03.tci-thaijo.org/index.php/JMND/article/view/272687/180403 (in Thai)

Zhu, C., Zhang, C., Wang, R., Tian, J., Hu, R., Zhao, J., Ke, Y., & Liu, N. (2023). Building of safer urban hubs: Insights from a comparative study on cyber telecom scams and early warning design. *Urban Governance, 3*(3), 200-210. https://doi.org/10.1016/j.ugj. 2023.05.004