ภัยคุกคามจากอาชญากรรมไซเบอร์: กรณีศึกษาอาชญากรรมรูปแบบการโจมตีแบบฟิชชิง
Cybercrime Threats: A Case Study of Phishing Attacks

หทัยชนก อินทรวิจิตร[1]
Hathaichanok Intravichit

Received: May 27, 2025
Revised: July 7, 2025
Accepted: July 25, 2025

บทคัดย่อ

บทความวิจัยนี้มีวัตถุประสงค์เพื่อศึกษารูปแบบของภัยคุกคามจากอาชญากรรมไซเบอร์ กรณีการโจมตีแบบฟิชชิงที่เกิดขึ้นในประเทศไทย และเพื่อเสนอแนวทางป้องกันที่เหมาะสมและมีประสิทธิภาพในบริบทของสังคมดิจิทัล โดยใช้การวิเคราะห์เชิงเอกสารจากงานวิจัยและข้อมูลจากหน่วยงานที่เกี่ยวข้อง ร่วมกับการประยุกต์ใช้กรอบแนวคิดทางอาชญาวิทยา

ผลการศึกษาแสดงให้เห็นว่า การโจมตีแบบฟิชชิงในประเทศไทยมีความหลากหลายและซับซ้อนยิ่งขึ้น โดยรูปแบบการโจมตีแบบฟิชชิงนั้น มักอาศัยเทคนิควิศวกรรมสังคมเพื่อหลอกลวงเหยื่อโดยอาศัยช่องว่างของระบบดิจิทัลและความไม่รู้เท่าทันของเหยื่อ ขณะเดียวกันจากการศึกษา พบว่า ประเทศไทยยังเผชิญกับอุปสรรคด้านกฎหมาย ความร่วมมือระหว่างประเทศ และข้อจำกัดด้านทรัพยากรบุคลากร จึงนำไปสู่การนำเสนอแนวทางการป้องกันที่สำคัญเพื่อสร้างความมั่นคงทางไซเบอร์อย่างยั่งยืนในระยะยาว

คำสำคัญ: **ภัยคุกคามทางไซเบอร์, อาชญากรรมไซเบอร์, การโจมตีแบบฟิชชิง**

Abstract

This research article aims to examine the patterns of cybercrime threats, with a particular focus on phishing attacks in Thailand, and propose appropriate and effective preventive measures within the context of a digital society. The study employs a documentary research methodology, drawing on academic literature and data from relevant agencies, together with the application of criminological theoretical frameworks.

The findings indicate that phishing attacks in Thailand have become increasingly diverse and sophisticated. These attacks commonly utilize social engineering techniques to deceive victims by exploiting vulnerabilities in digital systems and their lack of cybersecurity awareness. Furthermore, the study reveals that Thailand continues to face several challenges in combating phishing, including legal limitations, barriers to international cooperation, and shortages of skilled personnel. To address these challenges, this research article proposes key preventive strategies aimed at enhancing long-term cybersecurity resilience and fostering a more secure digital environment.

Keywords: Cyber Threats, Cybercrime, Phishing Attacks

[1] นักศึกษาปริญญาเอก คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
Ph.D. Student, Faculty of Political Science, Chulalongkorn University
E-mail: 6381019624@student.chula.ac.th

บทนำ

ในยุคที่เทคโนโลยีสารสนเทศและอินเทอร์เน็ตมีบทบาทสำคัญในการดำเนินชีวิต อาชญากรรมก็ปรับเปลี่ยนรูปแบบตามไปด้วย โดยเฉพาะการเคลื่อนย้ายของอาชญากรเข้าสู่โลกออนไลน์ ซึ่งส่งผลให้อาชญากรรมไซเบอร์ (Cybercrime) กลายเป็นภัยคุกคามสำคัญของสังคมยุคใหม่ที่ไม่อาจมองข้าม เนื่องจากสามารถก่อให้เกิดความเสียหายได้ทั้งต่อชีวิต ทรัพย์สิน และความมั่นคงของรัฐ โดยอาศัยเพียงอุปกรณ์อิเล็กทรอนิกส์และอินเทอร์เน็ตเป็นเครื่องมือ ถึงแม้ว่าอาชญากรรมไซเบอร์จะยังไม่มีนิยามทางกฎหมายที่เป็นสากล แต่สามารถเข้าใจโดยทั่วไปว่า หมายถึงการกระทำผิดกฎหมายที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศ ไม่ว่าจะในฐานะเครื่องมือหรือเป้าหมายของการโจมตี โดยแบ่งได้เป็น 2 ประเภทหลัก ได้แก่ อาชญากรรมไซเบอร์โดยตรง เช่น การแฮกระบบหรือปล่อยมัลแวร์ และอาชญากรรมที่ใช้เทคโนโลยีเป็นเครื่องมือ เช่น การฉ้อโกง ฟอกเงิน และการโจมตีแบบฟิชชิง เป็นต้น และในส่วนของฟิชชิง (Phishing) ถือเป็นภัยคุกคามอาชญากรรมทางเทคโนโลยีที่พบได้บ่อยในปัจจุบัน โดยใช้กลวิธีวิศวกรรมสังคม (Social Engineering) หลอกให้เหยื่อหลงเชื่อและเปิดเผยข้อมูลส่วนบุคคลผ่านการปลอมแปลงอัตลักษณ์ เช่น การแอบอ้างเป็นหน่วยงานราชการ ธนาคาร หรือบริษัทเอกชน (Cambridge Dictionary, n.d.) ทั้งนี้ จากรายงานของ Anti-Phishing Working Group (APWG) ประจำไตรมาสที่ 4 ปี 2566 ระบุว่า มีเหตุการณ์ฟิชชิงที่ถูกรายงานทั่วโลกมากกว่า **4.7 ล้านครั้งภายในปีเดียว** และมีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่องในปี 2567 โดยเฉพาะในกลุ่มบริการการเงินและโซเชียลมีเดีย (APWG, 2024) ซึ่งสะท้อนให้เห็นถึงการปรับตัวของอาชญากรที่สอดรับกับพฤติกรรมผู้ใช้งานในโลกยุคดิจิทัล

ในประเทศไทย แนวโน้มอาชญากรรมฟิชชิงยังคงขยายตัวอย่างต่อเนื่องและมีความหลากหลายมากขึ้น โดยเฉพาะหลังวิกฤตการแพร่ระบาดของโควิด-19 ซึ่งส่งผลให้ประชาชนจำนวนมากหันมาใช้บริการออนไลน์เพิ่มขึ้นอย่างรวดเร็ว ทั้งในการศึกษา การทำงาน และการทำธุรกรรมทางการเงิน แม้เทคโนโลยีจะช่วยเพิ่มความสะดวกสบายในชีวิตประจำวัน แต่อาชญากรก็อาศัยช่องโหว่ในระบบเหล่านี้ในการก่อเหตุได้เช่นเดียวกัน

จากบริบทและข้อมูลที่กล่าวมาข้างต้น การศึกษาครั้งนี้จึงมีวัตถุประสงค์เพื่อศึกษารูปแบบของภัยคุกคามจากอาชญากรรมไซเบอร์ กรณีการโจมตีแบบฟิชชิงที่เกิดขึ้นในประเทศไทย พร้อมทั้งนำเสนอแนวทางการป้องกันที่เหมาะสมและมีประสิทธิภาพ เพื่อเสริมสร้างความสามารถในการรับมือกับภัยไซเบอร์อย่างยั่งยืน

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษารูปแบบภัยคุกคามจากอาชญากรรมไซเบอร์ กรณีการโจมตีแบบฟิชชิงที่เกิดขึ้นในประเทศไทย
2. เพื่อศึกษาแนวทางการป้องกันภัยคุกคามอาชญากรรมไซเบอร์ กรณีการโจมตีแบบฟิชชิง

ทบทวนวรรณกรรม

ความหมายของอาชญากรรมไซเบอร์

อาชญากรรมไซเบอร์ (Cybercrime) อาจไม่มีนิยามทางกฎหมายที่ชัดเจนเพียงประการเดียว แต่มีลักษณะร่วมกันที่สามารถเข้าใจได้ว่า เป็นการกระทำผิดกฎหมายที่เกี่ยวข้องกับการใช้ระบบคอมพิวเตอร์ เทคโนโลยีสารสนเทศและเครือข่ายอินเทอร์เน็ต ทั้งในฐานะเครื่องมือในการกระทำผิด หรือเป้าหมายของการโจมตี

โดยทั่วไป อาชญากรรมไซเบอร์สามารถจำแนกได้เป็น 2 กลุ่มหลัก คือ 1) อาชญากรรมทางไซเบอร์โดยแท้ ซึ่งมุ่งเน้นที่การทำลายหรือแทรกแซงระบบคอมพิวเตอร์โดยตรง และ 2) อาชญากรรมที่ใช้ไซเบอร์เป็นเครื่องมือ

สำหรับในประเทศไทย แม้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (แก้ไขเพิ่มเติม 2560) จะยังไม่มีนิยามคำว่า อาชญากรรมไซเบอร์ ไว้อย่างชัดเจน แต่จากบริบทของกฎหมาย ก็สามารถอนุมานได้ว่า หมายถึงการกระทำใด ๆ ที่ใช้ระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์เพื่อก่อให้เกิดความเสียหาย โดยมีมูลเหตุจูงใจทางอาญาและเจตนาแสวงหาผลประโยชน์อย่างมิชอบ

กล่าวโดยสรุป อาชญากรรมไซเบอร์ คือ การกระทำผิดกฎหมายที่เกี่ยวข้องกับการใช้ระบบคอมพิวเตอร์ เทคโนโลยีสารสนเทศ หรือเครือข่ายอินเทอร์เน็ต ทั้งในฐานะเครื่องมือหรือเป้าหมาย เพื่อแสวงหาผลประโยชน์หรือก่อให้เกิดความเสียหายโดยมิชอบ

การศึกษาเกี่ยวกับสถานการณ์ภัยคุกคามอาชญากรรมไซเบอร์ และอาชญากรรมไซเบอร์รูปแบบการโจมตีแบบฟิชชิง

ในปัจจุบันภัยคุกคามอาชญากรรมทางไซเบอร์ไม่ได้เป็นเรื่องไกลตัวอีกต่อไป แต่กลายเป็นปัญหาที่แทรกซึมอยู่ในชีวิตประจำวันของประชาชนไทยอย่างแนบเนียน โดยเฉพาะ “การโจมตีแบบฟิชชิง” ที่ไม่ต้องใช้ความสามารถทางเทคนิคสูงก็สามารถก่อเหตุได้ เพียงมีข้อความที่ดูน่าเชื่อถือ ลิงก์ปลอมสักลิงก์ หรือเสียงปลอมที่แอบอ้างว่าเป็นเจ้าหน้าที่ ผู้ใช้งานก็อาจตกเป็นเหยื่อในชั่วพริบตา

สิ่งที่น่ากังวลคือ อาชญากรไซเบอร์มีการพัฒนารูปแบบอย่างต่อเนื่องและรวดเร็ว จนผู้ใช้งานทั่วไปตามไม่ทัน ไม่ว่าจะเป็นการใช้ AI ปลอมเสียง Deepfake โทรหลอกเหยื่อ หรือการสร้างเว็บปลอมให้ติดอันดับ Google Search ได้ภายในไม่กี่ชั่วโมง และจากข้อมูลหลายแหล่งชี้ตรงกันว่า ฟิชชิงยังคงเป็นรูปแบบอาชญากรรมไซเบอร์ที่สร้างความเสียหายมากที่สุดในระดับโลกและในประเทศไทย

ทั้งนี้จากการศึกษา พบว่าประเทศไทยมีการใช้งานอินเทอร์เน็ตสูงและพฤติกรรมการใช้โซเชียลอย่างกว้างขวาง ยิ่งทำให้กลายเป็นเป้าหมายของเหล่าอาชญากรไซเบอร์ ไม่ว่าจะเป็นในระดับบุคคลหรือองค์กร ดังนั้น การเข้าใจรูปแบบการโจมตีอย่างลึกซึ้ง พร้อมทั้งรับรู้สถานการณ์ปัจจุบันอย่างเท่าทัน จึงเป็นสิ่งสำคัญที่สุดในการลดความเสี่ยงและรับมือกับภัยคุกคามเหล่านี้อย่างมีประสิทธิภาพ

สถานการณ์ภัยคุกคามอาชญากรรมไซเบอร์ รูปแบบการโจมตีแบบฟิชชิง

จากการศึกษาสถานการณ์การโจมตีแบบฟิชชิงในประเทศไทย พบว่าอัตราการตกเป็นเหยื่อฟิชชิงของประชาชนเพิ่มขึ้นอย่างต่อเนื่อง โดยอาชญากรมักใช้เทคนิควิศวกรรมสังคม (Social Engineering) เพื่อหลอกลวงเหยื่อให้เปิดเผยข้อมูลส่วนบุคคล หรือข้อมูลทางการเงิน โดยประเทศไทยเผชิญกับการโจมตีฟิชชิงหลากหลายรูปแบบ จากการศึกษารวบรวมข้อมูลทั้งจากงานวิจัย สื่อมวลชน และสถิติของหน่วยงานรัฐ พบว่ามี 8 รูปแบบฟิชชิงหลัก ได้แก่

1. **Email Phishing** จากการศึกษาถือเป็นรูปแบบฟิชชิงที่พบมากที่สุด โดยอาชญากรจะส่งอีเมลที่ปลอมแปลงว่าเป็นหน่วยงานน่าเชื่อถือ เช่น ธนาคาร ไปรษณีย์ หรือหน่วยงานรัฐ พร้อมแนบลิงก์ปลอมไปยังเว็บไซต์ที่มีหน้าตาเหมือนจริง เพื่อหลอกให้เหยื่อกรอกข้อมูลสำคัญ เช่น Username, Password หรือรหัส OTP เป็นต้น

2. **Spear Phishing** จากการศึกษาถือเป็นฟิชชิงที่เจาะจงเป้าหมายเฉพาะ เช่น พนักงานการเงินขององค์กร ข้าราชการ หรือกลุ่มผู้สูงวัย โดยอาชญากรจะศึกษาข้อมูลเหยื่อจากโซเชียลมีเดียและแหล่งออนไลน์ต่าง ๆ เพื่อสร้างความน่าเชื่อถือ เช่น รู้ชื่อ ตำแหน่ง เบอร์โทร และจะส่งอีเมลหรือข้อความที่ดูเป็นเรื่องส่วนตัว เพื่อหลอกให้เปิดไฟล์แนบหรือคลิกลิงก์อันตราย

3. **Whaling Phishing** จากการศึกษา พบว่าเป็นลักษณะมุ่งเป้าไปที่ผู้บริหารระดับสูงหรือผู้มีอำนาจตัดสินใจในองค์กร เช่น CEO หรือ CFO โดยแฮกเกอร์อาจปลอมอีเมลเป็นคู่ค้า หรือนักกฎหมาย แจ้งเตือนเรื่องเร่งด่วนเกี่ยวกับเอกสาร หรือการดำเนินคดี พร้อมลิงก์แนบปลอม องค์กรขนาดใหญ่ในไทยตกเป็นเป้าโจมตีลักษณะนี้หลายกรณี เช่น บริษัทพลังงาน บริษัทการเงิน และหน่วยงานราชการ

4. **Smishing (SMS Phishing)** จากการศึกษาถือเป็นการฟิชชิงผ่านข้อความ SMS และมักอ้างว่ามาจากธนาคาร บริษัทขนส่ง หรือแอปชำระเงิน เช่น "พบธุรกรรมผิดปกติในบัญชีของคุณ กรุณาคลิกที่นี่" เหยื่อที่คลิกมักถูกขโมย OTP หรือรหัสผ่าน พบสถิติในปี 2566 ว่ามีผู้เสียหายจาก SMS ปลอมมากกว่า 30,000 รายทั่วประเทศ โดยหลายคนไม่ทันสังเกตว่า URL นั้นเป็นของปลอม

5. **Vishing (Voice Phishing)** จากการศึกษา ฟิชชิงประเภทนี้เป็นเทคนิคที่แก๊งคอลเซนเตอร์ใช้โดยคนร้ายจะโทรศัพท์ติดต่อเหยื่อโดยตรง แอบอ้างเป็นเจ้าหน้าที่จากหน่วยงานที่มีความน่าเชื่อถือ เช่น ตำรวจ ธนาคาร

สำนักงานศุลกากร หรือหน่วยงานรัฐต่าง ๆ พร้อมแจ้งว่าเหยื่อมีส่วนเกี่ยวข้องกับการกระทำผิดกฎหมาย หรือมีปัญหาทางบัญชีทางการเงิน จากนั้นจะใช้เทคนิคกดดันทางจิตวิทยา เช่น ข่มขู่ว่าเหยื่อจะถูกดำเนินคดี ถูกอายัดบัญชี หรือมีหมายจับ เพื่อให้เหยื่อตื่นตระหนก และยอมทำตามคำสั่ง ซึ่งมักลงท้ายด้วยการให้โอนเงินเข้าบัญชีตรวจสอบที่อ้างว่าใช้ตรวจสอบเส้นทางการเงิน แท้จริงแล้วเป็นเพียงบัญชีม้าที่กลุ่มมิจฉาชีพใช้โอนเงินต่อไปยังเครือข่ายฟิชชิงในรูปแบบนี้ทำให้เหยื่อจำนวนมากสูญเสียเงินอย่างรวดเร็ว บางรายเสียหายเป็นหลักแสนถึงหลักล้านบาทภายในเวลาไม่กี่ชั่วโมง

6. Angler Phishing จากการศึกษา พบว่ามักเกิดบนแพลตฟอร์มโซเชียลมีเดีย เช่น Facebook, Instagram หรือ X (Twitter) โดยแฮกเกอร์จะแฝงตัวเป็นแอดมินแบรนด์สินค้า/บริการที่เหยื่อร้องเรียน และส่งข้อความ “ติดต่อกลับด่วน” พร้อมลิงก์ปลอม โดยอ้างว่าจะช่วยเหลือหรือตรวจสอบให้ พบมากในกรณีร้องเรียนบริษัทขนส่ง ธนาคาร และบริการโทรศัพท์มือถือ

7. Search Engine Phishing จากการศึกษา พบว่าเป็นเทคนิคใหม่ที่ใช้การ “ปลอมเว็บไซต์” แล้วซื้อโฆษณาผ่าน Google Ads หรือทำ SEO ให้ติดอันดับแรก ๆ ของผลการค้นหา เช่น เว็บปลอมของธนาคาร หรือเว็บปลอมรับสมัครงาน เมื่อผู้ใช้คลิกและกรอกข้อมูล จะตกเป็นเหยื่อทันที พบมากในกลุ่มผู้สูงอายุหรือผู้ใช้ที่ไม่เชี่ยวชาญเทคโนโลยี

8. CEO Fraud (Business Email Compromise) จากการศึกษาถือเป็นรูปแบบที่พบในองค์กรระดับกลางถึงใหญ่ โดยแฮกเกอร์จะปลอมอีเมลของผู้บริหาร เช่น CEO แล้วส่งคำสั่งให้ฝ่ายบัญชีโอนเงินไปยังบัญชีปลอม โดยใช้ถ้อยคำที่ดูเป็นทางการ และมีความเร่งด่วน

แนวคิดเกี่ยวกับอาชญากรรมไซเบอร์กับการเปลี่ยนแปลงเทคโนโลยี

Jonathan Clough (2016) ชี้ให้เห็นว่า อาชญากรรมไซเบอร์มิได้เกิดจากการกระทำของผู้กระทำผิดเพียงฝ่ายเดียวเท่านั้น หากแต่เป็นผลลัพธ์จากโครงสร้างทางสังคมและเทคโนโลยีที่เอื้อต่อการกระทำผิด ซึ่งพัฒนาควบคู่ไปกับความก้าวหน้าของเทคโนโลยีดิจิทัล โดยเฉพาะอย่างยิ่งในบริบทที่ข้อมูลได้กลายเป็นทรัพย์สินที่มีมูลค่าสูงในยุคเศรษฐกิจดิจิทัล การป้องกันภัยคุกคามทางไซเบอร์จึงมิใช่เพียงการใช้เครื่องมือด้านเทคโนโลยี เช่น ซอฟต์แวร์รักษาความปลอดภัยเท่านั้น หากแต่ต้องอาศัยการตระหนักรู้และความเข้าใจในลักษณะของภัยคุกคามที่มีการเปลี่ยนแปลงอยู่ตลอดเวลา ทั้งนี้ Jonathan Clough (2016) ระบุว่า โลกไซเบอร์มีลักษณะเฉพาะที่เอื้อต่อการก่ออาชญากรรมในสามมิติหลัก ได้แก่ ขนาดของความเสียหาย (Scale), ความง่ายในการเข้าถึง (Accessibility), การปกปิดตัวตน (Anonymity)

เมื่อรวมเข้ากับแนวคิด Space Transition Theory ของ Karuppannan Jaishankar (2008) จะพบว่าพฤติกรรมของมนุษย์สามารถเปลี่ยนแปลงได้เมื่อเข้าสู่พื้นที่ออนไลน์ โดยเฉพาะเมื่อรู้สึกว่าไร้ตัวตน และไม่ต้องรับผิดชอบบุคคลธรรมดาในโลกออฟไลน์จึงอาจกลายเป็นผู้กระทำผิดในโลกไซเบอร์ได้ แนวคิดนี้สามารถอธิบายพฤติกรรมของอาชญากรในรูปแบบ **ฟิชชิง (Phishing)** ได้อย่างน่าสนใจ กล่าวคือ ฟิชชิงเป็นหนึ่งในอาชญากรรมไซเบอร์ที่เติบโตควบคู่กับเทคโนโลยีดิจิทัล โดยอาศัยการแอบอ้างตัวตน อาทิเช่น ธนาคาร หน่วยงานรัฐ หรือผู้บริหาร ผ่านช่องทางต่าง ๆ ไม่ว่าจะเป็นอีเมล ข้อความ หรือเว็บไซต์เลียนแบบ เป็นต้น เพื่อหลอกให้เหยื่อเปิดเผยข้อมูลสำคัญ เช่น รหัสผ่าน หรือข้อมูลบัญชี การกระทำของผู้กระทำผิดมักใช้เทคนิค **วิศวกรรมสังคม (Social Engineering)** เข้าถึงจุดอ่อนของเหยื่อ ทั้งจากความไม่รู้เท่าทัน ความไว้ใจ และความเร่งรีบ จนนำไปสู่ความเสียหายที่รุนแรงได้

ในประเทศไทย พฤติกรรมของผู้ใช้งานอินเทอร์เน็ตมีการเปลี่ยนแปลงอย่างชัดเจน โดยเฉพาะในช่วงการแพร่ระบาดของโรคโควิด-19 ซึ่งเป็นปัจจัยเร่งให้ผู้บริโภคย้ายกิจกรรมจากออฟไลน์สู่โลกออนไลน์อย่างเต็มรูปแบบ ส่งผลให้การโจมตีแบบฟิชชิงเพิ่มขึ้นอย่างรวดเร็ว ตัวอย่างเช่น **Vishing Phishing** ในรูปแบบแก๊งคอลเซนเตอร์ และ **Smishing Phishing** ผ่านข้อความ SMS พร้อมลิงก์ปลอม ซึ่งมักอาศัยช่องโหว่จากความเร่งรีบ ความเป็นส่วนตัวที่ต่ำ และการกระตุ้นอารมณ์ เช่น ความกลัวหรือความโลภของเหยื่อ เป็นต้น

แนวคิดทฤษฎีเกี่ยวกับการกระทำผิดอาชญากรรมไซเบอร์

ทฤษฎีการเลือกอย่างมีเหตุผล (Rational Choice Theory)

ทฤษฎีการเลือกอย่างมีเหตุผล (Rational Choice Theory) เสนอว่า การกระทำผิดของมนุษย์เกิดจากกระบวนการตัดสินใจที่มีเหตุผล โดยผู้กระทำจะทำการประเมินและชั่งน้ำหนักระหว่าง “ต้นทุน” กับ “ผลตอบแทน” ก่อนตัดสินใจกระทำผิด (Becker, 1968; Sullivan, 1973) กล่าวคือ หากบุคคลประเมินแล้วว่าผลตอบแทนจากการกระทำผิดมีมากกว่าความเสี่ยงที่จะถูกจับกุม ถูกลงโทษ หรือเสียชื่อเสียง ก็มีแนวโน้มที่จะเลือกกระทำผิดในที่สุด และเมื่อพิจารณาในบริบทของอาชญากรรมไซเบอร์ โดยเฉพาะ การโจมตีแบบฟิชชิง (Phishing) จะพบว่าทฤษฎีนี้สามารถอธิบายพฤติกรรมของผู้กระทำผิดได้อย่างชัดเจน เนื่องจากการกระทำผิดในลักษณะนี้ มีต้นทุนต่ำ ความเสี่ยงต่ำ แต่ผลตอบแทนสูง ตัวอย่างเช่น การสร้างเว็บไซต์ปลอม การส่งอีเมลหลอก หรือการใช้ SMS เพื่อล่อลวงข้อมูลส่วนตัวของเหยื่อ ล้วนสามารถดำเนินการได้โดยไม่ต้องลงทุนด้านอุปกรณ์หรือทักษะที่ซับซ้อนมากนัก ที่สำคัญคือ ความเสี่ยงในการถูกจับกุมในคดีฟิชชิงมักจะต่ำกว่าคดีอาชญากรรมทั่วไป เนื่องจากผู้กระทำผิดสามารถซ่อนตัวอยู่ในโลกออนไลน์ ใช้เทคนิคปกปิดตัวตน หรือกระทำจากต่างประเทศ ซึ่งทำให้กระบวนการสืบสวนมีข้อจำกัดเชิงเทคนิคและกฎหมายข้ามแดน นี่จึงเป็นปัจจัยที่ทำให้ “ผลตอบแทนคุ้มค่า” ในมุมมองของอาชญากรไซเบอร์

กล่าวโดยสรุป ทฤษฎีการเลือกอย่างมีเหตุผลช่วยให้เข้าใจว่า การกระทำผิดในโลกไซเบอร์ โดยเฉพาะ ฟิชชิง มิได้เกิดจากแรงกดดันทางสังคมเพียงอย่างเดียว แต่เป็นผลจากกระบวนการตัดสินใจเชิงเหตุผลของผู้กระทำผิดที่มองเห็นต้นทุนต่ำ ความเสี่ยงน้อย และผลตอบแทนที่คุ้มค่าในบริบทของโลกออนไลน์ ซึ่งเอื้อต่อการก่ออาชญากรรมได้มากกว่าสังคมจริง

ทฤษฎีการคบค้าสมาคมที่แตกต่าง (Differential Association Theory)

Edwin H. Sutherland (1939) ได้เสนอทฤษฎีการคบค้าสมาคมที่แตกต่าง (Differential Association Theory) ซึ่งเป็นหนึ่งในแนวคิดหลักของอาชญาวิทยาเชิงสังคม โดยอธิบายว่า พฤติกรรมอาชญากรรมเกิดจากกระบวนการเรียนรู้ผ่านการปฏิสัมพันธ์กับบุคคลหรือกลุ่มที่มีค่านิยมสนับสนุนการกระทำผิด หากบุคคลได้รับอิทธิพลจากกลุ่มที่มองว่าการกระทำผิดเป็นเรื่องยอมรับได้บ่อยกว่ากลุ่มที่ต่อต้าน บุคคลนั้นก็มีแนวโน้มจะพัฒนาเป็นผู้กระทำผิด ในบริบทของฟิชชิง (Phishing) ทฤษฎีนี้สามารถอธิบายได้อย่างชัดเจน โดยเฉพาะในยุคดิจิทัลที่กระบวนการเรียนรู้ทางสังคมไม่ได้จำกัดอยู่เพียงในโลกจริง หากแต่ขยายสู่แพลตฟอร์มดิจิทัล เช่น กลุ่มใน Telegram, Discord, Dark Web หรือคลิปวิดีโอบน YouTube และ TikTok ซึ่งอาจเผยแพร่เทคนิคการหลอกลวงอย่างเปิดเผย ทำให้พฤติกรรมการกระทำผิดสามารถถ่ายทอดและเรียนรู้ได้รวดเร็วและกว้างขวางยิ่งขึ้น ทั้งนี้ บุคคลที่เริ่มต้นจากความอยากรู้อยากลอง หรือแม้เพียงการเข้าไปสังเกตการณ์ในกลุ่มที่สนับสนุนพฤติกรรมผิดกฎหมาย อาจนำไปสู่การซึมซับแนวคิดและพฤติกรรมผ่านกระบวนการเรียนรู้เชิงประสบการณ์ เช่น การสร้างเว็บไซต์ปลอมเลียนแบบธนาคาร การพัฒนาโปรแกรมหรือสคริปต์เพื่อหลอกขอรหัส OTP การจัดการข้อมูลของเหยื่อ การถอนเงินผ่านช่องทางต่าง ๆ หรือแม้แต่การซื้อขายบัญชีธนาคารของผู้อื่น (บัญชีม้า) เมื่อบุคคลมีปฏิสัมพันธ์บ่อยครั้ง กับกลุ่มที่มองว่าการกระทำผิดเป็นพฤติกรรมที่ยอมรับได้ ย่อมเพิ่มความเสี่ยงต่อการเกิดพฤติกรรมเลียนแบบ และอาจนำไปสู่การกลายเป็นส่วนหนึ่งของเครือข่ายอาชญากรรมทางไซเบอร์โดยไม่รู้ตัว **Sutherland และ Cressey (1996)** ระบุว่า การเรียนรู้พฤติกรรมอาชญากรไม่ได้จำกัดเพียงแค่ทักษะทางเทคนิคเท่านั้น แต่ยังครอบคลุมถึงการเรียนรู้เจตคติ แรงจูงใจ และเหตุผลที่สนับสนุนการกระทำผิด เช่น แนวคิดที่มองว่า “เหยื่อสมยอมเอง” หรือ “เป็นเพียงการหลอกลวงไม่ได้ใช้ความรุนแรง” ซึ่งกรอบความคิดเหล่านี้มีส่วนสำคัญในการลดทอนความรู้สึกผิดของผู้กระทำ และเพิ่มแนวโน้มที่จะตัดสินใจกระทำความผิดมากยิ่งขึ้น

กล่าวสรุปได้ว่า ในปัจจุบัน โลกออนไลน์มิได้เป็นเพียงพื้นที่สำหรับการแลกเปลี่ยนข้อมูลข่าวสารอย่างเสรีเท่านั้น หากแต่ได้กลายเป็นพื้นที่สำหรับการก่อให้เกิดชุมชนอาชญากรรมที่เอื้อต่อการเรียนรู้ และถ่ายทอดพฤติกรรมผิดกฎหมายได้อย่างรวดเร็ว ไร้พรมแดน การเข้าถึงกลุ่มที่ส่งเสริมพฤติกรรมฟิชชิงผ่านช่องทางดิจิทัลจึงไม่ใช่เรื่องยาก และมักนำไปสู่การก้าวเข้าสู่วงจรอาชญากรรมไซเบอร์ของบุคคลได้อย่างง่ายดายในบริบทของยุคดิจิทัล

ทฤษฎีข้อแก้ตัว (Neutralization Theory)

Sykes และ Matza (1957) ได้เสนอ ทฤษฎีข้อแก้ตัว (Techniques of Neutralization) โดยมีจุดมุ่งหมายเพื่ออธิบายว่า เหตุใดบุคคลจำนวนมากซึ่งโดยปกติแล้วยึดถือค่านิยมทางศีลธรรมและรู้ว่าการกระทำผิดเป็นสิ่งไม่ดี กลับสามารถตัดสินใจกระทำความผิดได้โดยไม่รู้สึกผิดหรือขัดแย้งกับจิตสำนึกของตนเอง ทั้งนี้ ผู้กระทำผิดมักใช้ข้อแก้ตัว (Neutralization Techniques) เพื่อลดแรงต้านภายในจิตใจ ทำให้การกระทำผิดของตนดูสมเหตุสมผลในสายตาของตนเองหรือแม้แต่ในสังคม และรูปแบบข้อแก้ตัวที่พบได้บ่อย ได้แก่ 1) การปฏิเสธความรับผิด โดยอ้างว่าไม่มีทางเลือก เช่น แค่เปิดบัญชีให้ผู้อื่น หรือกดส่งลิงก์ตามคำสั่งโดยไม่รู้ว่าผิดกฎหมาย 2) การปฏิเสธความเสียหาย เช่น มองว่าการกระทำไม่ร้ายแรง ไม่ได้ขโมยเงินเอง 3) การปฏิเสธการมีเหยื่อ เช่น มองว่าเหยื่อสมควรได้รับผลเพราะโลภหรือไม่ยอมฟังคำเตือน 4) การกล่าวโทษผู้อื่น เช่น โทษระบบธนาคาร แอปพลิเคชัน หรือการทำงานของเจ้าหน้าที่รัฐ และ 5) การยกเหตุผลด้านอุดมการณ์ เช่น ต้องหาเงินเลี้ยงดูครอบครัว ส่งลูกเรียน หรือรักษาคนในบ้าน เป็นต้น

จากการศึกษากรณีอาชญากรรมฟิชชิง พบว่า ผู้กระทำผิดมักใช้ข้อแก้ตัวเพื่อลดแรงกดดันทางศีลธรรมภายในจิตใจ ซึ่งช่วยให้การกระทำที่ผิดกฎหมายดูเหมือนเป็นสิ่งที่ยอมรับได้ โดยเฉพาะในบริบทของแรงกดดันทางเศรษฐกิจและสังคมที่ส่งผลต่อกระบวนการตัดสินใจ แม้ผู้กระทำผิดจะทราบดีว่าการกระทำนั้นผิดกฎหมาย แต่ข้อแก้ตัวเหล่านี้กลับทำหน้าที่เป็นกลไกทางจิตใจ ที่ช่วยลดความรู้สึกผิดและความขัดแย้งในตนเอง ทฤษฎีนี้จึงชี้ให้เห็นว่า เบื้องหลังของการโจมตีแบบฟิชชิงในหลายกรณี ไม่ได้เกี่ยวข้องเพียงแค่ทักษะหรือเทคนิคเท่านั้น แต่ยังเกี่ยวข้องกับกระบวนการคิดและการให้เหตุผลของผู้กระทำผิด ที่ทำให้พฤติกรรมผิดกฎหมายถูกมองว่าชอบธรรมชั่วคราวในมุมมองของผู้กระทำผิดเอง

ทฤษฎีการเปลี่ยนผ่านเชิงพื้นที่ (Space Transition Theory)

Karuppannan Jaishankar (2008) ได้นำเสนอทฤษฎี Space Transition Theory เพื่ออธิบายพฤติกรรมที่เปลี่ยนแปลงไปของบุคคลเมื่อเคลื่อนย้ายจากโลกแห่งความเป็นจริงเข้าสู่โลกไซเบอร์ ซึ่งเป็นพื้นที่ไร้พรมแดนมีลักษณะไม่ระบุตัวตน และเปลี่ยนแปลงอย่างรวดเร็ว โดยระบุว่าบุคคลอาจแสดงพฤติกรรมที่แตกต่างกันระหว่างสองบริบทนี้ ในกรณีของอาชญากรรมไซเบอร์ประเภทฟิชชิง (Phishing) ทฤษฎีดังกล่าวสามารถอธิบายได้ว่า บุคคลที่ไม่กล้ากระทำผิดในชีวิตจริง เช่น การหลอกลวงหรือการขอข้อมูลส่วนบุคคล อาจกล้ากระทำในโลกออนไลน์มากขึ้น เนื่องจากสามารถปกปิดตัวตน แอบอ้างเป็นบุคคลหรือหน่วยงานที่น่าเชื่อถือ และลดแรงกดดันทางสังคมหรือความกลัวต่อการถูกลงโทษได้ (Jaishankar, 2011)

กล่าวได้ว่า ทฤษฎีนี้อธิบายได้อย่างชัดเจนว่า โลกไซเบอร์กลายเป็นพื้นที่ใหม่ที่เอื้อต่อพฤติกรรมอาชญากรรมฟิชชิง โดยเฉพาะในกลุ่มบุคคลที่ไม่สามารถหรือไม่กล้ากระทำผิดในชีวิตจริง แต่พบว่าตนเองสามารถลงมือได้ง่ายขึ้นภายใต้การปกปิดตัวตนและขาดการควบคุมจากสังคม

แนวคิดทฤษฎีเกี่ยวกับสาเหตุของการตกเป็นเหยื่ออาชญากรรมไซเบอร์

การศึกษาพฤติกรรมของ “เหยื่อ” ถือเป็นองค์ประกอบสำคัญในการวิเคราะห์อาชญากรรมไซเบอร์ โดยเฉพาะกรณีฟิชชิง (Phishing) ที่เหยื่อมักถูกหลอกลวงให้เปิดเผยข้อมูลสำคัญของตนเองผ่านวิธีที่ดูเหมือนไม่เป็นอันตราย เช่น การคลิกลิงก์ในอีเมลปลอม หรือการกรอกข้อมูลผ่านเว็บไซต์เลียนแบบองค์กรทางการ ฟิชชิงจึงไม่ใช่อาชญากรรมที่เกิดจากตัวอาชญากรเพียงฝ่ายเดียว หากแต่เกี่ยวข้องกับพฤติกรรมของเหยื่อที่อาจเปิดช่องทางให้การกระทำผิดเกิดขึ้นได้เช่นกัน

ทฤษฎีกิจวัตรประจำวัน (Routine Activity Theory)

Cohen และ Felson (1979) ได้นำเสนอทฤษฎี **กิจวัตรประจำวัน (Routine Activity Theory)** โดยระบุว่าอาชญากรรมจะเกิดขึ้นได้เมื่อมีองค์ประกอบ 3 ประการ ได้แก่ (1) ผู้ที่มีแนวโน้มจะกระทำผิด, (2) เป้าหมายที่เหมาะสม และ (3) การขาดผู้พิทักษ์ที่มีประสิทธิภาพ

ในกรณีของอาชญากรรมไซเบอร์ประเภท **ฟิชชิง (Phishing)** ทฤษฎีนี้สามารถนำมาใช้ในการวิเคราะห์ได้อย่างเหมาะสม โดยผู้ใช้งานอินเทอร์เน็ตที่มีพฤติกรรมออนไลน์เป็นประจำ เช่น การใช้โซเชียลมีเดียอย่างต่อเนื่องหรือการทำธุรกรรมออนไลน์บ่อยครั้ง มักตกอยู่ในสถานะของ “เป้าหมายที่เหมาะสม” โดยเฉพาะเมื่อขาดการป้องกัน

ด้านความปลอดภัย เช่น การไม่ตั้งรหัสผ่านที่รัดกุม การไม่ตรวจสอบความถูกต้องของ URL หรือการคลิกลิงก์จากแหล่งที่ไม่น่าเชื่อถือ ซึ่งล้วนเป็นช่องโหว่ที่ผู้กระทำผิดสามารถใช้เป็นจุดเริ่มต้นในการโจมตีทางไซเบอร์ ไม่ว่าจะเป็นการเปิดเผยข้อมูลในที่สาธารณะ การคลิกลิงก์โดยไม่ตรวจสอบแหล่งที่มา หรือการดาวน์โหลดไฟล์จากอีเมลที่ไม่น่าเชื่อถือ ล้วนสะท้อนถึงการขาดผู้พิทักษ์ที่มีประสิทธิภาพ ซึ่งเป็นองค์ประกอบสำคัญประการหนึ่งในทฤษฎีกิจวัตรประจำวัน และเป็นปัจจัยที่เอื้อต่อการเกิดอาชญากรรมไซเบอร์ประเภทฟิชชิงได้อย่างชัดเจน

แนวคิดเกี่ยวกับแนวทางการป้องกันอาชญากรรมไซเบอร์

ทฤษฎีการบังคับใช้กฎหมาย (Law Enforcement Theory) เป็นแนวคิดทางอาชญาวิทยาที่เน้นบทบาทของรัฐในการควบคุม ป้องกัน และปราบปรามอาชญากรรมผ่านกระบวนการทางกฎหมายอย่างมีประสิทธิภาพ (Grabosky, 2001) โดยมุ่งหวังให้สังคมมีความสงบเรียบร้อย และสามารถยับยั้งพฤติกรรมที่ผิดกฎหมายได้ ทั้งในเชิงป้องปรามและการดำเนินคดีกับผู้กระทำผิด ในบริบทของอาชญากรรมไซเบอร์ที่มีลักษณะไร้พรมแดนและเปลี่ยนแปลงอย่างรวดเร็ว โดยเฉพาะการโจมตีแบบฟิชชิง ซึ่งส่งผลกระทบต่อประชาชนอย่างกว้างขวาง การบังคับใช้กฎหมายจึงต้องปรับตัวให้ทันกับภัยคุกคามรูปแบบใหม่ ทั้งด้านองค์ความรู้ เทคโนโลยี และแนวทางปฏิบัติ (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2566) ทฤษฎีนี้สนับสนุนแนวทางเชิงรุกของเจ้าหน้าที่รัฐในการลดความเสี่ยงของการตกเป็นเหยื่อฟิชชิง โดยผ่านกลไกหลัก 3 ประการ ได้แก่

1. **การป้องกันเชิงรุก** ได้แก่ หน่วยงานที่เกี่ยวข้องควรติดตามภัยคุกคามอย่างใกล้ชิด เช่น เฝ้าระวังเว็บไซต์ต้องสงสัย แจ้งเตือนประชาชน และร่วมมือกับภาคเอกชน
2. **การสืบสวนและดำเนินคดีอย่างมีประสิทธิภาพ** ต้องอาศัยความเชี่ยวชาญด้านนิติวิทยาศาสตร์ดิจิทัล การวิเคราะห์ข้อมูล และการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ที่ถูกต้องตามกฎหมาย เพื่อให้สามารถดำเนินคดีได้อย่างมั่นคงและโปร่งใส
3. **การป้องปรามผ่านบทลงโทษที่ชัดเจน** ถือเป็นการลงโทษผู้กระทำผิดอย่างเด็ดขาด ช่วยลดแรงจูงใจในการก่อเหตุ และการประชาสัมพันธ์ผลการจับกุมหรือการดำเนินคดีมีส่วนเสริมสร้างความกลัวต่อกฎหมาย

กล่าวโดยสรุป การนำแนวคิดทฤษฎีการบังคับใช้กฎหมายมาใช้ในการวางยุทธศาสตร์ป้องกันอาชญากรรมไซเบอร์ โดยเฉพาะการตกเป็นเหยื่อฟิชชิง เป็นแนวทางที่มีความจำเป็นอย่างยิ่งในยุคที่ภัยคุกคามเปลี่ยนแปลงรวดเร็วและซับซ้อน เจ้าหน้าที่ตำรวจจึงต้องมีบทบาทมากกว่าการปราบปราม คือ เป็นผู้สร้างกลไกเชิงป้องกันในระดับสังคม พร้อมทั้งรักษาสมดุลระหว่างการบังคับใช้กฎหมายอย่างเด็ดขาดกับการคุ้มครองสิทธิของเหยื่ออย่างเหมาะสม

ทฤษฎีการป้องกัน (Defense หรือ Deterrence Theory)

ทฤษฎีการป้องกันอาชญากรรม หรือที่รู้จักกันทั่วไปในชื่อ **ทฤษฎียับยั้ง (Deterrence Theory)** เป็นแนวคิดพื้นฐานในศาสตร์อาชญาวิทยา ซึ่งมุ่งเน้นการป้องกันไม่ให้อาชญากรรมเกิดขึ้นตั้งแต่ต้นทางการแก้ไขภายหลัง โดยเชื่อว่าการลงโทษผู้กระทำผิดอย่างชัดเจน เด็ดขาด และทันเวลา จะทำให้ผู้ที่มีแนวโน้มจะกระทำผิดเกิดความกลัวต่อผลที่จะตามมา และเลือกจะไม่ลงมือกระทำความผิดในที่สุด (Beccaria, 1764 อ้างใน Siegel, 2015)

ทั้งนี้ในบริบทของอาชญากรรมไซเบอร์ โดยเฉพาะการโจมตีแบบฟิชชิง ทฤษฎีนี้มีบทบาทสำคัญในการออกแบบมาตรการป้องกัน โดยมุ่งเน้นการใช้กลไกความกลัวต่อกฎหมายเป็นเครื่องมือขัดขวางพฤติกรรมของอาชญากร เช่น การเผยแพร่ผลการจับกุมคดีฟิชชิง การประกาศบทลงโทษในกรณีการใช้บัญชีม้า หรือการเข้าถึงข้อมูลโดยมิชอบผ่านทางแอปพลิเคชันปลอม การที่ประชาชนรับรู้ว่าการกระทำเหล่านี้มีโทษรุนแรงและมีแนวโน้มสูงที่จะถูกติดตามจับกุมได้ จะช่วยสร้างแรงยับยั้งเชิงจิตวิทยาให้กับผู้ที่คิดจะกระทำผิด (Paternoster, 2010)

กล่าวโดยสรุป **Deterrence Theory** ถือเป็นแนวคิดที่สามารถนำมาประยุกต์ใช้กับการป้องกันอาชญากรรมไซเบอร์ยุคใหม่ได้อย่างสอดคล้อง โดยเฉพาะในกรณีของฟิชชิง ซึ่งผู้กระทำผิดมักใช้วิธีการแฝงตัว ปกปิดตัวตน และเล็งเป้าหมายไปยังผู้ที่ไม่มีภูมิคุ้มกันทางเทคโนโลยี การใช้บทลงโทษอย่างชัดเจน การดำเนินคดีอย่างรวดเร็ว และการประชาสัมพันธ์ให้ประชาชนรู้เท่าทัน จึงเป็นแนวทางที่สะท้อนจิตวิญญาณของทฤษฎีนี้อย่างแท้จริง ทั้งในมิติของการยับยั้งผู้กระทำผิด และการป้องกันไม่ให้ประชาชนตกเป็นเหยื่อ

ทฤษฎีชุมชนสัมพันธ์ (Community Relations Approach)

แนวคิดด้านสิ่งแวดล้อมทางอาชญาวิทยา (The Ecological School of Criminology) เป็นหนึ่งในทฤษฎีที่มีรากฐานมาจากการศึกษาของสำนักชิคาโก (Chicago School) ซึ่งเชื่อว่า **อาชญากรรมสามารถควบคุมได้จากภายในชุมชน** โดยไม่จำเป็นต้องพึ่งพาหน่วยงานรัฐเพียงอย่างเดียว (Shaw & McKay, 1942) ทฤษฎีนี้เสนอว่าโครงสร้างทางสังคม เช่น ความสัมพันธ์ระหว่างเพื่อนบ้าน ความไว้วางใจ และการมีส่วนร่วมทางสังคม มีอิทธิพลต่อระดับการเกิดอาชญากรรมในพื้นที่อย่างมีนัยสำคัญ เมื่อประยุกต์แนวคิดดังกล่าวเข้าสู่บริบทของ **อาชญากรรมไซเบอร์** โดยเฉพาะการหลอกลวงแบบ **ฟิชชิง (Phishing)** จะพบว่า “ชุมชนออนไลน์” หรือ “เครือข่ายผู้ใช้งาน” ต่างก็สามารถทำหน้าที่คล้ายคลึงกับชุมชนในโลกแห่งความเป็นจริง กล่าวคือ หากประชาชนสามารถเชื่อมโยงและร่วมมือกับเจ้าหน้าที่รัฐโดยเฉพาะตำรวจไซเบอร์ ในการสอดส่องพฤติกรรมต้องสงสัย แจ้งเตือนกันเอง หรือแชร์ข้อมูลภัยคุกคามล่าสุด ก็จะเป็นการยกระดับกลไกการป้องกันอาชญากรรมได้โดยไม่ต้องรอการเข้ามาแทรกแซงจากรัฐแต่เพียงฝ่ายเดียว (Sampson, Raudenbush, & Earls, 1997)

แนวคิดข้างต้นสามารถเชื่อมโยงได้อย่างชัดเจนกับ **ทฤษฎีการเปลี่ยนผ่านในพื้นที่ไซเบอร์ (Space Transition Theory)** ของ Jaishankar (2008) ซึ่งเสนอว่า พฤติกรรมของคนในโลกไซเบอร์มักเปลี่ยนไปจากพฤติกรรมในโลกจริง เนื่องจากพื้นที่ออนไลน์มีลักษณะเปิดกว้าง ขาดโครงสร้างควบคุมที่เข้มแข็ง และเอื้อให้ผู้ใช้งานสามารถปกปิดตัวตนหรือทดลองพฤติกรรมใหม่ ๆ ได้โดยไม่ต้องรับผลกระทบในทันที จากมุมมองของ Space Transition Theory การที่ผู้กระทำผิดสามารถแฝงตัวภายใต้นามแฝง (anonymous) หรือซ่อนพฤติกรรมหลอกลวงไว้ในเว็บไซต์ปลอม แอปพลิเคชันเลียนแบบ หรือบัญชีโซเชียลมีเดียที่ดูน่าเชื่อถือ ย่อมส่งผลให้ผู้ใช้งานที่ขาดความรู้เท่าทันกลายเป็นเหยื่อได้อย่างง่ายดาย โดยเฉพาะในสถานการณ์ที่เกิดความเร่งรีบ ตกใจ หรือหลงเชื่อในบุคคลที่แอบอ้าง

กล่าวโดยสรุป การประยุกต์ใช้แนวคิดจาก The Ecological School of Criminology และ Space Transition Theory ช่วยขยายแนวทางการป้องกันอาชญากรรมไซเบอร์ให้ครอบคลุมทั้งในมิติของโครงสร้างทางสังคมและพฤติกรรมเชิงดิจิทัล ซึ่งล้วนมีบทบาทสำคัญในการลดความเสี่ยงของการตกเป็นเหยื่อ โดยเฉพาะในยุคที่ภัยฟิชชิงสามารถเข้าถึงผู้ใช้งานได้แทบทุกช่วงเวลาและทุกอุปกรณ์ที่เชื่อมต่ออินเทอร์เน็ต

งานวิจัยที่เกี่ยวข้อง

การศึกษาภัยคุกคามจากอาชญากรรมไซเบอร์ โดยเฉพาะรูปแบบการโจมตีแบบฟิชชิง (Phishing) เป็นประเด็นที่ได้รับความสนใจอย่างต่อเนื่องในวงวิชาการทั้งในระดับนโยบายและพฤติกรรมปัจเจก งานวิจัยหลายชิ้นได้เสนอข้อค้นพบที่สามารถเชื่อมโยงกับการศึกษาในครั้งนี้ ทั้งในด้านพฤติกรรมของผู้กระทำผิด วิธีการก่อเหตุ และปัจจัยของเหยื่อที่เปิดช่องให้เกิดอาชญากรรม โดยสามารถสรุปสาระสำคัญของงานวิจัยที่เกี่ยวข้องได้ดังนี้

จิรวัฒน์ มหรรณพ (2564) ศึกษาการแพร่กระจายของความรู้และเครื่องมือทางอาชญากรรมไซเบอร์ในกลุ่มออนไลน์ เช่น Telegram, Discord และ ใน Dark Web ซึ่งพบว่า กลุ่มเหล่านี้เป็นพื้นที่แลกเปลี่ยนเทคนิคการก่อเหตุฟิชชิงอย่างกว้างขวาง ไม่ว่าจะเป็นการเขียนสคริปต์หลอกลวง การปลอมแปลงเว็บไซต์ หรือแม้แต่การจัดหา “บัญชีม้า” เพื่อใช้รับเงินจากเหยื่อ ซึ่งสอดคล้องกับผลการศึกษาในบทความนี้ที่ชี้ให้เห็นว่า ผู้กระทำผิดส่วนหนึ่งไม่ได้มีพื้นฐานทางเทคนิคสูง แต่สามารถเรียนรู้วิธีการกระทำผิดได้จากแหล่งออนไลน์เหล่านี้

ธีรยุทธ สุคนธ์ (2566) พบว่า แพลตฟอร์มโซเชียลมีเดีย เช่น Facebook และ LINE ถูกใช้เป็นเครื่องมือหลักในการแอบอ้างตัวตนเพื่อหลอกเหยื่อ โดยการดึงข้อมูลจากโพสต์สาธารณะ เช่น ชื่อ เบอร์โทร ตำแหน่งงาน หรือกิจกรรมที่กำลังทำ เพื่อสร้างข้อความที่ดูน่าเชื่อถือและตรงกับบริบทชีวิตจริงของเหยื่อ จุดนี้สะท้อนกับการศึกษาครั้งนี้ที่พบว่าการโจมตีแบบ Spear Phishing และ Angler Phishing ในประเทศไทยมีการปรับเนื้อหาตามข้อมูลส่วนตัวของเหยื่ออย่างแนบเนียน

ในมิติของพฤติกรรมผู้ใช้งาน **สกาวเดือน แสงสุวรรณ (2565)** ได้ศึกษาความเปราะบางของกลุ่มผู้สูงวัยในการใช้เทคโนโลยี โดยพบว่าเหยื่อส่วนใหญ่มักเชื่อถือข้อความจากหน่วยงานที่ดูน่าเชื่อถือ และไม่สามารถแยกแยะ URL ปลอมจากจริงได้ โดยเฉพาะในสถานการณ์ที่ถูกกระตุ้นด้วยความกลัวหรือเร่งด่วน เช่น การถูกแจ้งว่าบัญชีจะถูกระงับหากไม่ยืนยันตัวตนภายใน 15 นาที ซึ่งตรงกับรูปแบบ Vishing และ Smishing ที่พบในกรณีศึกษาของบทความนี้

นอกจากนี้ **นภัสสร เรืองรอง (2563)** ยังระบุว่า กลุ่มเยาวชนและผู้ใช้งานทั่วไปที่มีทักษะรู้เท่าทันดิจิทัลต่ำมักตกเป็นเหยื่อของฟิชชิงที่แฝงมาในรูปแบบของโพรโมชัน หรือของรางวัล เช่น ลิงก์ให้กรอกข้อมูลเพื่อรับสิทธิ์ลดราคาหรือของแจกฟรี ซึ่งเป็นเทคนิคที่พบได้บ่อยในกรณี Angler Phishing และ Search Engine Phishing ที่กล่าวถึงในบทความนี้

ในด้านแนวทางเชิงนโยบาย **ปรัชญา พิพัฒน์พงศ์ (2562)** ได้ศึกษาการตอบสนองของภาครัฐต่ออาชญากรรมไซเบอร์ และเสนอให้มีการจัดตั้งเครือข่าย “อาสาสมัครดิจิทัล” เพื่อให้ประชาชนมีบทบาทในการเฝ้าระวังภัยไซเบอร์ร่วมกับหน่วยงานรัฐ ซึ่งสอดคล้องกับข้อเสนอของบทความนี้ที่ชี้ว่า ชุมชนออนไลน์สามารถมีบทบาทสำคัญในการแจ้งเตือนภัยและร่วมป้องกันอาชญากรรมได้ หากได้รับการส่งเสริมและเชื่อมโยงอย่างเหมาะสม

จากงานวิจัยที่กล่าวมาข้างต้น จะเห็นได้ว่า มีความสอดคล้องอย่างมีนัยสำคัญกับผลการศึกษาครั้งนี้ โดยเฉพาะในมิติของพฤติกรรมผู้กระทำผิด การใช้ช่องทางดิจิทัลในการก่อเหตุ และพฤติกรรมของเหยื่อที่ขาดความรู้เท่าทันภัยไซเบอร์ การหยิบยกงานวิจัยเหล่านี้มาประกอบการอภิปรายผล จึงมีส่วนช่วยยืนยันความถูกต้องของผลการศึกษาและแสดงให้เห็นถึงความเป็นไปได้ในการนำข้อค้นพบไปใช้ประโยชน์ต่อยอดในทางนโยบายและการป้องกัน

วิธีการดำเนินการวิจัย

การศึกษาวิจัยในครั้งนี้เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) โดยใช้วิธีการวิเคราะห์เนื้อหา (Content Analysis) เป็นกรอบแนวทางหลักในการรวบรวม วิเคราะห์ และตีความข้อมูลจากแหล่งข้อมูลทุติยภูมิ (Secondary Data) โดยเน้นการสังเคราะห์องค์ความรู้จากเอกสารทางวิชาการ บทความวิจัย รายงานของหน่วยงานภาครัฐและเอกชน รวมถึงข่าวสารจากสื่อมวลชนที่มีความน่าเชื่อถือ ซึ่งเกี่ยวข้องกับกรณีการโจมตีแบบฟิชชิง (Phishing Attacks) ที่เกิดขึ้นในประเทศไทย

ทั้งนี้ การเลือกกรณีศึกษา (Case Selection) เป็นไปตามหลักเกณฑ์การเลือกแบบมีจุดมุ่งหมาย (Purposive Sampling) โดยเน้นเหตุการณ์ที่มีความชัดเจนของรูปแบบการกระทำความผิด รวมถึงถูกเผยแพร่ในแหล่งข้อมูลที่น่าเชื่อถือ เช่น สื่อกระแสหลัก ฐานข้อมูลข่าวออนไลน์ งานวิจัย และรายงานหน่วยงานที่มีความน่าเชื่อถือ เพื่อให้ครอบคลุมสถานการณ์ภัยคุกคามในบริบทร่วมสมัยของยุคดิจิทัล โดยการวิเคราะห์ข้อมูลใช้กระบวนการถอดความ (Transcription) เพื่อหาความเชื่อมโยงระหว่างรูปแบบการกระทำผิด พฤติกรรมของเหยื่อ และประสิทธิภาพของการบังคับใช้กฎหมาย อันจะนำไปสู่ข้อเสนอแนะแนวทางในการป้องกันภัยคุกคามอาชญากรรมไซเบอร์ประเภทฟิชชิงได้อย่างมีประสิทธิภาพ

ผลการวิจัย

1. รูปแบบของภัยคุกคามการโจมตีแบบฟิชชิงในประเทศไทย

จากผลการศึกษา พบว่า การโจมตีแบบฟิชชิงในประเทศไทยมีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง ซึ่งสอดคล้องกับพฤติกรรมของประชาชนที่เปลี่ยนผ่านเข้าสู่โลกออนไลน์มากยิ่งขึ้น ไม่ว่าจะเป็นการทำธุรกรรมทางการเงิน การซื้อขายสินค้าและบริการผ่านแพลตฟอร์มดิจิทัล ตลอดจนการใช้บริการภาครัฐในรูปแบบอิเล็กทรอนิกส์ การโจมตีแบบฟิชชิงจึงทวีความถี่และมีความซับซ้อนมากยิ่งขึ้น โดยผู้กระทำผิดมีการพัฒนาเทคนิคให้แนบเนียน และยากต่อการตรวจจับด้วยวิธีการทั่วไป จากการวิเคราะห์ข้อมูล พบว่า รูปแบบการโจมตีแบบฟิชชิงในบริบทของประเทศไทยสามารถจำแนกได้เป็น 8 รูปแบบหลัก ได้แก่

1) Email Phishing เป็นรูปแบบฟิชชิงที่พบได้มากที่สุด โดยผู้กระทำผิดจะส่งอีเมลปลอมที่แอบอ้างว่าเป็นหน่วยงานหรือองค์กรที่มีความน่าเชื่อถือ เช่น ธนาคาร บริษัทเทคโนโลยี บริษัทขนส่ง หรือหน่วยงานของรัฐ อีเมลมักประกอบด้วยข้อความที่สร้างสถานการณ์เร่งด่วน เช่น “บัญชีของคุณถูกระงับชั่วคราว”, “ตรวจพบการเข้าสู่ระบบจากต่างประเทศ” หรือ “กรุณายืนยันตัวตนภายใน 24 ชั่วโมง” พร้อมแนบลิงก์ที่ปลอมแปลงให้มีหน้าตาคล้ายเว็บไซต์จริงของหน่วยงานเหล่านั้น เมื่อเหยื่อคลิกที่ลิงก์ จะเข้าสู่เว็บไซต์ที่มีแบบฟอร์มให้กรอกข้อมูลส่วนตัว เช่น ชื่อผู้ใช้ รหัสผ่าน เลขบัตรประชาชน หรือ OTP เมื่อกรอกข้อมูลเสร็จ ข้อมูลเหล่านี้จะถูกส่งไปยังคนร้ายทันที และอาจถูกใช้เพื่อเข้าสู่ระบบจริงของธนาคารหรือแพลตฟอร์มออนไลน์ เพื่อขโมยทรัพย์สินหรือข้อมูล ตัวอย่างเหตุการณ์ที่เกิดขึ้นจริงเมื่อปี พ.ศ.2566 ผู้ใช้งานอีเมลจำนวนมากได้รับอีเมลปลอมแอบอ้างเป็น “KBank Official” โดยมีหัวข้อเร่งด่วน เช่น

“บัญชีถูกระงับ” พร้อมแนบลิงก์ปลอมที่หน้าตาเหมือนเว็บไซต์ธนาคารกสิกรไทย (เช่น kbank-th-hecksecure.com) เมื่อเหยื่อกรอกข้อมูลและ OTP คนร้ายจะนำไปเข้าสู่ระบบ K PLUS และโอนเงินออกทันที เช่นในกรณีชายวัย 38 ปี ในกรุงเทพฯ ที่สูญเงินกว่า 85,000 บาท ภายใน 30 นาที อีเมลดังกล่าวส่งมาจากเซิร์ฟเวอร์ต่างประเทศ **หน่วยงาน ThaiCERT และธนาคาร** ได้ออกประกาศเตือน พร้อมแนะนำให้ประชาชนหลีกเลี่ยงการคลิกลิงก์จากอีเมลที่น่าสงสัย เป็นต้น และจากการศึกษาพบว่า **กลุ่มเป้าหมายของ Email Phishing** ส่วนใหญ่คือผู้ใช้ทั่วไปที่ใช้อีเมลในการทำธุรกรรมออนไลน์ เช่น การเข้าสู่ระบบธนาคาร, อีคอมเมิร์ซ, หรือบริการภาครัฐ โดยเฉพาะช่วงอายุ **25 - 45 ปี** ซึ่งเป็นกลุ่มที่มีพฤติกรรมออนไลน์สูง และมักมีบัญชีเงินเดือนหรือระบบชำระเงินดิจิทัล

2) Spear Phishing เป็นรูปแบบการโจมตีทางไซเบอร์ที่มุ่งเป้าแบบเฉพาะเจาะจง (Targeted Attack) โดยคนร้ายจะใช้วิธีการ **เก็บรวบรวมข้อมูลของเหยื่อ** จากแหล่งต่าง ๆ เช่น โซเชียลมีเดีย (LinkedIn, Facebook), เว็บไซต์บริษัท, รายชื่อพนักงานในเอกสารประชาสัมพันธ์ หรือแม้แต่ข้อมูลจากการรั่วไหลของระบบฐานข้อมูลออนไลน์ จากนั้นคนร้ายจะออกแบบอีเมลหรือข้อความให้ดูเหมือนเป็นการติดต่อจากบุคคลที่เหยื่อรู้จัก เช่น หัวหน้าในที่ทำงาน เพื่อนร่วมโครงการ หรือคู่ค้าทางธุรกิจ โดยใช้น้ำเสียงและเนื้อหาที่สมจริง อีเมลมักแนบไฟล์เอกสาร เช่น .pdf, .docx หรือ .xls ที่ฝังมัลแวร์ไว้ หรือมีลิงก์ปลอมที่เมื่อคลิกแล้วจะติดตั้ง Remote Access Trojan (RAT) หรือดึงข้อมูลสำคัญออกจากเครื่องเหยื่อ ตัวอย่างเหตุการณ์ที่เกิดขึ้นจริง เมื่อปี พ.ศ.2565 มีพนักงานการเงินของบริษัทเทคโนโลยีในกรุงเทพฯ ได้รับอีเมลจากผู้บริหารฝ่ายบัญชีของบริษัทในต่างประเทศ โดยเป็นอีเมลที่เขียนอย่างเป็นทางการ ใช้ชื่อที่ถูกต้อง และแนบไฟล์เอกสารเกี่ยวกับ “แผนการโอนเงินระหว่างบริษัท” ซึ่งเป็นเรื่องที่อยู่ในขอบเขตงานของผู้รับ และเมื่อเปิดไฟล์และกรอกพาสเวิร์ดเพื่อดูเอกสาร (ตามคำแนะนำในอีเมล) เครื่องของเหยื่อก็ถูกมัลแวร์เจาะระบบและดึงรหัสผ่านของระบบบัญชีออกไป จากนั้นมีการพยายามโอนเงินออกจากบัญชีบริษัทภายในไม่กี่ชั่วโมงถัดมา เคราะห์ดีที่ฝ่ายตรวจสอบบัญชีของสำนักงานใหญ่สังเกตเห็นความผิดปกติและระงับธุรกรรมได้ทันเวลา **โดยจากการศึกษา พบว่า กลุ่มเป้าหมายของ Spear Phishing** ได้แก่ พนักงานบริษัทระดับกลางขึ้นไป เจ้าหน้าที่รัฐ หรือบุคลากรฝ่ายการเงิน ที่มีอำนาจเข้าถึงระบบภายในหรือข้อมูลสำคัญขององค์กร

3) Whaling Phishing เป็นการโจมตีทางไซเบอร์ที่เจาะจงกลุ่มผู้บริหารระดับสูงขององค์กร เช่น ผู้อำนวยการฝ่ายบัญชีและการเงิน เป็นต้น โดยใช้เทคนิควิศวกรรมสังคม (Social Engineering) ที่มีความซับซ้อนสูง และออกแบบเนื้อหาให้เหมาะสมกับตำแหน่งหน้าที่ของเหยื่อโดยเฉพาะ อีเมลมักถูกเขียนให้มี ภาษาทางธุรกิจที่เป็นทางการ, มีรายละเอียดที่เฉพาะเจาะจงเกี่ยวกับองค์กร และมีลักษณะเร่งด่วน เช่น “ขอให้คุณตรวจสอบและอนุมัติเอกสารบัญชีที่แนบภายในวันนี้อย่างเป็นความลับ” หรือ “มีเอกสารจากหน่วยงานกำกับดูแล ขอให้คุณดูรายละเอียดในไฟล์แนบโดยด่วน” ภายในอีเมลมักแฝงลิงก์ปลอม หรือแนบไฟล์เอกสารที่ฝังมัลแวร์ เมื่อเหยื่อเปิดไฟล์ ระบบขององค์กรอาจถูกดึงข้อมูลออกไปโดยไม่รู้ตัว ตัวอย่างเหตุการณ์ที่เกิดขึ้นจริง กล่าวคือ ในช่วง ปี พ.ศ. 2565 มีการรายงานจากหลายจังหวัดว่ามีข้าราชการในสำนักงานจังหวัดต่าง ๆ ได้รับอีเมลจากผู้ที่ปลอมชื่อและที่อยู่อีเมลให้เหมือนเป็น “ผู้ว่าราชการจังหวัด” โดยมีเนื้อหาขอให้ **อนุมัติงบประมาณเร่งด่วน** เพื่อจัดซื้ออุปกรณ์หรือครุภัณฑ์ เช่น คอมพิวเตอร์โน้ตบุ๊ก และเครื่องมือทางการแพทย์ พร้อมแนบไฟล์ที่มีข้อมูลบัญชีธนาคารของ “ผู้จัดจำหน่าย” ซึ่งเป็นปลายทางของคนร้าย แม้อีเมลดังกล่าวเขียนด้วยภาษาทางการ ใช้รูปแบบลายเซ็นและตำแหน่งคล้ายของจริง และมีหัวเรื่องว่า “เรื่องเร่งด่วน - อนุมัติการดำเนินการจัดซื้อเพื่อสนับสนุนภารกิจส่วนกลาง” มีเจ้าหน้าที่บางรายเกือบดำเนินการอนุมัติตามคำสั่ง แต่พบความผิดปกติ เช่น ที่อยู่อีเมลที่ลงท้ายด้วย @gmail.com แทนที่จะเป็นอีเมลทางราชการ และเอกสารแนบไม่มีเลขที่หนังสือราชการหรือลายเซ็นรับรอง จึงแจ้งเตือนและรายงานไปยังหน่วยงานระดับจังหวัดและ **กระทรวงมหาดไทย**

กรณีนี้แสดงให้เห็นถึงการใช้เทคนิค Whaling Phishing กับกลุ่มเป้าหมายระดับ “ข้าราชการระดับกลาง-สูง” โดยอาศัยความเคารพในลำดับชั้นการสั่งงานของระบบราชการ เพื่อเร่งรัดให้เจ้าหน้าที่ดำเนินการอนุมัติรายการที่ผิดปกติโดยไม่ตรวจสอบให้รอบคอบ และจากการศึกษาพบว่า**กลุ่มเป้าหมายของการโจมตีครั้งนี้** คือ ข้าราชการหรือเจ้าหน้าที่พัสดุ-การเงิน ในสำนักงานจังหวัด หรือหน่วยงานราชการ ที่มีหน้าที่อนุมัติงบประมาณ โดยเฉพาะระดับหัวหน้างาน อายุ 35 - 55 ปี

4) Smishing เป็นการโจมตีผ่านข้อความ SMS โดยผู้กระทำผิดจะส่งข้อความสั้นที่ปลอมตัวเป็นหน่วยงานที่ประชาชนรู้จักและไว้วางใจ เช่น ธนาคาร บริษัทขนส่ง ร้านค้าออนไลน์ หรือหน่วยงานของรัฐ โดยมักอ้างเหตุผลเร่งด่วน เช่น **“พบการใช้จ่ายผิดปกติในบัญชีของคุณ”**, **“พัสดุของคุณถูกระงับ”** หรือ **“กรุณายืนยันตัวตนภายใน** 24 **ชั่วโมง”** พร้อมแนบลิงก์ปลอมให้คลิกเพื่อกรอกข้อมูลส่วนตัว เช่น เลขบัตรประชาชน หมายเลขบัตร ATM รหัส OTP หรือข้อมูลเข้าสู่ระบบของแอปธนาคารเนื้อความใน SMS มักสั้น กระชับ และมีการใช้ถ้อยคำที่ก่อให้เกิดความตกใจ เช่น “ด่วน!”, “บัญชีของคุณถูกล็อก”, หรือ “มีรายการต้องยืนยัน” เพื่อกระตุ้นให้เหยื่อคลิกลิงก์และตอบสนองโดยไม่ทันพิจารณาตัวอย่างเหตุการณ์ที่เกิดขึ้นจริง กล่าวคือในห้วง พ.ศ. 2566 มีผู้เสียหายจำนวนมากในเขตกรุงเทพมหานครและปริมณฑลได้รับข้อความ SMS ที่แอบอ้างว่าเป็นของธนาคารโดยมีเนื้อความว่า“บัญชีของคุณถูกระงับชั่วคราว กรุณายืนยันตัวตนทันทีโดยมีการแนบลิงก์เว็บไซต์มาพร้อมข้อความด้วย ซึ่งเว็บไซต์ดังกล่าวเป็นเว็บไซต์ปลอมที่มีหน้าตาคล้ายแอปพลิเคชัน K PLUS ของธนาคารจริง เมื่อผู้ใช้งานกรอกหมายเลขบัตรประชาชน รหัส PIN และ OTP ที่ได้รับใน SMS จริง ๆ คนร้ายจะนำข้อมูลไปเข้าสู่บัญชีของเหยื่อและทำธุรกรรมโอนเงินออกทันที ผู้เสียหายหลายรายสูญเงินตั้งแต่หลักพันจนถึงหลักแสนบาท โดยหนึ่งในนั้นเป็นหญิงวัย 34 ปี สูญเงินกว่า**หลักแสนบาท** ภายในเวลา 15 นาทีหลังจากกรอกข้อมูล เนื่องจากคนร้ายใช้ระบบโอนเงินรวดเร็วแบบพร้อมเพย์ และโอนต่อไปยังบัญชีปลายทางหลายชั้นอย่างรวดเร็ว ทำให้ติดตามได้ยาก จากการศึกษาพบว่า **กลุ่มเป้าหมายของ Smishing** ส่วนใหญ่เป็นผู้ใช้งานโทรศัพท์มือถือที่มีแอปธนาคาร โดยเฉพาะผู้ที่มีอายุ **30 ปีขึ้นไป** ซึ่งมักมีบัญชีเงินเดือน บัญชีออมทรัพย์และทำธุรกรรมออนไลน์เป็นประจำ

5) Vishing เป็นเทคนิคที่ผู้กระทำผิดใช้ การโทรศัพท์หลอกลวง โดยปลอมตัวเป็นเจ้าหน้าที่ของหน่วยงานรัฐ ธนาคาร บริษัทเอกชน หรือแม้แต่เจ้าหน้าที่ตำรวจหรือเจ้าหน้าที่ศาล มักอ้างว่าเหยื่อมีความเกี่ยวข้องกับคดีอาญา เช่น การฟอกเงิน การเปิดบัญชีม้า หรือมีหมายจับออกในระบบ ซึ่งสร้างความตกใจให้กับเหยื่อ จนนำไปสู่การโอนเงินเพื่อ “พิสูจน์ความบริสุทธิ์” หรือการให้รหัส OTP เพื่อเข้าถึงบัญชีธนาคารหรือแอปพลิเคชันทางการเงิน ผู้กระทำผิดมักปลอมหมายเลขโทรศัพท์ ตัวตนให้ดูเหมือนว่ามาจากหน่วยงานราชการจริง เช่น เบอร์สำนักงานตำรวจแห่งชาติ เบอร์ธนาคาร หรือเบอร์ศาล เพื่อเพิ่มความน่าเชื่อถือ และเร่งรัดให้เหยื่อตอบสนองทันที เช่น การยืนยันตัวตนภายใน 5 นาที หรือการโอนเงินเข้าบัญชีที่อ้างว่าเป็น “บัญชีกลางของศาล” ตัวอย่างเหตุการณ์ที่เกิดขึ้นจริง ในห้วงปี พ.ศ. 2566 มีผู้เสียหายรายหนึ่งอายุ 62 ปี อาศัยอยู่ในจังหวัดนครราชสีมา ได้รับโทรศัพท์จากบุคคลที่แอบอ้างว่าเป็นเจ้าหน้าที่จากกรมสอบสวนคดีพิเศษ (DSI) แจ้งว่าเธอมีชื่อพัวพันกับการฟอกเงินจากบัญชีม้าในจังหวัดเชียงรายและหากไม่โอนเงินเข้าบัญชีเพื่อให้ “ศาลตรวจสอบเส้นทางการเงิน” จะมีหมายจับออกภายในวันเดียวกัน ผู้เสียหายตื่นตระหนกและโอนเงินทั้งหมดที่มีอยู่ในบัญชีจำนวน 450,000 บาท ภายในเวลาไม่ถึงชั่วโมง โดยอ้างว่าได้รับคำแนะนำให้ “ยุติการติดต่อกับผู้อื่น” และอย่าบอกข้อมูลกับใครเพราะอยู่ใน “ขั้นตอนลับของกระบวนการยุติธรรม” ต่อมาจึงทราบว่าถูกหลอกลวงจากข่าวเตือนภัยของสำนักงานตำรวจแห่งชาติ จึงเข้าร้องทุกข์ต่อเจ้าพนักงานตำรวจ

จากการศึกษากลุ่มเป้าหมายที่ตกเป็นเหยื่อส่วนใหญ่มักเป็น ผู้สูงอายุ หรือบุคคลที่ไม่คุ้นเคยกับเทคโนโลยีดิจิทัล เช่น ผู้ที่ไม่ได้ใช้อินเทอร์เน็ตเป็นประจำ หรือไม่สามารถตรวจสอบความถูกต้องของหมายเลขโทรศัพท์ เว็บไซต์ หรือเอกสารที่ได้รับได้ด้วยตนเอง นอกจากนี้ ยังพบว่ากลุ่มเป้าหมายเหล่านี้มักมีแนวโน้มที่จะเชื่อฟังบุคคลในเครื่องแบบหรือเจ้าหน้าที่รัฐโดยไม่ตั้งคำถาม ทำให้ตกอยู่ในภาวะตื่นตระหนกและยินยอมทำตามคำสั่งของคนร้ายโดยง่าย เช่น โอนเงิน ส่ง OTP หรือให้ข้อมูลส่วนตัว แนวโน้มการหลอกลวงด้วยวิธีการโทรศัพท์จึงกลายเป็นภัยคุกคามที่สำคัญต่อความมั่นคงปลอดภัยของประชาชน โดยเฉพาะในกลุ่มเปราะบางทางเทคโนโลยี และจำเป็นต้องได้รับการแก้ไขด้วยมาตรการทั้งเชิงเทคนิค เช่น ระบบแจ้งเตือนสายหลอกลวง และเชิงสังคม เช่น การรณรงค์ให้ความรู้แก่ผู้สูงวัยและบุคคลทั่วไปเกี่ยวกับรูปแบบของการหลอกลวงที่เปลี่ยนแปลงอยู่ตลอดเวลา

6) Angler Phishing เป็นการหลอกลวงผ่าน โซเชียลมีเดีย เช่น Facebook, X (Twitter) หรือ Instagram โดยคนร้ายมักปลอมแปลงตัวเองเป็นผู้ดูแลเพจหรือฝ่ายบริการลูกค้าของแบรนด์ที่มีชื่อเสียง เช่น บริษัทขนส่ง แพลตฟอร์มอีคอมเมิร์ซ หรือธนาคาร โดยใช้ชื่อเพจที่คล้ายกับของจริง พร้อมโลโก้และภาพประกอบที่น่าเชื่อถือเพื่อสร้างความไว้วางใจ รูปแบบการโจมตีจะเริ่มจากการที่ผู้ใช้งานแสดงความคิดเห็นหรือโพสต์ร้องเรียนเกี่ยวกับปัญหา

การใช้บริการ เช่น สินค้าส่งล่าช้า หรือบริการล้มเหลว จากนั้น “มิจฉาชีพ” จะเข้าไปตอบกลับโดยใช้บัญชีปลอมที่ดูเหมือนเจ้าหน้าที่จริง พร้อมแนบลิงก์ปลอม เช่น ฟอร์มขอคืนเงิน, ลิงก์ตรวจสอบสถานะ หรือ แบบสอบถามรับส่วนลด เพื่อหลอกให้กรอกข้อมูลส่วนตัว หมายเลขบัตรเครดิต หรือ OTP ตัวอย่างเหตุการณ์ที่เกิดขึ้นจริงในช่วงต้นปี พ.ศ. 2566 เกิดกรณี ผู้ใช้บริการขนส่งเอกชนรายหนึ่ง (J&T Express) ได้โพสต์ร้องเรียนบน Facebook ว่าสินค้าส่งล่าช้า หลังจากนั้นไม่นานมี “เพจปลอม” ที่ใช้ชื่อคล้าย J&T Express พร้อมโลโก้สีแดง เข้าไปแสดงความคิดเห็นว่า “ขออภัยในความไม่สะดวก กรุณาคลิกที่ลิงก์นี้เพื่อตรวจสอบสถานะพัสดุของคุณและกรอกข้อมูลรับเงินคืน” ซึ่งผู้ใช้จำนวนหนึ่งหลงเชื่อและคลิกลิงก์ดังกล่าว ก่อนจะกรอกข้อมูลบัตรเครดิต และต่อมาพบว่ามีการถูกหักเงินออกจากบัญชีจำนวนหลายหมื่นบาท จากการศึกษากลุ่มเป้าหมายของ Angler Phishing พบว่ามักเป็นผู้ใช้งานโซเชียลมีเดียในช่วงอายุ 20 - 35 ปี ซึ่งมีพฤติกรรมติดต่อสอบถามบริการหรือร้องเรียนผ่านเพจต่าง ๆ เป็นประจำ และมักตอบสนองอย่างรวดเร็วต่อข้อความที่ดูเหมือนมาจาก “แอดมินจริง”

7) Search Engine Phishing เป็นเทคนิคที่ผู้กระทำผิดสร้างเว็บไซต์ปลอมขึ้นมาโดยเลียนแบบเว็บไซต์ของธนาคาร หน่วยงานรัฐ หรือร้านค้าออนไลน์ที่ประชาชนใช้บริการบ่อย เช่น เว็บไซต์กรมการขนส่งทางบก เว็บไซต์ยื่นภาษี หรือเว็บไซต์ของบริษัทขนส่ง จากนั้นใช้เทคนิคการทำ Search Engine Optimization (SEO) หรือซื้อโฆษณาผ่านแพลตฟอร์มเช่น Google Ads เพื่อให้เว็บไซต์ปลอมแสดงอยู่ในอันดับต้น ๆ ของผลการค้นหาเมื่อผู้ใช้งานค้นหาข้อมูล เช่น “ต่อทะเบียนรถออนไลน์” หรือ “สมัครสินเชื่อ ธ.ก.ส.” แล้วคลิกเข้าเว็บไซต์ที่ดูน่าเชื่อถือ แต่เป็นเว็บไซต์ปลอมที่มีหน้าตาคล้ายของจริง ระบบจะให้กรอกข้อมูลส่วนตัว เช่น ชื่อ-นามสกุล เลขบัตรประชาชน หมายเลขบัญชีธนาคาร และรหัส OTP ซึ่งคนร้ายจะนำข้อมูลเหล่านี้ไปใช้โจรกรรมทางการเงิน ทั้งนี้พบมีตัวอย่างเหตุการณ์ที่เกิดขึ้นจริงในปี พ.ศ. 2566 มีผู้ใช้งานจำนวนมากหลงเชื่อเข้าเว็บไซต์ปลอมที่เลียนแบบเว็บของกรมการขนส่งทางบก โดยเว็บไซต์ดังกล่าวถูกทำ SEO และซื้อ Google Ads ให้ขึ้นเป็นอันดับแรกในการค้นหาคำว่า “ต่อทะเบียนรถยนต์ออนไลน์” เมื่อผู้ใช้เข้าไปและกรอกข้อมูลบัตรประชาชน เลขทะเบียนรถ และข้อมูลบัญชีธนาคาร ระบบจะส่ง OTP เพื่อตรวจสอบแล้วนำข้อมูลเหล่านี้ไปใช้ถอนเงินออกจากบัญชีจริงของเหยื่อ ทั้งนี้มีผู้เสียหายรายหนึ่งในจังหวัดชลบุรี สูญเงินกว่า 92,000 บาท ภายใน 5 นาทีหลังกรอกข้อมูลผ่านเว็บปลอม โดยไม่ทันรู้ตัวว่าไม่ใช่เว็บไซต์ของหน่วยงานรัฐ ข้อมูลดังกล่าวได้รับการเผยแพร่ผ่านช่องข่าวหลัก และได้รับการเตือนจาก **ThaiCERT** ว่า Search Engine Phishing กำลังเป็นภัยคุกคามที่เพิ่มขึ้นอย่างรวดเร็วในประเทศไทย โดยเฉพาะกับประชาชนทั่วไปที่มีอายุตั้งแต่ 40 ปีขึ้นไป ซึ่งไม่คุ้นชินกับการตรวจสอบ URL หรือไม่ทราบถึงความแตกต่างระหว่างเว็บไซต์จริงและปลอม

8) CEO Fraud เป็นเทคนิคที่ผู้กระทำผิดปลอมแปลงอีเมลของผู้บริหารระดับสูงในองค์กร เช่น CEO หรือ CFO โดยใช้วิธีการ email spoofing เพื่อให้ดูเหมือนว่าอีเมลส่งมาจากบุคคลจริง เช่น ceo@company.com จากนั้นจะส่งคำสั่งไปยังฝ่ายบัญชีหรือการเงินให้ดำเนินการโอนเงินไปยังบัญชีที่คนร้ายควบคุมอยู่ โดยมักเป็นคำสั่งที่มีลักษณะ **เร่งด่วน มีความเป็นทางการ และแฝงความลับ** เช่น “ขอให้โอนเงินจำนวน xx ล้านบาทไปยังบัญชีต่างประเทศภายในวันนี้ ห้ามแจ้งทีมอื่น เนื่องจากเป็นโครงการลับของบริษัท”

ลักษณะสำคัญของ CEO Fraud คือการ **ใช้ความไว้วางใจในตำแหน่งหน้าที่และลำดับอำนาจ** ในองค์กรมาเป็นเครื่องมือในการกดดันให้ผู้รับคำสั่งเร่งดำเนินการโดยไม่ตรวจสอบซ้ำ อีกทั้งมักพุ่งเป้าไปยังผู้ที่รับผิดชอบด้านบัญชี การเงิน หรือเลขานุการส่วนตัวของผู้บริหาร ที่อยู่ในช่วงอายุ 30 - 45 ปี ซึ่งเป็นวัยทำงานหลักขององค์กร

รูปแบบเหล่านี้ล้วนมีจุดร่วมสำคัญคือ การใช้เทคนิควิศวกรรมสังคม (Social Engineering) ที่อาศัยความไว้วางใจ ความไม่รู้เท่าทัน และสถานการณ์ที่บีบบังคับทางอารมณ์ของเหยื่อเพื่อให้เกิดการกระทำที่เป็นประโยชน์ต่อผู้กระทำผิด เช่น การเปิดเผยข้อมูลส่วนบุคคล การโอนเงิน หรือการให้สิทธิ์เข้าถึงระบบ เป็นต้น

2. ปัจจัยที่ส่งผลต่อการเกิดอาชญากรรมฟิชชิง

จากผลการศึกษาพบว่า การเกิดอาชญากรรมฟิชชิงเป็นผลลัพธ์ของความเชื่อมโยงกันระหว่างพฤติกรรมของผู้กระทำผิดและเหยื่อ ซึ่งทั้งสองฝ่ายล้วนมีปัจจัยสนับสนุนที่ส่งผลให้อาชญากรรมเกิดขึ้นได้อย่างมีประสิทธิภาพ โดยเฉพาะในยุคดิจิทัลที่ช่องทางการกระทำความผิดมีความหลากหลายและซับซ้อนยิ่งขึ้น ผู้กระทำผิดในคดีฟิชชิงไม่ได้จำกัดอยู่เฉพาะกลุ่มอาชญากรมืออาชีพ หากแต่รวมถึงบุคคลทั่วไปที่เข้าสู่วงจรนี้จากการเรียนรู้ผ่านสื่อสังคมออนไลน์

แพลตฟอร์มอย่าง Telegram, Discord และฟอรัมใน Dark Web กลายเป็นแหล่งเรียนรู้การกระทำผิดที่มีทั้งเครื่องมือ เทคนิค และการสนับสนุนเชิงแนวคิดอย่างครบถ้วน พฤติกรรมของผู้กระทำผิดสามารถอธิบายได้ผ่านกรอบคิดของทฤษฎีการเลือกอย่างมีเหตุผล (Rational Choice Theory) ที่เสนอว่าผู้กระทำผิดจะตัดสินใจโดยพิจารณาผลตอบแทนและความเสี่ยง ซึ่งในกรณีฟิชชิงถือว่ามีความเสี่ยงต่ำและผลตอบแทนสูง จึงเป็นทางเลือกที่น่าสนใจโดยเฉพาะสำหรับผู้ที่มองหาแหล่งรายได้รวดเร็วโดยไม่ต้องใช้ต้นทุนมากนัก ทั้งนี้ ทฤษฎีการคบค้าสมาคมที่แตกต่าง (Differential Association Theory) ยังช่วยอธิบายว่าการเรียนรู้พฤติกรรมอาชญากรรมเกิดจากปฏิสัมพันธ์กับกลุ่มที่มีแนวโน้มสนับสนุนการกระทำผิด หากบุคคลถูกแวดล้อมด้วยกลุ่มที่เห็นว่าฟิชชิงเป็นเรื่องปกติหรือน่าทดลอง ก็จะมีแนวโน้มรับเอาความคิดและพฤติกรรมนั้นมาใช้ ทฤษฎีข้อแก้ตัว (Neutralization Theory) ก็ให้มุมมองเสริมว่าผู้กระทำผิดจำนวนไม่น้อยใช้ข้ออ้างเชิงจริยธรรมและสังคม เช่น "เหยื่อประมาทเอง" หรือ "ไม่ได้ขโมยเอง" เพื่อลดแรงกดดันภายในใจและทำให้การกระทำของตนดูสมเหตุสมผล ขณะที่ทฤษฎีการเปลี่ยนผ่านเชิงพื้นที่ (Space Transition Theory) ระบุว่า โลกออนไลน์เอื้อให้คนที่ไม่กล้าทำผิดในชีวิตจริงสามารถกล้าทำในสภาพแวดล้อมที่ไร้ตัวตนและไร้ขอบเขต เช่นเดียวกับที่พบในกรณีผู้กระทำผิดที่เริ่มต้นจากความอยากรู้อยากลองแต่กลับกลายเป็นหนึ่งในเครือข่ายอาชญากรรมไซเบอร์อย่างเต็มตัว

ในด้านของเหยื่อ พบว่าเหยื่อจำนวนมากตกเป็นเป้าหมายจากพฤติกรรมที่เปิดโอกาส เช่น การคลิกลิงก์จากข้อความแปลกปลอม การกรอกข้อมูลในเว็บไซต์ที่ไม่น่าเชื่อถือ หรือการเปิดเผยข้อมูลส่วนตัวโดยไม่ตระหนักถึงความเสี่ยง ทฤษฎีกิจวัตรประจำวัน (Routine Activity Theory) และทฤษฎีสามเหลี่ยมอาชญากรรม (Crime Triangle Theory) ช่วยอธิบายว่าเมื่อผู้กระทำผิดมีแรงจูงใจ เหยื่อมีลักษณะเป็นเป้าหมายที่เหมาะสม และไม่มีระบบป้องกันที่เพียงพอ อาชญากรรมก็มีแนวโน้มจะเกิดขึ้นได้อย่างง่ายดาย ทั้งนี้ ทฤษฎีการมีส่วนร่วมของเหยื่อ (Victim Participation Theory) ของ Wolfgang ยังเน้นย้ำว่าแม้เหยื่อจะไม่ได้ตั้งใจยั่วยุ แต่พฤติกรรมบางประการของเหยื่อ เช่น ความไม่ระมัดระวัง หรือความไว้วางใจต่อเทคโนโลยี ก็อาจกลายเป็นปัจจัยกระตุ้นให้เกิดเหตุการณ์ฟิชชิงได้โดยไม่รู้ตัว ในบริบทนี้ ทฤษฎีเทคโนโลยีสมัยใหม่ (New Technology Theory) ได้ชี้ให้เห็นว่า ความสะดวกของเทคโนโลยีกลับกลายเป็นความเปราะบางใหม่ โดยผู้ใช้งานที่คุ้นชินกับการใช้แอปพลิเคชัน ธนาคารออนไลน์ และโซเชียลมีเดียมักหลงเชื่อการหลอกลวงที่แนบเนียนโดยขาดการตรวจสอบ

กล่าวได้ว่า การเกิดอาชญากรรมฟิชชิงไม่ใช่เพียงการกระทำผิดเชิงเทคนิค แต่เป็นผลรวมของพฤติกรรมที่มีกลไกคิดและวัฒนธรรมดิจิทัลเป็นพื้นฐานรองรับ ทั้งในมุมของผู้กระทำผิดที่มีเหตุผล แรงจูงใจ และข้อแก้ตัวในเชิงจิตวิทยา และในมุมของเหยื่อที่ขาดการป้องกันตัว ขาดความรู้เท่าทัน และเปิดโอกาสให้ตนเองกลายเป็นเป้าหมายโดยไม่รู้ตัว ความเข้าใจปัจจัยทั้งสองด้านจึงเป็นพื้นฐานสำคัญในการออกแบบมาตรการป้องกันและรับมือกับภัยคุกคามอาชญากรรมไซเบอร์ในยุคปัจจุบัน

3. แนวทางการป้องกันอาชญากรรมไซเบอร์ กรณีการโจมตีแบบฟิชชิง

จากการศึกษา พบว่าแนวทางการรับมือกับภัยคุกคามอาชญากรรมไซเบอร์ รูปแบบการโจมตีแบบฟิชชิงจำเป็นต้องอาศัยกลไกเชิงรุกในหลายระดับ ทั้งด้านกฎหมาย การยับยั้งเชิงจิตวิทยา และการมีส่วนร่วมของสังคม โดยสามารถจำแนกแนวทางที่สำคัญออกเป็น 5 ด้าน ดังนี้

1) การเสริมสร้างศักยภาพของกลไกการบังคับใช้กฎหมายอย่างครอบคลุมและทันสมัย กล่าวคือ หน่วยงานของรัฐ โดยเฉพาะหน่วยงานด้านความมั่นคงและตำรวจไซเบอร์ ต้องพัฒนาขีดความสามารถทั้งด้านองค์ความรู้ เทคโนโลยี และบุคลากรให้สามารถรับมือกับภัยคุกคามรูปแบบใหม่ได้อย่างรวดเร็วและมีประสิทธิภาพ

2) การบังคับใช้กฎหมายเพื่อสร้างแรงยับยั้งทางจิตวิทยา ในการลงโทษผู้กระทำผิดเป็นเพียงส่วนหนึ่งของการดำเนินงานทางกฎหมาย แต่การยับยั้งไม่ให้เกิดอาชญากรรมตั้งแต่แรกเริ่มนั้นมีประสิทธิภาพยิ่งกว่า ทฤษฎีการป้องกัน (Deterrence Theory) ชี้ให้เห็นว่าการถูกลงโทษส่งผลต่อการตัดสินใจของผู้ที่กำลังจะกระทำผิดมากกว่าความรุนแรงของบทลงโทษ ดังนั้น ภาครัฐควรเน้นการเปิดเผยข้อมูลผลการจับกุมคดีฟิชชิง การเร่งรัดกระบวนการพิจารณาคดี และการประชาสัมพันธ์บทลงโทษผ่านช่องทางต่าง ๆ เพื่อสร้างแรงกดดันในเชิงจิตวิทยาแก่ผู้ที่มีแนวโน้มจะก่ออาชญากรรม

3) การสร้างกลไกความร่วมมือจากชุมชนออนไลน์ในฐานะเกราะป้องกัน ควรส่งเสริมให้มีกลไกการป้องกันในระดับชุมชน โดยเฉพาะในบริบทของชุมชนออนไลน์ ตามแนวคิดจาก The Ecological School of Criminology ชี้ให้เห็นว่า เมื่อสมาชิกในชุมชนมีความสัมพันธ์ที่เข้มแข็งและมีความไว้วางใจกัน ย่อมสามารถลดโอกาสการเกิดอาชญากรรมได้

4) การส่งเสริมความรู้เท่าทันภัยไซเบอร์ในระดับประชาชน จากการศึกษาประชาชนส่วนใหญ่ที่ตกเป็นเหยื่อฟิชชิงมักเป็นผู้ที่ขาดความรู้หรือประสบการณ์เกี่ยวกับการใช้งานเทคโนโลยีสารสนเทศ โดยเฉพาะกลุ่มเปราะบาง เช่น ผู้สูงอายุ เยาวชน หรือผู้มีการศึกษาด้านเทคโนโลยีน้อย การส่งเสริมให้ประชาชนมีภูมิคุ้มกันไซเบอร์ (Cyber Immunity) จึงเป็นสิ่งจำเป็น

5) การทำความเข้าใจพฤติกรรมของผู้กระทำผิดในพื้นที่ดิจิทัล จากการศึกษาแนวคิดจาก Space Transition Theory ของ Jaishankar ชี้ให้เห็นว่าพฤติกรรมของบุคคลในโลกไซเบอร์มักแตกต่างจากโลกแห่งความเป็นจริงอย่างมีนัยสำคัญ เนื่องจากพื้นที่ออนไลน์เปิดโอกาสให้ผู้ใช้งานสามารถปกปิดตัวตน หรือแสดงพฤติกรรมที่ตนไม่กล้าทำในโลกจริง ดังนั้น การรับมือกับอาชญากรไซเบอร์จึงจำเป็นต้องเข้าใจธรรมชาติของอาชญากรรมแบบแฝงตัวด้วย

สรุปและอภิปรายผล

จากการศึกษาพบว่า การโจมตีแบบฟิชชิงในประเทศไทยมีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่องและมีความซับซ้อนมากขึ้น โดยอาชญากรปรับเปลี่ยนกลยุทธ์ให้สอดคล้องกับพฤติกรรมของผู้ใช้งานดิจิทัล เช่น การปลอมตัวผ่านเว็บไซต์หรือโซเชียลมีเดีย สะท้อนให้เห็นว่า ฟิชชิงเป็นทั้งอาชญากรรมเชิงเทคโนโลยีและอิงพฤติกรรมมนุษย์ และเมื่อวิเคราะห์ผ่านกรอบทฤษฎีต่าง ๆ ได้แก่ ทฤษฎีการบังคับใช้กฎหมาย ทฤษฎียับยั้ง ทฤษฎีชุมชนสัมพันธ์ และทฤษฎีการเปลี่ยนผ่านเชิงพื้นที่ พบว่าการรับมือกับฟิชชิงต้องอาศัยความร่วมมือแบบบูรณาการจากทุกภาคส่วน จะเห็นได้ว่า ผู้กระทำผิดมักตัดสินใจก่ออาชญากรรมจากการประเมินผลตอบแทนที่คุ้มค่าเมื่อเทียบกับความเสี่ยงที่ต่ำ ขณะที่เหยื่อส่วนใหญ่มักตกเป็นเป้าหมายจากความไม่รู้เท่าทันและการขาดระบบป้องกัน แม้จะมีความพยายามในด้านกฎหมาย แต่ข้อจำกัดด้านการตีความ การเข้าถึงข้อมูล และบุคลากรเฉพาะทาง ยังคงเป็นอุปสรรคต่อการป้องกันและ ปราบปราม ทั้งนี้ แนวทางการป้องกันที่มีประสิทธิภาพควรครอบคลุมทั้งการพัฒนากลไกกฎหมาย การใช้บทลงโทษเชิงยับยั้ง การสร้างเครือข่ายชุมชนออนไลน์ การยกระดับความรู้ประชาชน และการเข้าใจพฤติกรรมของผู้กระทำผิดในโลกไซเบอร์ ซึ่งสามารถนำไปต่อยอดเป็นนโยบายป้องกันเชิงรุกได้อย่างเป็นรูปธรรม

ข้อเสนอแนะ

จากผลการศึกษา ผู้วิจัยเห็นว่าการรับมือกับภัยคุกคามดังกล่าวควรดำเนินไปทั้งในระดับนโยบายและระดับปฏิบัติ โดยมีข้อเสนอแนะ ดังนี้

1. ข้อเสนอแนะเชิงนโยบาย

1.1 ปรับปรุงและพัฒนากฎหมายให้สอดรับกับภัยคุกคามรูปแบบใหม่ กล่าวคือ กฎหมายที่มีอยู่ในปัจจุบัน แม้จะสามารถบังคับใช้กับการกระทำผิดหลายลักษณะได้ แต่ยังขาดความยืดหยุ่นและความทันสมัยในการรองรับภัยคุกคามที่เปลี่ยนแปลงตลอดเวลา ดังนั้น ควรมีการทบทวนบทบัญญัติกฎหมายให้ครอบคลุมมากขึ้น

1.2 ส่งเสริมความร่วมมือระหว่างประเทศ เนื่องจากอาชญากรรมไซเบอร์มักมีลักษณะข้ามพรมแดน การสืบสวนสอบสวนจำเป็นต้องอาศัยความร่วมมือจากต่างประเทศ เพื่อให้เจ้าหน้าที่สามารถขอข้อมูลได้อย่างมีประสิทธิภาพ ลดระยะเวลาในการดำเนินคดี และเพิ่มอัตราการจับกุมผู้กระทำผิดในระดับนานาชาติ

1.3 จัดตั้งศูนย์ปฏิบัติการไซเบอร์ระดับชาติแบบเบ็ดเสร็จ เพื่อให้การรับมือภัยคุกคามทางไซเบอร์มีความคล่องตัวและทันต่อสถานการณ์

2. ข้อเสนอแนะเชิงปฏิบัติ

2.1 พัฒนาทักษะบุคลากรด้านอาชญากรรมไซเบอร์อย่างต่อเนื่อง เพื่อให้สามารถตอบสนองต่อเทคนิคการหลอกลวงแบบใหม่ ๆ ได้อย่างมีประสิทธิภาพ

2.2 ออกแบบสื่อการเรียนรู้ที่เข้าถึงง่ายและทันสมัยสำหรับประชาชน กล่าวคือ ประชาชนควรได้รับการสื่อสารข้อมูลในรูปแบบที่เข้าใจง่าย สนุก และสื่อสารผ่านช่องทางที่เข้าถึงได้ โดยควรใช้ภาษาที่เป็นมิตร ทันสมัย และไม่ซับซ้อน เพื่อให้ประชาชนทุกช่วงวัยสามารถเข้าใจได้

2.3 ส่งเสริมบทบาทของชุมชนออนไลน์และอาสาสมัครดิจิทัล รัฐควรส่งเสริมให้เกิดเครือข่ายอาสาสมัครดิจิทัลในชุมชน เพื่อรายงานพฤติกรรมต้องสงสัยไปยังหน่วยงานที่เกี่ยวข้องเพื่อสร้างเครือข่ายและการป้องกันที่เหมาะสม

2.4 ส่งเสริมบทบาทเชิงรุกของภาคเอกชน โดยเฉพาะธนาคาร กล่าวคือองค์กรภาคเอกชนต่าง ๆ ควรมีระบบแจ้งเตือนภัยล่วงหน้าแก่ลูกค้าหรือผู้มีส่วนเกี่ยวข้อง รวมถึงควรมีนโยบายการเยียวยาเหยื่อในกรณีที่พบว่าเป็นความผิดพลาดจากระบบ เพื่อสร้างความมั่นใจในการใช้งานระบบดิจิทัลอย่างปลอดภัย

เอกสารอ้างอิง

กชพรรณ มณีภาค และ อุนิษา เลิศโตมรสกุล. (2563). การตกเป็นเหยื่ออาชญากรรมจากการกระทำผิดในโลกอินเทอร์เน็ต: กรณีศึกษา การรังแกกันในโลกไซเบอร์ในรูปแบบการคุกคามทางเพศในเขตกรุงเทพมหานคร. คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย.

กรุงเทพธุรกิจ. (2565). แคสเปอร์สกี้เผย 4 ภัยคุกคาม สะเทือนโลกออนไลน์ปี 2565. สืบค้นจาก https://www.bangkokbiznews.com/tech/982543

คำสั่งคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติที่ 11/2542 เรื่อง แต่งตั้งคณะอนุกรรมการเฉพาะกิจยกร่างกฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์จำนวน 22 คน.

จิรวัฒน์ มหรรณพ. (2564). *การแพร่กระจายความรู้ด้านอาชญากรรมไซเบอร์ในกลุ่มออนไลน์*. วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, มหาวิทยาลัยเชียงใหม่.

ญาณพล ยั่งยืน. (2548). อาชญากรรมคอมพิวเตอร์. สืบค้นจาก http://www.ku.ac.th/netday2005/document/yanpon.pdf

ธีรยุทธ สุคนธ์. (2566). *การใช้ Social Engineering ในอาชญากรรมไซเบอร์: กรณีศึกษาแพลตฟอร์มโซเชียลมีเดีย*. วารสารอาชญาวิทยาและนโยบายอาญา, 28(2), 55–74.

นภัสสร เรืองรอง. (2563). *แนวทางการป้องกันการหลอกลวงทางอินเทอร์เน็ตในกลุ่มเยาวชน: กรณีศึกษาเขตกรุงเทพมหานคร*. วารสารเทคโนโลยีสารสนเทศและนวัตกรรม, 9(1), 45–62.

ปรัชญา พิพัฒน์พงศ์. (2562). *การตอบสนองของหน่วยงานรัฐต่ออาชญากรรมไซเบอร์: ศึกษากรณีการหลอกลวงแบบฟิชชิง*. วารสารรัฐประศาสนศาสตร์, 21(3), 112–130.

สกาวเดือน แสงสุวรรณ. (2565). *พฤติกรรมการใช้งานอินเทอร์เน็ตของผู้สูงอายุที่มีความเสี่ยงต่อการตกเป็นเหยื่อฟิชชิง*. วิทยานิพนธ์รัฐศาสตรมหาบัณฑิต, มหาวิทยาลัยธรรมศาสตร์.

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2565). *รายงานผลการสำรวจพฤติกรรมผู้ใช้อินเทอร์เน็ตในประเทศไทย ปี พ.ศ. 2565*. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม.

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2566). *รายงานผลการสำรวจพฤติกรรมผู้ใช้อินเทอร์เน็ตในประเทศไทย ปี พ.ศ. 2566*. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม.

สาวตรี สุขศรี. (2563). *กฎหมายว่าด้วยอาชญากรรมคอมพิวเตอร์และอาชญากรรมไซเบอร์* (พิมพ์ครั้งที่ 2). คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์.

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย. (2562). สถิติด้านภัยคุกคามไซเบอร์ของไทยเมื่อ พ.ศ. 2562. สืบค้นจาก https://www.thaicert.or.th/statistics/statistics2019.html

Anti-Phishing Working Group (APWG). (2024). *Phishing Activity Trends Report Q4 2023*. Retrieved from https://apwg.org/trendsreports/

Beccaria, C. (1764). *On crimes and punishments.* (Reprinted and translated editions available; commonly cited from modern interpretations).

Becker, G. S. (1968). Crime and punishment: An economic approach. *Journal of Political Economy*, *76*, 169.

Cambridge Dictionary. (n.d.). *Phishing*. Retrieved from https://dictionary.cambridge.org

Clough, J. (2016). *Principles of cybercrime* (2nd ed.). Cambridge University Press.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608.

Council of Europe. (2001). *Convention on Cybercrime*. Retrieved from http://www.refworld.org/docid/47fdfb202.html

Eck, J. E. (1994). *Drug markets and drug places: A case-control study of the spatial structure of illicit drug dealing*. Crime Prevention Studies, 2, 67–115.

Grabosky, P. N. (1996). Unintended consequences of crime prevention. Crime Prevention Studies, 5, 1–30.

Jaishankar, K. (2008). *Space Transition Theory of Cyber Crimes.* Indian Journal of Criminology, 36(2), 1–9.

Jaishankar, K. (2008). Space transition theory of cyber crime. In F. Schmallager & M. Pittaro (Eds.), *Crimes of the internet* (pp. 283–301). Prentice Hall Press.

Nagin, D. S. (2013). Deterrence in the twenty-first century. *Crime and Justice*, *42*(1), 199–263.

Paternoster, R. (2010). How much do we really know about deterrence? *Journal of Criminal Law and Criminology*, *100*(3), 765–824.

Sampson, R. J., Raudenbush, S. W., & Earls, F. (1997). Neighborhoods and violent crime: A multilevel study of collective efficacy. *Science, 277*(5328), 918–924.

Shaw, C. R., & McKay, H. D. (1942). *Juvenile delinquency and urban areas*. Chicago, IL: University of

Siegel, L. J. (2015). *Criminology: The core* (5th ed.). Belmont, CA: Cengage Learning.

Sullivan, L. (1973). *Criminal Behavior: A Process of Rational Decision Making*. In S. B. Warner (Ed.), *Theories of Criminal Behavior*. New York: Random House.

Sutherland, E. H., & Cressey, D. R. (1996). *Principles of criminology* (10th ed.). Lippincott.

Sutherland, E. H., & Cressey, D. R. (1996). *Principles of Criminology* (11th ed.). Lanham, MD: Rowman & Littlefield

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review, 22*(6), 664–670.

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.