การศึกษาการเปลี่ยนแปลงการโจมตีด้วยวิศวกรรมสังคมของภัยคุกคามไซเบอร์ กรณีศึกษาการโจมตีแบบฟิชชิง

A Study of Changes in Social Engineering Attacks of Cybersecurity Threats: A Case Study of Phishing Attacks

จิณณ์ฟ้า รักไทยเจริญชีพ[1*] และ ดร.ชนะกัญจน์ ศรีรัตนบัลล์[2]

Jinnpha Rakthaicharoencheep[1*] and Dr. Chanakan Sriratanaban[2]

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อศึกษาการเปลี่ยนแปลงของการโจมตีด้วยวิศวกรรมสังคมของภัยคุกคามไซเบอร์ โดยมุ่งเน้นกรณีศึกษาการโจมตีในรูปแบบฟิชชิง (Phishing) ในประเทศไทย ใช้ระเบียบวิธีวิจัยเชิงคุณภาพผ่านการศึกษาเอกสารและการสัมภาษณ์เชิงลึกกับกลุ่มตัวอย่างประกอบด้วย ผู้เสียหายจากภัยคุกคามไซเบอร์ ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ และเจ้าหน้าที่ตำรวจ ผลการศึกษาพบว่าลักษณะการโจมตีแบบฟิชชิงมีการพัฒนาอย่างต่อเนื่องจากอดีตในปี พ.ศ. 2560 ที่เน้นการส่งอีเมลหลอกลวงแบบหว่านแห (Mass Phishing) ไปสู่การโจมตีที่มีความซับซ้อนสูงในปี พ.ศ. 2567 โดยมีการนำเทคโนโลยีปัญญาประดิษฐ์ (AI) และ Deepfake มาใช้สร้างความสมจริงเพื่อหลอกลวงเฉพาะบุคคล (Spear Phishing) การโจมตีเปลี่ยนจากการมุ่งเน้นเพียงการขโมยข้อมูลส่วนบุคคล ไปสู่การบงการพฤติกรรม (Action Manipulation) เพื่อยึดสิทธิ์ควบคุมอุปกรณ์และโอนย้ายทรัพย์สินโดยตรง ผลการวิจัยชี้ให้เห็นว่าปัจจัยทางจิตวิทยาและการอาศัยความก้าวหน้าของเทคโนโลยีเป็นตัวขับเคลื่อนหลักที่ทำให้การโจมตีประสบความสำเร็จ ข้อเสนอแนะจากการวิจัยคือควรมีการสร้างความตระหนักรู้แก่ประชาชนในรูปแบบร่วมสมัยควบคู่ไปกับการพัฒนามาตรการด้านเทคโนโลยี เช่น ชีวมาตรเชิงพฤติกรรม เพื่อรับมือกับภัยคุกคามที่มีความซับซ้อนในอนาคต

คำสำคัญ: วิศวกรรมสังคม, ฟิชชิง, ภัยคุกคามไซเบอร์, การเปลี่ยนแปลงการโจมตี, ปัญญาประดิษฐ์

Abstract

This research aims to study the changes of social engineering attack patterns in cybersecurity, specifically focusing on phishing in Thailand. The study employs a qualitative research methodology involving documentary research and in-depth interviews with a sample group consisting of cybersecurity victims, cybersecurity experts, and police officers. The findings reveal that phishing attack characteristics have continuously changed from the past in 2017, which primarily focused on mass phishing emails, to highly sophisticated attacks in

[1] หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการจัดการนวัตกรรมดิจิทัลและเทคโนโลยี

[2] หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการจัดการนวัตกรรมดิจิทัลและเทคโนโลยี

* ผู้ประสานงานนิพนธ์ e-mail: jinnpha.p@gmail.com

2024. These modern attacks utilize Artificial Intelligence (AI) and Deepfake technology to create highly realistic scenarios for spear phishing. The objective of these attacks has shifted from merely stealing personal data to action manipulation, aiming to seize control of devices and directly transfer assets. The research indicates that psychological factors and the advancement of technology are the primary drivers of attack success. Recommendations from this study include fostering public awareness through new methods alongside developing technical measures, such as behavioral biometrics, to counter increasingly complex future threats.

Keywords: Social Engineering, Phishing, Cybersecurity Threats, Attack Patterns, Artificial Intelligence

บทนำ

ในยุคปัจจุบันที่เทคโนโลยีดิจิทัลเข้ามามีบทบาทสำคัญในทุกมิติของชีวิตประจำวัน ตั้งแต่การสื่อสารไปจนถึงการทำธุรกรรมทางการเงินที่ซับซ้อน ประเทศไทยได้ก้าวเข้าสู่สังคมดิจิทัลอย่างเต็มรูปแบบ โดยมีประชากรเข้าถึงอินเทอร์เน็ตสูงถึง 63.21 ล้านคน หรือประมาณร้อยละ 88 ของประชากรทั้งหมด อย่างไรก็ตาม ท่ามกลางความสะดวกสบายนี้ กลับพบการแพร่ระบาดของภัยคุกคามไซเบอร์ที่ทวีความรุนแรงและซับซ้อนขึ้นอย่างต่อเนื่อง โดยเฉพาะการโจมตีด้วยวิศวกรรมสังคม (Social Engineering) ซึ่งเป็นรูปแบบการหลอกลวงที่มุ่งเน้นการใช้จิตวิทยาเพื่อฉวยโอกาสจากจุดอ่อนของมนุษย์ เช่น ความไว้วางใจ ความกลัว หรือความไม่รู้เท่าถึงการณ์ มนุษย์จึงยังคงเป็นจุดอ่อนสำคัญที่สุดของระบบความปลอดภัยไซเบอร์ เนื่องจากสามารถถูกโน้มน้าวให้เปิดเผยข้อมูลสำคัญหรือดำเนินการตามที่ผู้โจมตีต้องการได้ง่ายกว่าการเจาะระบบทางเทคโนโลยีเพียงอย่างเดียว

สำหรับสถานการณ์ปัจจุบันในปี พ.ศ. 2567 ภัยคุกคามในรูปแบบฟิชชิง (Phishing) ได้การเปลี่ยนแปลงไปสู่จุดที่น่ากังวลอย่างยิ่ง โดยประเทศไทยมีสถิติการโจมตีฟิชชิงทางการเงินสูงที่สุดในภูมิภาคเอเชียตะวันออกเฉียงใต้ และมีอัตราการเพิ่มขึ้นจากปีที่ผ่านมาสูงถึงร้อยละ 582 รูปแบบการโจมตีได้เปลี่ยนผ่านจากยุคการส่งอีเมลหรือข้อความสั้น (SMS) แบบหว่านแหในอดีต เข้าสู่ยุคของการใช้ปัญญาประดิษฐ์ (AI-powered Phishing) และการสร้างความจริงจำลอง (Synthetic Reality) ผู้โจมตีไซเบอร์สามารถใช้เทคโนโลยี Deepfake เพื่อปลอมแปลงใบหน้าและเสียงขณะวิดีโอคอลสดเพื่อยืนยันตัวตนปลอมเป็นเจ้าหน้าที่รัฐหรือบุคคลใกล้ชิด ซึ่งเป็นการกดดันทางจิตวิทยาขั้นสูงสุดจนผู้เสียหายสิ้นสงสัย

นอกจากนี้ วัตถุประสงค์ของการโจมตีในปัจจุบันไม่ได้จำกัดอยู่เพียงการขโมยข้อมูลส่วนบุคคล แต่ได้พัฒนาไปสู่การบงการพฤติกรรม (Action Manipulation) โดยตรง ผู้โจมตีมักล่อลวงให้ผู้เสียหายติดตั้งแอปพลิเคชันอันตรายเพื่อขอสิทธิ์การเข้าถึงระบบในระดับราก (Accessibility Service) อันนำไปสู่การควบคุมอุปกรณ์จากระยะไกล (Remote Access) และการโอนย้ายทรัพย์สินออกไปในขณะที่ผู้เสียหายยังถือโทรศัพท์อยู่ การทำงานของผู้โจมตีได้ยกระดับสู่รูปแบบขบวนการองค์กรที่มีการประสานงานหลายช่องทาง (Omnichannel) อย่างเป็นระบบ

ทบทวนวรรณกรรมและทฤษฎีที่เกี่ยวข้อง

แนวคิดวิศวกรรมสังคมและจิตวิทยาพฤติกรรม วิศวกรรมสังคมคือศิลปะการหลอกลวงที่มุ่งเน้นการใช้จิตวิทยาเพื่อให้ได้มาซึ่งข้อมูลหรือการเข้าถึงระบบ โดยอาศัยหลักการชักจูงของ Robert B. Cialdini เช่น การใช้อำนาจ (Authority) และความเร่งด่วน (Urgency) เพื่อกระตุ้นให้ผู้เสียหายตอบสนองอย่างรวดเร็วโดยขาดการยับยั้งชั่งใจ มนุษย์จึงถูกมองว่าเป็นจุดอ่อนที่สำคัญที่สุดในระบบความปลอดภัย เนื่องจากสามารถถูกหลอกลวงได้ง่ายกว่าการเจาะช่องโหว่ทางเทคนิค

รูปแบบและประเภทของการโจมตีฟิชชิง ฟิชชิงมีการพัฒนาไปหลายรูปแบบ ตั้งแต่อีเมลหว่านแหพื้นฐาน ไปจนถึงเทคนิคขั้นสูงอย่าง Spear Phishing ที่มุ่งเป้าบุคคลเฉพาะราย และ Vishing ที่ใช้การโทรศัพท์แอบอ้างเป็นเจ้าหน้าที่ นอกจากนี้ยังมีแนวคิดเรื่อง Nudge ที่ถูกนำมาใช้ในเชิงลบเพื่อปรับเปลี่ยนบริบทสถานการณ์ให้เป้าหมายดำเนินการตามที่ผู้โจมตีต้องการโดยไม่ตั้งคำถาม ปัจจุบันยังพบเทคนิคการโจมตีร่วมสมัย เช่น การใช้ Deepfake ปลอมแปลงใบหน้าและเสียงเพื่อสร้างความน่าเชื่อถือระดับสูง

งานวิจัยที่เกี่ยวข้องและบริบทการป้องกัน จากการศึกษางานวิจัยในอดีต พบว่าผู้โจมตีในประเทศไทยมีความซับซ้อนทั้งในมิติของกฎหมายและพฤติกรรม งานวิจัยของจิตราภรณ์ (2565) และเพชรกล้า (2564) ชี้ให้เห็นถึงความสำคัญของการใช้ เขตอำนาจตามหลักป้องกัน และการปรับปรุงกฎหมายให้รองรับการตรวจสอบหลักฐานดิจิทัลแบบเรียลไทม์ ในขณะที่งานวิจัยด้านพฤติกรรมระบุว่า ประสบการณ์และการตระหนักรู้มีบทบาทสำคัญต่อความปลอดภัย โดยผู้ที่มีความเข้าใจในกลไกทางจิตวิทยาของผู้โจมตีจะมีแนวโน้มในการป้องกันตนเองได้ดีกว่า สอดคล้องกับแนวคิดของ Schneier ที่ว่าความปลอดภัยต้องบูรณาการทั้งบุคลากร กระบวนการ และเทคโนโลยี เข้าด้วยกัน

วัตถุประสงค์

1. การศึกษาการเปลี่ยนแปลงการโจมตีด้วยวิศวกรรมสังคมของภัยคุกคามไซเบอร์ กรณีศึกษาการโจมตีแบบฟิชชิงตั้งแต่พ.ศ. 2560 ถึง พ.ศ. 2567

ขอบเขตการวิจัย

1. ขอบเขตด้านเนื้อหา การวิจัยครั้งเป็นการวิจัยเชิงคุณภาพ (Qualitative Research) ด้วยรูปแบบการที่ประกอบไปด้วยการวิจัยเอกสาร (Documentary Research) และใช้การสัมภาษณ์เชิงลึก (In-depth Interview) เป็นเครื่องมือหลักในการเก็บข้อมูลจากกลุ่ม

ตัวอย่างและผู้เชี่ยวชาญที่เกี่ยวข้องกับการโจมตีด้วยวิศวกรรมสังคมของภัยคุกคามไซเบอร์ (Social Engineering Attacks)

2. ขอบเขตด้านระยะเวลา การเก็บข้อมูลดำเนินการระหว่างวันที่ 1 สิงหาคม 2567 ถึงวันที่ 29 มกราคม 2568
3. ขอบเขตด้านประชากรและกลุ่มตัวอย่าง
   3.1. กลุ่มผู้ใช้งานอินเทอร์เน็ตในเขตกรุงเทพมหานคร ผู้ใช้งานที่มีอายุ 25 ปีขึ้นไป จำนวน 3 ท่าน ที่มีประสบการณ์จากการโดยโจมตีด้วยวิศกรรมสังคมในกรณีฟิชชิง
   3.2. ผู้เชี่ยวชาญด้าน Cybersecurityผู้เชี่ยวชาญที่มีประสบการณ์ในด้านการรักษาความปลอดภัยทางไซเบอร์ โดยเฉพาะการป้องกันการโจมตีด้วยวิศวกรรมสังคม จำนวน 1 ท่าน
   3.3. เจ้าหน้าที่ตำรวจผู้ดูแลคดีไซเบอร์ เจ้าหน้าที่ตำรวจที่มีประสบการณ์ในคดีฟิชชิงและภัยคุกคามไซเบอร์ที่เกี่ยวข้อง จำนวน 1 ท่าน
4. ขอบเขตด้านพื้นที่ การเก็บข้อมูลจะดำเนินการใน
   4.1. เขตกรุงเทพมหานคร

วิธีดำเนินการวิจัย

การศึกษาวิจัยครั้งนี้เลือกใช้ระเบียบวิธีวิจัยเชิงคุณภาพ (Qualitative Research Methodology) เพื่อให้ได้ข้อเท็จจริงเชิงประจักษ์และข้อมูลเชิงลึก (Empirical & Deep Knowledge) เกี่ยวกับพลวัตและการเปลี่ยนแปลงรูปแบบการโจมตีด้วยวิศวกรรมสังคมของภัยคุกคามไซเบอร์ กรณีศึกษาการโจมตีแบบฟิชชิง โดยผู้วิจัยได้วางโครงสร้างขั้นตอนการดำเนินงานอย่างเป็นระบบ ดังนี้

1. การกำหนดประชากรและการคัดเลือกผู้ให้ข้อมูลสำคัญ (Key Informants) ผู้วิจัยใช้วิธีการเลือกกลุ่มตัวอย่างแบบเจาะจง (Purposive Sampling) ในการคัดเลือกผู้ให้ข้อมูลสำคัญรวมทั้งสิ้นจำนวน 5 ราย โดยมีการออกแบบสัดส่วนและเกณฑ์คุณสมบัติของประชากร ดังนี้

1.1 กลุ่มผู้เสียหายจากภัยคุกคามไซเบอร์ (สัดส่วนร้อยละ 60 ของผู้ให้ข้อมูลทั้งหมด) ได้แก่ ผู้ใช้งานอินเทอร์เน็ตในเขตกรุงเทพมหานครที่มีอายุตั้งแต่ 25 ปีขึ้นไป และมีประสบการณ์ตรงในการตกเป็นผู้เสียหายพฤติการณ์คดีโจมตีฟิชชิงในช่วงปี พ.ศ. 2560 หรือ พ.ศ. 2567 จำนวน 3 ท่าน เพื่อสะท้อนพฤติกรรมการตอบสนองและกลยุทธ์ทางจิตวิทยาที่เกิดขึ้นจริงเชิงประจักษ์

1.2 กลุ่มผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ (สัดส่วนร้อยละ 20 ของผู้ให้ข้อมูลทั้งหมด) ได้แก่ ผู้เชี่ยวชาญที่มีคุณวุฒิและประสบการณ์ตรงในมิติด้านวิทยาการเทคโนโลยีและการรักษาความปลอดภัยทางไซเบอร์ โดยเฉพาะกลไกการป้องกันวิศวกรรมสังคม จำนวน 1 ท่าน เพื่อให้ข้อมูลเชิงเทคนิคเกี่ยวกับมัลแวร์และนวัตกรรมการโจมตีที่ผ่านมา

1.3 กลุ่มเจ้าหน้าที่บังคับใช้กฎหมาย (สัดส่วนร้อยละ 20 ของผู้ให้ข้อมูลทั้งหมด) ได้แก่ เจ้าหน้าที่ตำรวจผู้ดูแลคดีอาชญากรรมทางเทคโนโลยีที่มีประสบการณ์ตรงในการสืบสวนสอบสวนคดีฟิชชิงและภัยคุกคามไซเบอร์ที่เกี่ยวข้อง จำนวน 1 ท่าน เพื่อระบุข้อเท็จจริงเกี่ยวกับโครงสร้างขบวนการอาชญากรรมและช่องขยายผลเชิงนโยบาย

2. เครื่องมือที่ใช้ในการวิจัย เครื่องมือหลักที่ใช้ในการวิจัยแบ่งออกเป็น (1) แบบบันทึกข้อมูลสำหรับการวิจัยเชิงเอกสาร และ (2) แนวคำถามสำหรับการสัมภาษณ์เชิงลึกแบบกึ่งโครงสร้าง (Semi-structured Interview) โดยผู้วิจัยได้ออกแบบชุดคำถามเพื่อเก็บข้อมูลเชิงคุณภาพที่มุ่งเน้นการวิเคราะห์เปรียบเทียบพลวัตความเปลี่ยนแปลงใน 8 ส่วนสำคัญ ได้แก่ กระบวนการโจมตี กลยุทธ์ เทคนิค การใช้จิตวิทยา ลักษณะการหลอกล่อ ข้อมูลที่ถูกเปิดเผย และเทคโนโลยีที่ใช้ในการโจมตีระหว่างอดีตและปัจจุบัน

3. การเก็บรวบรวมข้อมูล ผู้วิจัยดำเนินการเก็บรวบรวมข้อมูลดิบขนานกันผ่าน 2 ช่องทางหลัก ประกอบด้วย การวิจัยเชิงเอกสาร (Documentary Research) จากฐานข้อมูลวารสารวิชาการ สถิติคดีไซเบอร์ และคู่มือระเบียบข้อบังคับที่เกี่ยวข้อง ควบคู่ไปกับการลงพื้นที่สัมภาษณ์เชิงลึก (In-depth Interview) กับผู้ให้ข้อมูลสำคัญทั้ง 5 ราย โดยทำการบันทึกเสียงและจดบันทึกรายละเอียดอนุทินแบบคำต่อคำ (Verbatim) เพื่อรักษารายละเอียดเนื้อหาและคำสัมภาษณ์ (Direct Quote) ของผู้ให้ข้อมูลแต่ละตำแหน่งไว้ใช้ในการอภิปรายผลผลการศึกษา

4. การวิเคราะห์ข้อมูล ผู้วิจัยใช้เทคนิคการวิเคราะห์เชิงเนื้อหา (Content Analysis) โดยนำข้อมูลที่ได้จากการถอดเทปสัมภาษณ์เชิงลึกและการศึกษาเอกสารมาทำการประมวลผล จำแนกหมวดหมู่ และลงรหัส (Coding) ตามวัตถุประสงค์การวิจัย นอกจากนี้ ผู้วิจัยยังได้ประยุกต์ใช้เทคนิคการตรวจสอบข้อมูลแบบสามเส้า (Data Triangulation) ทั้งในมิติด้านข้อมูล (แหล่งที่มาจากกลุ่มบุคคลที่ต่างกัน) และมิติด้านวิธีรวบรวมข้อมูล เพื่อพิสูจน์ความถูกต้องและความน่าเชื่อถือขององค์ความรู้เชิงประจักษ์ที่ค้นพบ

5. การนำเสนอผลการศึกษา ข้อมูลผลการศึกษาที่ผ่านการสังเคราะห์ระบบนิเวศการโจมตีจะถูกนำเสนอในรูปแบบความเรียงเชิงวิเคราะห์ (Analytical Descriptive) ควบคู่กับการจัดทำตารางเปรียบเทียบผลการวิจัยเชิงลึก เพื่อแสดงให้เห็นภาพพจน์และพลวัตความแตกต่างของการเปลี่ยนแปลงรูปแบบการโจมตีระหว่างปี พ.ศ. 2560 และ พ.ศ. 2567 อย่างชัดเจนเป็นรูปธรรม

ผลการวิจัย

จากการศึกษาการเปลี่ยนแปลงการโจมตีด้วยวิศวกรรมสังคมของภัยคุกคามไซเบอร์ กรณีศึกษาการโจมตีแบบฟิชชิง พบว่าในช่วงปี พ.ศ. 2560 ถึง พ.ศ. 2567 รูปแบบการหลอกลวงได้เปลี่ยนแปลงจากการโจมตีเชิงปริมาณที่ความซับซ้อนต่ำ (Mass & Low Credibility) ไปสู่การโจมตีเชิงคุณภาพที่มีความแนบเนียนสูง (Targeted & High Credibility) โดยมีตารางเปรียบเทียบรายละเอียดการเปลี่ยนแปลงที่สำคัญในด้านรูปแบบการโจมตี ดังนี้

ตารางที่ 1 สรุปเปรียบเทียบการเปลี่ยนแปลงรูปแบบการโจมตีฟิชชิงตามกรอบแนวคิดการวิจัย

รูปแบบการโจมตี	ลักษณะในปี พ.ศ. 2560 (Manual Era)	ลักษณะในปี พ.ศ. 2567 (Synthetic Era)
1. อีเมลฟิชชิงพื้นฐาน (Basic Email Phishing)	เน้นการส่งแบบสุ่มในปริมาณมาก (Mass Spam) โดยใช้ภาษาที่ไม่เป็นธรรมชาติ และมุ่งเน้นการจารกรรมรหัสผ่านเข้าใช้งานเป็นหลัก	พัฒนาสู่การโจมตีแบบเจาะจง (Spear Phishing) โดยใช้ปัญญาประดิษฐ์สร้างเนื้อหาเฉพาะบุคคล และแทรกซึมเข้าสู่บทสนทนาจริง (Thread Hijacking) เพื่อสร้างความน่าเชื่อถือ
2. การโจมตีผ่าน SMS (Smishing)	ส่งข้อความแจ้งสิทธิประโยชน์หรือรางวัลปลอมพร้อมลิงก์ย่อ เพื่อนำทางไปสู่การกรอกข้อมูลบนหน้าเว็บไซต์ปลอม	ใช้อุปกรณ์ฮาร์ดแวร์ส่งสัญญาณปลอม (Stingray) เข้าถึงเป้าหมายโดยตรง และดึงผู้เสียหายเข้าสู่แอปพลิเคชันสนทนาเพื่อโน้มน้าวแบบเรียลไทม์
3. การใช้สื่อสังเคราะห์และปัญญาประดิษฐ์ (Deepfake & AI)	เทคโนโลยียังอยู่ในวงจำกัด พึ่งพาการตัดต่อภาพนิ่ง (Manual Editing) เพื่อสร้างหลักฐานปลอมประกอบการหลอกลวงเท่านั้น	ใช้เทคโนโลยี Live Deepfake สังเคราะห์ใบหน้าและเสียงขณะวิดีโอคอลสด เพื่อยืนยันตัวตนเจ้าหน้าที่หรือบุคคลใกล้ชิดและทำลายความสงสัย
4. การโจมตีผ่าน Mobile Banking	สร้างแอปพลิเคชันปลอมนอก Store มาตรฐาน หรือใช้มัลแวร์ Overlay เพื่อดักจับรหัส PIN และรหัสผ่านชั่วคราว (OTP)	หลอกล่อให้ติดตั้งแอปพลิเคชันอันตรายและยินยอมสิทธิ์การเข้าถึงระบบ (Accessibility Service) เพื่อเข้าควบคุมอุปกรณ์ระยะไกล (RAT) และโอนเงินออกโดยตรง
5. การโจมตีแบบสอดประสานหลายช่องทาง (Multi-channel)	การโจมตีมีลักษณะแยกส่วนเป็นเอกเทศ (Siloed) มักเป็นกระบวนการเส้นตรงซึ่งหากไม่สำเร็จในช่องทางหนึ่งจะยุติการโจมตีทันที	ทำงานเป็นขบวนการอาชญากรรม (Syndicate) ที่ประสานงานข้ามแพลตฟอร์ม โดยมีการแชร์ข้อมูลผู้เสียหายระหว่างทีมแบบเรียลไทม์เพื่อให้เรื่องราวสอดคล้องกัน

6. การใช้ข้อมูลส่วนบุคคลที่รั่วไหล (Data Leakage)	นำฐานข้อมูลดิบมาใช้ส่งสแปมเพื่อสุ่มหาเป้าหมายในวงกว้าง โดยขาดการนำข้อมูลมาสร้างบริบทหลอกลวงรายบุคคล	ใช้เทคนิคการเติมเต็มข้อมูลอัจฉริยะ (Data Enrichment) วิเคราะห์ประวัติและพฤติกรรมเพื่อสร้างสถานการณ์หลอกลวงที่สมจริงและเฉพาะเจาะจงรายบุคคล

ที่มา : จิณณ์ฟ้า รักไทยเจริญชีพ (2568)

จากผลการศึกษาวิจัยเชิงประจักษ์ในตารางที่ 1 ผู้วิจัยได้นำข้อมูลดิบจากการสืบค้นเอกสารและข้อมูลที่ได้จากการถอดบทสัมภาษณ์เชิงลึกแบบคำต่อคำ (Verbatim Transcription) จากกลุ่มผู้ให้ข้อมูลสำคัญ (Key Informants) ทั้ง 3 กลุ่ม มาทำการวิเคราะห์เชิงเนื้อหา (Content Analysis) เพื่อจำแนกและอธิบายพลวัตการเปลี่ยนแปลงรูปแบบพฤติการณ์โจมตีร่วมกับการร้อยเรียงคำอธิบายศัพท์เทคนิคเชิงปฏิบัติการให้กลืนไปกับเนื้อหาบรรยายเชิงลึก ดังนี้

1. พลวัตการเปลี่ยนแปลงเชิงโครงสร้างของรูปแบบการส่งและการหลอกล่อผ่านสื่อสังคม จากการศึกษาวิเคราะห์ข้อมูลพฤติการณ์คดี พบว่าระบบนิเวศการหลอกลวงได้แปรเปลี่ยนจาก "การโจมตีเชิงปริมาณที่ความซับซ้อนต่ำ (Mass & Low Credibility) ในยุคปี พ.ศ. 2560 ไปสู่การโจมตีเชิงคุณภาพที่มีความแนบเนียนสูง (Targeted & High Credibility) ในยุคปี พ.ศ. 2567 อย่างเป็นรูปธรรม ในอดีตนั้นผู้โจมตีจะพึ่งพาการส่งอีเมลฟิชชิงพื้นฐาน (Basic Email Phishing) โดยเป็นการหว่านแหในปริมาณมาก (Mass Spam) เพื่อสุ่มหาเป้าหมาย สัญญาณเตือนภัย (Red Flags) ที่เด่นชัดในยุคนั้นคือการสะกดคำผิดและการใช้รูปประโยคที่ไม่เป็นธรรมชาติเนื่องจากพึ่งพาโปรแกรมแปลภาษาแบบหยาบ ๆ และมีวัตถุประสงค์เพียงเพื่อล่อลวงให้ผู้เสียหายคลิกดาวน์โหลดไฟล์แนบอันตรายหรือกรอกรหัสผ่าน (Credentials) บนหน้าเว็บไซต์ปลอม (Phishing Landing Page) ที่ทำเลียนแบบสถาบันการเงิน ว่าในยุคปัจจุบัน พฤติการณ์ดังกล่าวได้ถูกยกระดับขึ้นโดยอาศัยกระบวนการเติมเต็มข้อมูลอัจฉริยะ (Data Enrichment) นำฐานข้อมูลที่รั่วไหล (Data Leakage) จากแพลตฟอร์มต่าง ๆ มาทำการวิเคราะห์ร่วมกับการสืบค้นข้อมูลจากแหล่งเปิด (Open Source Intelligence: OSINT) เพื่อศึกษาประวัติ พฤติกรรม และความสัมพันธ์ของผู้เสียหายรายบุคคล นำไปสู่การโจมตีแบบเจาะจงกลุ่มเป้าหมาย (Spear Phishing) ที่มีความแม่นยำสูง สอดคล้องกับข้อมูลเชิงลึกจากผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Expert) ที่ได้อธิบายกลไกเทคนิคขั้นสูงว่า ผู้โจมตีไม่ได้ส่งอีเมลอีกต่อไป แต่ใช้เทคนิคที่เรียกว่า เทรด ไฮแจ็กกิง (Thread Hijacking) คือการใช้มัลแวร์เข้าไปแฮกบัญชีอีเมลของคู่ค้าหรือบุคคลที่ผู้เสียหายติดต่ออยู่จริง จากนั้นระบบปัญญาประดิษฐ์ (AI) จะวิเคราะห์ประวัติการคุยเพื่อสวมรอยส่งอีเมลแทรกซึมเข้าไปในกล่องข้อความสนทนาเดิม (Reply-to Chain) พร้อมแนบลิงก์หรือใบแจ้งหนี้ปลอม ทำให้ผู้เสียหายแยกแยะได้ยากมากเพราะเป็นคู่สนทนาที่ไว้ใจและเป็นเรื่องที่คุยค้างกันไว้จริง

2. พลวัตการเปลี่ยนผ่านทางนวัตกรรมเทคโนโลยีและการใช้สื่อสังเคราะห์ ในส่วนของการโจมตีผ่านเครือข่ายโทรศัพท์เคลื่อนที่ พลวัตความเปลี่ยนแปลงได้ฉายภาพชัดจากการส่งข้อความสั้นหลอกลวงหรือสมิชชิง (Smishing) ในปี พ.ศ. 2560 ที่ส่งผ่านช่องทาง SMS Gateway ปกติ ไปสู่การใช้นวัตกรรมฮาร์ดแวร์ขั้นสูงในปี พ.ศ. 2567 สอดคล้องกับบทสัมภาษณ์ของเจ้าหน้าที่ตำรวจผู้ดูแลคดีไซเบอร์ ระดับสารวัตร กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) ที่ระบุว่าปัจจุบันเครือข่ายคอลเซ็นเตอร์มีการใช้เครื่องสติงเรย์ (Stingray) หรืออุปกรณ์จำลองเสาสัญญาณปลอม (False Base Station) ใส่ไว้ในรถยนต์แล้วขับเคลื่อนที่ไปตามชุมชนหนาแน่น อุปกรณ์นี้จะส่งคลื่นความถี่วิทยุแรงสูงไปบังคับให้โทรศัพท์มือถือในรัศมีตัดขาดจากเสาสัญญาณจริงของเครือข่าย แล้วมาจับสัญญาณปลอมแทน ผู้โจมตีจึงสามารถยิงข้อความ SMS หลอกลวงเข้าสู่มือถือของผู้เสียหายได้โดยตรงโดยไม่ผ่านระบบคัดกรองของผู้ให้บริการเครือข่าย และที่น่ากลัวคือสามารถตั้งชื่อผู้ส่ง (Sender Name) ให้ปลอมเป็นชื่อธนาคารหรือหน่วยงานรัฐ ส่งผลให้ข้อความปลอมนั้นเข้าไปแทรกอยู่ในกล่องข้อความจริงของธนาคารที่ผู้เสียหายเคยได้รับ สร้างความน่าเชื่อถือในระดับสูงสุด เมื่อผู้เสียหายหลงเชื่อกดลิงก์จาก SMS หรือช่องทางอื่น ขบวนการอาชญากรรมจะเปลี่ยนผ่านช่องทางการสื่อสารไปสู่แอปพลิเคชันสนทนา (เช่น Line) และก้าวเข้าสู่ยุคความจริงจำลองด้วยสื่อสังเคราะห์ (Synthetic Reality) ซึ่งแตกต่างจากปี พ.ศ. 2560 ที่ทำได้เพียงการตัดต่อเอกสารหรือภาพนิ่งทำมือ (Manual Editing) โดยในปัจจุบันผู้โจมตีได้นำเทคโนโลยี ไลฟ์ ดีปเฟก (Live Deepfake) และการจำลองเสียงด้วยปัญญาประดิษฐ์ (AI Voice Cloning) มาใช้งานร่วมกับการวิจัยเชิงปริมาณทางจิตวิทยาเพื่อทำลายความสงสัย สอดคล้องกับคำให้การของผู้เสียหายจากภัยคุกคามไซเบอร์ (กรณีศึกษาผู้เสียหายแอปพลิเคชันดูดเงิน พ.ศ. 2567) ที่สะท้อนว่า “ตอนแรกที่ผู้โจมตีอ้างตัวเป็นเจ้าหน้าที่ตำรวจโทรมาเรายังไม่เชื่อ แต่พอเขาขอเปิดวิดีโอคอล ภาพที่ปรากฏคือเจ้าหน้าที่ตำรวจแต่งเครื่องแบบเต็มยศนั่งอยู่ในสถานีตำรวจ ขยับปากพูดคุยตอบโต้กับเราได้แบบเรียลไทม์ มีการเรียกชื่อ-นามสกุล และข่มขู่เรื่องคดีความฟอกเงินอย่างกดดัน เทคโนโลยี Live Deepfake ตัวนี้แนบเนียนมากจนทำให้เราเกิดความกลัวอย่างสุดขีดและยอมทำตามข้อสั่งการทุกอย่างโดยไม่มีข้อโต้แย้ง

3. พลวัตการเปลี่ยนผ่านวัตถุประสงค์เชิงกลยุทธ์จากการจารกรรมข้อมูลสู่การบงการพฤติกรรม ผลการวิจัยชี้ให้เห็นถึงจุดเปลี่ยนผ่านที่สำคัญที่สุด (Paradigm Shift) ในมิติของวัตถุประสงค์และผลลัพธ์ของการโจมตี โดยแปรเปลี่ยนจากการมุ่งจารกรรมข้อมูลอัตลักษณ์ส่วนบุคคล ไปสู่กระบวนการบงการพฤติกรรมเพื่อเข้าควบคุมอุปกรณ์จากระยะไกล (Action Manipulation) ในอดีตช่วงปี พ.ศ. 2560 หากผู้โจมตีต้องการกระทำการอุบายผ่านระบบโมบายแบงกิ้ง (Mobile Banking) มักจะใช้วิธีพัฒนาแอปพลิเคชันปลอมนอกตลาดแอปพลิเคชันมาตรฐาน (Store) หรือประยุกต์ใช้เทคนิคการซ้อนทับหน้าต่างอินเทอร์เฟซ (Overlay Attack) ซึ่งเป็นการฝังมัลแวร์ลงในอุปกรณ์ของผู้เสียหายเพื่อดักจับจังหวะการเข้าใช้งานแอปพลิเคชันธนาคารพาณิชย์จริง จากนั้นจะส่งหน้าต่างอินเทอร์เฟซปลอมขึ้นมาแสดงผลซ้อนทับเพื่อล่อลวงให้ผู้เสียหายกรอกรหัส PIN หรือรหัสผ่านชั่วคราว (One-Time Password: OTP) อันนำไปสู่การจารกรรมข้อมูลเพื่อนำไปเข้าสู่ระบบในอุปกรณ์ของผู้โจมตีเอง ทว่าพฤติการณ์คดีในปี พ.ศ. 2567 ได้วิวัฒน์ไปสู่การหลอกล่อให้ผู้เสียหายติดตั้งไฟล์

ชุดคำสั่งประเภท .APK ซึ่งภายในมีการฝังมัลแวร์ควบคุมระยะไกลประเภทโทรจัน (Remote Access Trojan: RAT) หลังจากนั้นผู้โจมตีจะประยุกต์ใช้กลวิธีทางจิตวิทยาเพื่อบงการพฤติกรรม (Action Manipulation) ให้ผู้เสียหายทำการกดอนุมัติสิทธิ์และยินยอมให้แอปพลิเคชันเข้าถึงระบบในระดับรากขั้นสูงสุด หรือที่เรียกว่าการก้าวล่วงสิทธิ์บริการช่วยเหลือการเข้าถึงระบบ (Accessibility Service Abuse) ข้อมูลจากการถอดบทสัมภาษณ์เชิงลึกของกลุ่มผู้ให้ข้อมูลสำคัญในกลุ่มผู้เสียหาย ได้ระบุพฤติการณ์เชิงประจักษ์ในขั้นตอนนี้ไว้ว่าหลังจากถูกหลอกล่อให้กดเปิดสิทธิ์ Accessibility Service หน้าจอโทรศัพท์เคลื่อนที่จะเกิดอาการตอบสนองช้าหรือแสดงผลหน้าจอสีดำพร้อมข้อความจำลองว่ากำลังอยู่ในกระบวนการอัปเดตระบบ ในจังหวะนั้นมัลแวร์ RAT จะเริ่มปฏิบัติการร่วมกับฟังก์ชันการสะท้อนหน้าจอ (Screen Mirroring หรือ Screen Casting) ส่งผลให้ผู้โจมตีสามารถมองเห็นทุกพลวัตความเคลื่อนไหวบนหน้าจอโทรศัพท์เคลื่อนที่จากระยะไกล และสามารถสั่งการเชิงปฏิบัติการแทนเจ้าของเครื่อง ตรวจดักรหัสผ่านในขณะสแกนลายนิ้วมือหรือกดรหัส PIN และกระทำการโอนย้ายสินทรัพย์ออกจากบัญชีผ่านแอปพลิเคชันธนาคารไปยังบัญชีม้า (Mule Account) หลากหลายทอดในลักษณะเรียลไทม์ โดยที่ระบบตรวจจับความผิดปกติของสถาบันการเงินไม่แจ้งเตือน เนื่องจากพฤติกรรมการโอนเงินดังกล่าวเกิดขึ้นจากตัวอุปกรณ์และหมายเลขที่อยู่ไอพี (IP Address) ประจำเครื่องของผู้เสียหายเองโดยตรง

บทวิเคราะห์เชิงคุณภาพข้างต้นสะท้อนให้เห็นว่า โครงสร้างและระบบนิเวศของการโจมตีด้วยวิศวกรรมสังคม (Social Engineering Ecosystem) ในปัจจุบัน ไม่ได้จำกัดอยู่เพียงปัญหาทางเทคนิคหรือความบกพร่องส่วนบุคคลอีกต่อไป หากแต่เป็นกระบวนการอาชญากรรมทางปัญญา (Cognitive Warfare) ที่มีการแลกเปลี่ยนและเติมเต็มข้อมูลข้ามแพลตฟอร์มแบบเรียลไทม์ และประสานงานร่วมกันเป็นขบวนการอาชญากรรมข้ามชาติ (Cyber Syndicate) ที่มีประสิทธิภาพสูง การค้นพบข้อเท็จจริงเชิงประจักษ์ (Empirical Knowledge) เหล่านี้ จะเป็นฐานรากสำคัญในการนำไปสู่การอภิปรายผลเชิงทฤษฎีเพื่อออกแบบแนวทางการป้องกันและกำหนดนโยบายความมั่นคงปลอดภัยไซเบอร์ที่ยั่งยืนต่อไป

ประโยชน์ที่ได้รับ

การศึกษาวิจัยเรื่อง การเปลี่ยนแปลงการโจมตีฟิชชิงด้วยวิศวกรรมสังคม การปรับเปลี่ยนกลยุทธ์และผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ ไม่เพียงแต่เป็นการสำรวจสถานการณ์ภัยคุกคามที่เกิดขึ้น แต่ยังก่อให้เกิดประโยชน์เชิงประจักษ์ในหลายมิติ ดังนี้

ในด้านวิชาการ งานวิจัยฉบับนี้ได้นำเสนอองค์ความรู้ในมุมมองที่ผ่านมา แบบจำลองการเปลี่ยนแปลงการโจมตีฟิชชิงด้วยวิศวกรรมสังคม ซึ่งถือเป็นการสร้างกรอบแนวคิดที่ช่วยอธิบายพลวัตของภัยคุกคามไซเบอร์ในช่วงปี พ.ศ. 2560–2567 ได้อย่างเป็นระบบ การค้นพบการเปลี่ยนผ่านจากยุคการหลอกถามข้อมูล (Manual Era) สู่ยุคการบงการสมบูรณ์ด้วย AI (Synthetic Era) ช่วยเติมเต็มช่องว่างทางทฤษฎีความมั่นคง

ปลอดภัยไซเบอร์แบบเดิม ให้ครอบคลุมถึงเทคโนโลยีสื่อสังเคราะห์ (Deepfake) และการใช้มัลแวร์ควบคุมระยะไกล (RAT) ซึ่งเป็นประเด็นที่ทฤษฎีดั้งเดิมยังให้ความสำคัญไม่เพียงพอ

ในมิติด้านนโยบายและการปฏิบัติ ผลจากการศึกษาสามารถนำไปประยุกต์ใช้เป็นฐานข้อมูลสำคัญสำหรับหน่วยงานภาครัฐและสถาบันการเงินในการยกระดับกลยุทธ์การป้องกันเชิงรุก (Proactive Defense) โดยเปลี่ยนจุดเน้นจากการป้องกันเชิงระบบพื้นฐาน ไปสู่การเฝ้าระวังที่จุดปลายทาง (Endpoint Security) และการพัฒนาระบบตรวจจับพฤติกรรมผิดปกติ (Behavioral Detection) เพื่อตัดวงจรการเข้าควบคุมอุปกรณ์ของผู้เสียหายก่อนที่จะเกิดความเสียหายทางการเงินในมูลค่าสูง

สำหรับประโยชน์ต่อสังคมและประชาชน งานวิจัยนี้ทำหน้าที่เป็นเครื่องมือในการสร้างภูมิคุ้มกันทางดิจิทัล (Digital Immunity) ผ่านการให้ข้อมูลที่ทันต่อเหตุการณ์ ทำให้ประชาชนตระหนักว่าสื่อในรูปแบบภาพและเสียงอาจถูกสังเคราะห์ขึ้นมาเพื่อการหลอกลวงได้ และการสูญเสียทรัพย์สินในปัจจุบันอาจเกิดขึ้นโดยที่ผู้เสียหายไม่ได้เปิดเผยรหัสผ่าน ความเข้าใจนี้จะส่งผลต่อการปรับเปลี่ยนพฤติกรรมการใช้งานอินเทอร์เน็ตให้มีความรอบคอบและยึดหลักการตรวจสอบก่อนให้ความเชื่อใจ (Verify then Trust) เพื่อลดโอกาสในการตกเป็นผู้เสียหายของอาชญากรรมไซเบอร์อย่างยั่งยืน

สุดท้ายในด้านการพัฒนาบุคลากร ข้อมูลเชิงลึกที่ได้จากการวิจัยสามารถนำไปบูรณาการเข้ากับหลักสูตรการฝึกอบรมด้านความปลอดภัยไซเบอร์ (Security Awareness Training) ขององค์กรต่างๆ ให้มีความทันสมัย โดยเน้นการจำลองสถานการณ์จริง (Scenario-based) ในรูปแบบต่างๆ เช่น การรับมือกับขบวนการ Call Center ที่ใช้ Deepfake หรือการตรวจสอบความปลอดภัยของแอปพลิเคชันมือถือ ซึ่งจะช่วยเพิ่มศักยภาพของทรัพยากรมนุษย์ในการเผชิญหน้ากับภัยคุกคามในยุคดิจิทัลได้อย่างมีประสิทธิภาพ

สรุปและอภิปรายผล

สรุป

จากการศึกษาวิจัยเชิงคุณภาพและศึกษาการเปลี่ยนแปลงคดีฟิชชิงในช่วงปี พ.ศ. 2560 และ พ.ศ. 2567 ผู้วิจัยพบว่าโครงสร้างและระบบนิเวศของการโจมตีด้วยวิศวกรรมสังคมมีความเปลี่ยนแปลงไปอย่างสิ้นเชิงตามระดับความก้าวหน้าของนวัตกรรมดิจิทัล การวิเคราะห์การเปลี่ยนแปลงดังกล่าวสามารถสรุปออกมาเป็นแบบจำลองเชิงระบบนิเวศ (Ecosystem Model) เพื่อให้เห็นพลวัตความสัมพันธ์ระหว่างผู้โจมตี เครื่องมือ และเป้าหมายได้อย่างชัดเจน

ในระยะแรกของการโจมตีช่วงปี พ.ศ. 2560 ระบบนิเวศมีลักษณะเป็นยุคการโจมตีเชิงปริมาณแบบทำมือ (Manual Era) ซึ่งเป็นกระบวนการที่อาศัยแรงงานมนุษย์และเครื่องมือพื้นฐานในการหว่านแหหาผู้เสียหาย ดังปรากฏรายละเอียดในแบบจำลองลำดับที่ 1

ภาพที่ 1 แบบจำลองการเปลี่ยนแปลงการโจมตีฟิชชิงด้วยวิศวกรรมสังคมลำดับที่ 1

ที่มา: จิณณ์ฟ้า รักไทยเจริญชีพ (2568)

ภาพที่ 2 แบบจำลองการเปลี่ยนแปลงการโจมตีฟิชชิงด้วยวิศวกรรมสังคมลำดับที่ 2

ที่มา: จิณณ์ฟ้า รักไทยเจริญชีพ (2568)

การเปรียบเทียบระหว่างแบบจำลองทั้งสองลำดับนี้ สะท้อนให้เห็นถึงจุดเปลี่ยนสำคัญของการโจมตีในปัจจุบัน ถือเป็นองค์ความรู้ที่ทำให้เห็นมุมมองที่เห็นถึงการเคลื่อนตัวของเป้าหมายปลายทาง จากเดิมที่มุ่งหวังเพียงการจารกรรมข้อมูล (Information Theft) เพื่อนำไปขายต่อหรือเข้าถึงระบบในภายหลัง ได้พัฒนาสู่ การบงการพฤติกรรม (Action Manipulation) เพื่อเข้าควบคุมอุปกรณ์โดยสมบูรณ์ (Device Takeover) การหลอกล่อให้ติดตั้งแอปพลิเคชันอันตรายเพื่อเปิดสิทธิ์การเข้าถึงระบบ (Accessibility Service) ช่วยให้ผู้โจมตีสามารถมองเห็นหน้าจอและสั่งการธุรกรรมทางการเงินแทนผู้เสียหายได้ในทันที

แบบจำลองการเปลี่ยนแปลงการโจมตีฟิชชิงด้วยวิศวกรรมสังคมแสดงให้เห็นถึงภัยคุกคามไซเบอร์ในปัจจุบันได้ก้าวข้ามขอบเขตของการเป็นเพียงการส่งข้อมูลปลอมไปสู่การเป็นการสร้างความจริงปลอมเพื่อบงการมนุษย์ ซึ่งแนวทางป้องกันในอนาคตจึงต้องปรับเปลี่ยนจากการมุ่งเน้นความมั่นคงปลอดภัยเชิงระบบ (System Defense) ไปสู่การสร้างความมั่นคงปลอดภัยเชิงพฤติกรรม (Behavioral Defense) ที่ต้องอาศัยความเท่าทันต่อเทคโนโลยีสื่อสังเคราะห์เหล่านี้อย่างแท้จริง

การศึกษาวิจัยเชิงคุณภาพเรื่องการเปลี่ยนแปลงของการโจมตีด้วยวิศวกรรมสังคมของภัยคุกคามไซเบอร์ กรณีศึกษาการโจมตีแบบฟิชชิง สามารถสรุปผลการศึกษาข้อมูลดิบเชิงประจักษ์ (Empirical Knowledge) ที่สกัดจากฐานข้อมูลเอกสารเชิงระบบร่วมกับบทสัมภาษณ์เชิงลึกของกลุ่มผู้ให้ข้อมูลสำคัญ (Key Informants) จำนวนทั้งสิ้น 5 ราย (สัดส่วนผู้เสียหายร้อยละ 60, ผู้เชี่ยวชาญไซเบอร์ร้อยละ 20, และเจ้าหน้าที่ตำรวจร้อยละ 20) โดยสามารถแบ่งกลุ่มข้อค้นพบตามพลวัตการวิวัฒน์ของระบบนิเวศระหว่างปี พ.ศ. 2560 และ พ.ศ. 2567 ตามกรอบแนวคิดการวิเคราะห์ 8 ส่วนสำคัญ ได้ดังนี้

1. พลวัตด้านกระบวนการโจมตี กลยุทธ์ และเทคนิค

ผลการวิจัยสรุปได้ว่า โครงสร้างเชิงกระบวนการได้ปรับเปลี่ยนจากการโจมตีเชิงปริมาณที่ความซับซ้อนต่ำ (Mass & Low Credibility) ในอดีตปี พ.ศ. 2560 ไปสู่การโจมตีเชิงคุณภาพที่มีความแนบเนียนสูง (Targeted & High Credibility) ในปี พ.ศ. 2567 โดยกลยุทธ์การหว่านแหสุ่มส่งในปริมาณมาก (Mass Spam) ได้ถูกยกระดับไปสู่กระบวนการเจาะจงกลุ่มเป้าหมายส่วนบุคคล (Spear Phishing) ผ่านกลวิธีเชิงลึก เช่น เทคนิคการแทรกซึมสวมรอยเข้าสู่ระบบบทสนทนาทางอีเมลจริง (Thread Hijacking) และการทำงานประสานงานร่วมกันแบบสอดประสานทุกช่องทาง (Omnichannel) ของขบวนการองค์กรอาชญากรรม (Cyber Syndicate) ที่มิใช่การโจมตีทางเทคนิคแบบแยกส่วนเดี่ยว (Siloed) เช่นในอดีต

2. พลวัตด้านการใช้จิตวิทยาและลักษณะการหลอกล่อ

ลักษณะอุบายในการหลอกล่อได้เปลี่ยนผ่านจากการพึ่งพาการสร้างข้อความแจ้งสิทธิประโยชน์หรือรางวัลปลอมอันเป็นสิ่งเร้าเชิงบวก ไปสู่การสร้างกลไกเชิงจิตวิทยาที่เป็นตัวเร่งปฏิกิริยาพฤติกรรม (Psychological Triggers) โดยเฉพาะอย่างยิ่งการใช้กลวิธีสร้างความเร่งด่วนทางเงื่อนไขเวลา (Urgency Technique) และการประยุกต์ใช้จิตวิทยาเชิงกดดันให้เกิดความตระหนกกลัว (Fear-inducing Manipulation) ผ่านสถานการณ์จำลองคดีความทางกฎหมายที่เกี่ยวเนื่องกับการฟอกเงิน เพื่อให้ผู้เสียหายสูญเสียความสามารถในการคิดเชิงวิพากษ์และยอมปฏิบัติตามข้อสั่งการของผู้โจมตี

3. พลวัตด้านข้อมูลที่ถูกเปิดเผย เทคโนโลยีที่ใช้ และผลลัพธ์ของการโจมตี

จุดเปลี่ยนผ่านเชิงกระบวนทัศน์ที่สำคัญที่สุด (Paradigm Shift) คือวัตถุประสงค์และผลลัพธ์สุดท้ายของการโจมตี ซึ่งแปรเปลี่ยนจากการมุ่งจารกรรมข้อมูลอัตลักษณ์ส่วนบุคคลหรือชุดรหัสผ่านชั่วคราว (One-Time Password: OTP) ผ่านหน้าต่างอินเทอร์เฟซปลอมซ้อนทับ (Overlay Attack) ไปสู่กระบวนการบงการพฤติกรรมเพื่อเข้าควบคุมอุปกรณ์จากระยะไกลโดยตรง (Action Manipulation) โดยผู้โจมตีจะล่อลวงให้ติดตั้งไฟล์ชุดคำสั่งประเภท .APK ที่มีการฝังมัลแวร์ควบคุมระยะไกลประเภทโทรจัน (Remote Access Trojan: RAT) ร่วมกับการบงการให้ผู้เสียหายก้าวล่วงเปิดสิทธิ์บริการช่วยเหลือการเข้าถึงระบบในระดับรากขั้นสูงสุด (Accessibility Service Abuse) ส่งผลให้ผู้โจมตีสามารถตรวจดักรหัสผ่าน ทำการสะท้อนหน้าจอ (Screen Mirroring) และสั่งการโอนย้ายสินทรัพย์ออกจากแอปพลิเคชันธนาคารพาณิชย์ไปยังบัญชีม้า (Mule Account) ในลักษณะเรียลไทม์ผ่านเลขที่อยู่ไอพี (IP Address) ของอุปกรณ์ผู้เสียหายเองอย่างสมบูรณ์

อภิปรายผล

จากข้อค้นพบเชิงประจักษ์ (Empirical Knowledge) ในการศึกษาการเปลี่ยนแปลงของการโจมตีด้วยวิศวกรรมสังคมของภัยคุกคามไซเบอร์ กรณีศึกษาการโจมตีแบบฟิชชิง ผู้วิจัยสามารถนำประเด็นจุดเปลี่ยนผ่านเชิงกระบวนทัศน์ (Paradigm Shift) ทั้ง 3 ประการ มาอภิปรายผลร่วมกับหลักทฤษฎีพฤติกรรมศาสตร์และกรอบแนวคิดความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีนัยสำคัญ ดังนี้

1. การเปลี่ยนจากการหลอกด้วยข้อความเป็นการสร้างความจริงปลอม (Deceptive Message to Synthetic Reality) ในอดีตช่วงปี พ.ศ. 2560 ผู้โจมตีเน้นใช้ข้อความหว่านแห (Mass Phishing) ผ่านทาง SMS หรืออีเมลเพื่อกระตุ้นให้ผู้เสียหายเกิดความตื่นตระหนก ทว่าในปัจจุบันปี พ.ศ. 2567 พฤติการณ์คดีได้แปรเปลี่ยนไปสู่การประยุกต์ใช้นวัตกรรมระดับสูง เช่น เทคโนโลยีดีปเฟกเชิงปฏิบัติการ (Live Deepfake) และการจำลองเสียงด้วยปัญญาประดิษฐ์ (AI Voice Cloning) มาสร้างภาพและเสียงที่สามารถโต้ตอบเชิงรุกได้ในลักษณะเรียลไทม์ขณะวิดีโอคอล พลวัตความเปลี่ยนแปลงนี้อภิปรายได้ว่า สื่อสังเคราะห์และความจริงจำลอง (Synthetic Reality) ได้กลายสภาพมาเป็นเครื่องมือทางจิตวิทยาในการทำลายกลไกการยับยั้งชั่งใจและวิจารณญาณขั้นพื้นฐานของมนุษย์ เนื่องจากโดยธรรมชาติทางชีววิทยาและจิตวิทยาสังคม มนุษย์มีแนวโน้มที่จะให้ความปักใจเชื่อและลดมาตรการป้องกันตนเองเมื่อเกิดการรับรู้ผ่านสิ่งเร้าที่ ตาเห็นและหูได้ยิน ซึ่งสอดคล้องกับหลักทฤษฎีการชักจูง (Principles of Influence) ของ Cialdini (2021) ในมิติด้านการแอบอ้างเป็นผู้มีอำนาจอันชอบธรรม (Authority) การแสดงอัตลักษณ์ปลอมเป็นเจ้าหน้าที่ตำรวจในชุดเครื่องแบบผ่านวิดีโอคอลสด จึงเป็นกลวิธีเชิงปฏิบัติการทางปัญญา (Cognitive Warfare) ที่ส่งผลรบกวนกระบวนการตัดสินใจอย่างมีเหตุผล ปรากฏการณ์นี้ฉายภาพให้เห็นว่าแนวทางการศึกษาและการป้องกันภัยไซ

เบอร์ในอดีตที่มุ่งเน้นเพียงการตรวจสอบตัวสะกด ไวยากรณ์ภาษา หรือลิงก์ปลายทาง (URL) ไม่เพียงพอที่จะรองรับโครงสร้างภัยคุกคามในปัจจุบันได้อีกต่อไป

2. การเปลี่ยนจากขโมยข้อมูลเป็นการบงการคนให้เปิดประตู (Information Theft to Action Manipulation) ผลการวิจัยพบจุดเปลี่ยนสำคัญในมิติวัตถุประสงค์เชิงปฏิบัติการ โดยแปรเปลี่ยนจากการหลอกถามชุดรหัสผ่านเพื่อจารกรรมข้อมูล (Information Theft) ในอดีต ไปสู่กระบวนการล่อลวงเชิงพฤติกรรมศาสตร์เพื่อบงการให้ผู้เสียหายดำเนินการติดตั้งไฟล์ชุดคำสั่งอันตราย (.APK) และกดยินยอมอนุมัติสิทธิ์การเข้าถึงระบบในระดับรากขั้นสูงสุด หรือการก้าวล่วงสิทธิ์บริการช่วยเหลือการเข้าถึงระบบ (Accessibility Service Abuse) ประเด็นนี้สามารถอภิปรายได้ว่า ยิ่งสถาบันการเงินมีการยกระดับมาตรการรักษาความปลอดภัยทางเทคนิคเชิงระบบ (System Defense) ให้มีความเข้มงวดและซับซ้อนมากเพียงใด เช่น การบังคับสแกนอัตลักษณ์ใบหน้า (Biometrics) หรือการใช้รหัสผ่านชั่วคราว (2FA/OTP) ผู้โจมตียิ่งพัฒนาฝีมือทางวิศวกรรมสังคม (Social Engineering) มามุ่งเป้าเจาะจงที่ช่องโหว่ด้านพฤติกรรมมนุษย์ (Human Vulnerability) โดยตรง เพื่อแปรสภาพให้เจ้าของอุปกรณ์ทำหน้าที่เป็นผู้ เปิดประตูระบบ และส่งมอบอำนาจการควบคุมระยะไกล (Remote Access Trojan RAT) ให้แก่ผู้โจมตีด้วยความยินยอม สอดคล้องกับโมเดลความปลอดภัยของ Bruce Schneier (1999) ที่เน้นย้ำว่า ความมั่นคงปลอดภัยเป็นกระบวนการต่อเนื่องที่ต้องบูรณาการร่วมกันระหว่าง บุคลากร (People) กระบวนการ (Process) และเทคโนโลยี (Technology) ปรากฏการณ์แอปพลิเคชันควบคุมระยะไกลสะท้อนให้เห็นถึงความล้มเหลวของแนวป้องกันเชิงเทคนิคดั้งเดิม (Firewall) เพราะระบบตรวจจับพฤติกรรมทุจริตของธนาคารไม่แจ้งเตือนความผิดปกติ เนื่องจากคำสั่งการโอนย้ายสินทรัพย์ไปยังบัญชีม้า (Mule Account) ล้วนเกิดขึ้นบนตัวอุปกรณ์และที่อยู่ไอพี (IP Address) จริงของผู้เสียหายเอง องค์ความรู้เชิงประจักษ์นี้จึงเป็นเครื่องยืนยันว่ากลไกการบงการพฤติกรรม (Action Manipulation) สามารถเอาชนะเทคโนโลยีความปลอดภัยทางคอมพิวเตอร์ที่เข้มงวดที่สุดได้ผ่านสภาวะตื่นตระหนกของมนุษย์

3. การเปลี่ยนจากการสุ่มเป็นการรู้ลึกรายบุคคล (Mass Phishing deviance to Hyper-Personalized Profiling) ในมิติของกลุ่มเป้าหมาย พลวัตได้แปรเปลี่ยนจากการส่งข้อมูลหลอกลวงแบบสุ่มกระจายเชิงปริมาณ (Mass Phishing) ในอดีต ไปสู่ยุคของการใช้เทคนิคเติมเต็มข้อมูลอัจฉริยะ (Data Enrichment) นำฐานข้อมูลส่วนบุคคลที่รั่วไหลสู่สาธารณะ (Data Breach) ในอดีตมาทำการประมวลผลและวิเคราะห์ร่วมกับการสืบค้นข้อมูลจากแหล่งเปิด (Open Source Intelligence OSINT) ประเด็นนี้อภิปรายได้ว่า ข้อมูลอัตลักษณ์ส่วนบุคคลที่เคยหลุดรอดไปในอดีตไม่ได้สูญหายไปหากแต่ถูกขบวนการอาชญากรรมนำมาแปรรูปเป็น วัตถุดิบเชิงกลยุทธ์ ในการทำแฟ้มประวัติสร้างบทสนทนาล่อลวงเฉพาะบุคคล (Spear Phishing) ที่รู้ลึกถึงประวัติทางการเงิน เลขที่บัญชี หรือเลขฐานคดีความจริง สภาพการณ์ดังกล่าวสร้างความสมมาตรของข้อมูลลวง (Information Symmetry) ทำให้เรื่องราวสมมติที่ผู้โจมตีแต่งขึ้นมีความสมจริงและเฉพาะเจาะจงกับบริบทชีวิตของเป้าหมายจนยากที่จะปฏิเสธหรือตั้งข้อสงสัย สอดคล้องกับแนวคิดของ Hadnagy (2018) และผลการศึกษาของ จิตรา

ภรณ์ (2565) และ เพชรกล้า (2564) ในมิติด้านพฤติกรรมและการป้องกันทางกฎหมาย ที่ชี้ให้เห็นว่า ความซับซ้อนของภัยคุกคามในประเทศไทยได้ก้าวข้ามปัญหาทางเทคนิคขั้นพื้นฐาน ไปสู่โครงสร้างอาชญากรรมทางปัญญาจัดตั้ง (Fraud CRM / Cyber Syndicate) ที่มีการซื้อขายรายชื่อพร้อมโจมตี (Ready-to-attack Leads) ในตลาดมืด ซึ่งการค้นพบความเชื่อมโยงเชิงระบบนี้ถือเป็นองค์ความรู้ที่แสดงให้เห็นพลวัตของรูปแบบการโจมตีที่เปลี่ยนแปลงไปที่แสดงให้เห็นว่า การสร้างภูมิคุ้มกันทางดิจิทัลในยุคปัจจุบันจำเป็นต้องปรับเปลี่ยนจากการจำแนกเทคนิควิธี มาเป็นการกำหนดหลักการสากลที่ไม่พึ่งพาความไว้วางใจในโลกดิจิทัลจนกว่าจะได้รับการตรวจสอบจริง (Zero Trust / Verify then Trust) เพื่อรับมือกับการแทรกซึมเชิงพฤติกรรมศาสตร์ในอนาคตสืบไป

บทสรุปการอภิปราย การเปลี่ยนแปลงนี้สะท้อนให้เห็นว่า ภัยไซเบอร์ปัจจุบันไม่ได้โจมตีที่ ระบบคอมพิวเตอร์ แต่โจมตีที่ กระบวนการตัดสินใจของมนุษย์ องค์ความรู้สะท้อนให้เห็นแนวโน้มสำคัญของภัยคุกคามไซเบอร์ร่วมสมัยนี้จึงเป็นเครื่องยืนยันว่า การสร้างภูมิคุ้มกันทางดิจิทัลต้องเปลี่ยนจากการจำแค่เทคนิคการหลอก เป็นการสร้างหลักการ ไม่เชื่อใจใครในโลกดิจิทัลจนกว่าจะตรวจสอบได้จริง (Zero Trust) เพื่อรับมือกับการบงการมนุษย์ในยุคสื่อสังเคราะห์สืบไป

ข้อเสนอแนะ

เพื่อให้เกิดการต่อยอดองค์ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้มีความลึกซึ้งและครอบคลุมในระดับนโยบายและการปฏิบัติ ผู้วิจัยมีข้อเสนอแนะสำหรับการศึกษาวิจัยในอนาคตดังนี้

1. การขยายขอบเขตและกลุ่มเป้าหมายให้มีความหลากหลาย ควรพิจารณาขยายการศึกษากลุ่มตัวอย่างให้ครอบคลุมประชากรในทุกช่วงวัยและกลุ่มอาชีพเฉพาะ เช่น กลุ่มผู้สูงอายุหรือผู้ประกอบการรายย่อย รวมถึงการศึกษาเปรียบเทียบในมิติของภูมิภาคต่าง ๆ เพื่อวิเคราะห์ความแตกต่างของบริบทการใช้งานเทคโนโลยีและการตระหนักรู้ต่อภัยคุกคาม ซึ่งจะช่วยให้การกำหนดมาตรการป้องกันมีความสอดคล้องกับลักษณะของแต่ละกลุ่มเป้าหมายได้อย่างมีประสิทธิภาพ
2. การวิเคราะห์ปัจจัยเชิงบวกจากกลุ่มผู้ที่ไม่เคยตกเป็นผู้เสียหาย นอกจากการศึกษาผู้ที่มีประสบการณ์ตรงแล้ว การศึกษาเปรียบเทียบกับกลุ่มผู้ใช้งานทั่วไปที่สามารถหลีกเลี่ยงการโจมตีได้ จะช่วยให้ค้นพบปัจจัยเชิงบวก เช่น ทักษะการวิเคราะห์ข้อมูล หรือระดับการตระหนักรู้ที่จำเพาะเจาะจง ข้อมูลเหล่านี้จะเป็นประโยชน์อย่างยิ่งในการนำมาออกแบบแนวทางการสื่อสารและการฝึกอบรมที่มีประสิทธิภาพ โดยอ้างอิงจากพฤติกรรมที่ประสบความสำเร็จในการป้องกันตนเอง
3. การมุ่งเน้นการศึกษาในพื้นที่ชุมชนท้องถิ่น ควรขยายพื้นที่การศึกษาไปยังต่างจังหวัดและพื้นที่ชนบท เพื่อสะท้อนถึงความเหลื่อมล้ำด้านทักษะไซเบอร์ (Digital Divide) และความสามารถในการเข้าถึงข้อมูลข่าวสารด้านความปลอดภัย ข้อมูลที่ได้จะช่วยให้นักนโยบายสามารถออกแบบกลยุทธ์การ

ประชาสัมพันธ์ที่เหมาะสมกับกลุ่มประชากรที่มีข้อจำกัดด้านการศึกษาหรือการเข้าถึงเทคโนโลยีได้อย่างทั่วถึง

4. การรับมือกับภัยคุกคามจากเทคโนโลยีอุบัติของภัยคุกคามไซเบอร์ร่วมสมัย งานวิจัยในอนาคตควรให้ความสำคัญกับการศึกษาเชิงลึกเกี่ยวกับผลกระทบของเทคโนโลยีขั้นสูง โดยเฉพาะปัญญาประดิษฐ์ (AI) และ Deepfake ที่ใช้ในการสร้างสื่อสังเคราะห์เพื่อบงการพฤติกรรมมนุษย์ การวิเคราะห์ผลกระทบทางจิตวิทยาในรูปแบบการโจมตีที่เปลี่ยนแปลงไปนี้จะเป็นรากฐานสำคัญในการสร้างแนวทางป้องกันและเสริมสร้างภูมิคุ้มกันทางไซเบอร์ที่เท่าทันต่อโลกดิจิทัลในอนาคต

บรรณานุกรม

กรกัญญ์ญา รักบุญสุขเกิด. (2564). สถานการณ์และแนวทางการป้องกันอาชญากรรมไซเบอร์ในประเทศไทย. (วิทยานิพนธ์ปริญญามหาบัณฑิต). มหาวิทยาลัยหอการค้าไทย.

จิณณ์ฟ้า รักไทยเจริญชีพ. (2568). การศึกษาการโจมตีด้วยวิศวกรรมสังคมของภัยคุกคามไซเบอร์ กรณีศึกษาการโจมตีแบบฟิชชิง. (วิทยานิพนธ์ปริญญามหาบัณฑิต). มหาวิทยาลัยหอการค้าไทย.

ชฎาภรณ์ สิงห์แก้ว. (2564). บทบาทภาครัฐในการป้องกันอาชญากรรมไซเบอร์. (วิทยานิพนธ์ปริญญามหาบัณฑิต). มหาวิทยาลัยหอการค้าไทย.

จิตราภรณ์ โสตถิกุล. (2565). การก่อการร้ายทางไซเบอร์ ปัญหาการนิยาม เขตอำนาจ และการบังคับใช้กฎหมาย. (วิทยานิพนธ์ปริญญามหาบัณฑิต). มหาวิทยาลัยหอการค้าไทย.

ตำรวจสอบสวนกลาง. (2567). รายงานสถิติอาชญากรรมทางเทคโนโลยีและรูปแบบการหลอกลวงออนไลน์ประจำปี พ.ศ. 2567. กองบัญชาการตำรวจสอบสวนกลาง.

ธนาคารแห่งประเทศไทย. (2566). แนวทางการจัดการภัยทุจริตทางการเงินและการคุ้มครองผู้ใช้บริการดิจิทัล. https://www.bot.or.th

เพชรกล้า นัทธมน. (2564). การรับมือของภาครัฐกับการก่อการร้ายทางไซเบอร์ในประเทศไทย. (วิทยานิพนธ์ปริญญามหาบัณฑิต). มหาวิทยาลัยหอการค้าไทย.

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562. (2562, 27 พฤษภาคม). ราชกิจจานุเบกษา. เล่ม 136 ตอนที่ 69 ก. หน้า 20-54.

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. (2567). รายงานสถานการณ์ภัยคุกคามทางไซเบอร์ของประเทศไทย ประจำปี 2566. https://www.ncsa.or.th

อารยฤทธิ์ พรหมมะ. (2565). การรับรู้ตัวอย่างกรณีศึกษาสารอาชญากรรมทางเทคโนโลยีในรูปแบบวิธีหลอกรักออนไลน์ ทัศนคติ และพฤติกรรมการใช้งานของผู้บริโภคต่อแอปพลิเคชันหาคู่. (วิทยานิพนธ์ปริญญามหาบัณฑิต). มหาวิทยาลัยหอการค้าไทย.

Anderson, J. P. (1972). Computer Security Technology Planning Study (ESD-TR-72-122). Electronic Systems Division (AFSC).

Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems (3rd ed.). John Wiley & Sons.

Cialdini, R. B. (1984). Influence: The Psychology of Persuasion. William Morrow and Company.

ENISA. (2021). ENISA Threat Landscape 2021. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Europol. (2024). Internet Organised Crime Threat Assessment (IOCTA) 2024. https://www.europol.europa.eu/publications-documents/internet-organised-crime-threat-assessment-iocta-2024

Fortinet. (2024, November 26). Charting the Changes of the 2025 Threat Landscape. https://www.fortinet.com/blog/business-and-technology/charting-the-changes-of-the-2025-threat-landscape

Hadnagy, C. (2010). Social Engineering: The Art of Human Hacking. John Wiley & Sons.

INTERPOL. (2023). INTERPOL Cybercrime Report 2023. https://www.interpol.int/content/download/18153/file/INTERPOL_Cybercrime_Report_2023.pdf

Jagatic, G. W., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. Communications of the ACM, 50(10), 94-100.

Kaspersky. (2022). Kaspersky Southeast Asia Cyber Threat Report 2022. https://www.kaspersky.com/about/press-releases/2022_kaspersky-southeast-asia-cyber-threat-report-2022

Kaspersky. (2023). Kaspersky Southeast Asia Cyber Threat Report 2023. https://www.kaspersky.com/about/press-releases/2023_kaspersky-southeast-asia-cyber-threat-report-2023

Kaspersky. (2024). Phishing and Artificial Intelligence. https://www.kaspersky.com/resource-center/definitions/phishing-and-artificial-intelligence

Kemp, S. (2024, January). Digital 2024: Thailand. DataReportal. https://datareportal.com/reports/digital-2024-thailand

Luo, X., Li, H., Zhang, J., & Shim, J. P. (2021). Examining multi-stage phishing attacks: A life cycle perspective. Decision Support Systems, 141, 113450.

Mann, S. (2017). Hacking the Human: Social Engineering Techniques and Security. CRC Press.

Mitnick, K. D., & Simon, W. L. (2003). The Art of Deception: Controlling the Human Element of Security. John Wiley & Sons.

Palo Alto Networks. (2024). AI and Phishing: A New Age of Cyber Threats. https://www.paloaltonetworks.com/cyberpedia/what-is-ai-phishing

Proofpoint. (2024). AI in Phishing: The Future of Cybersecurity Threats. https://www.proofpoint.com/us/blog/security-awareness-training/ai-phishing-future-cybersecurity-threats

Salas-Zarate, R., & Valencia-García, R. (2022). Social engineering attacks: A systematic literature review. IEEE Access, 10, 11210-11235.

Schneier, B. (1999). Secrets and Lies: Digital Security in a Networked World. John Wiley & Sons.

Workman, M. (2008). Wisecrackers, hackers, and con artists: An analysis of social engineering. Journal of the American Society for Information Science and Technology, 59(4), 662-673.

World Economic Forum. (2021). The Global Risks Report 2021. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

World Economic Forum. (2022). The Global Risks Report 2022. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf