อาชญากรรมทางเทคโนโลยีในบริบทประเทศไทย : สถานการณ์ ผลกระทบ และแนวทางการรับมือ[1]

ร.ต.อ.เสริมศิริ แต่งตั้ง[2]

จากการศึกษาปัญหาเกี่ยวกับอาชญากรรมทางเทคโนโลยี ปัจจุบันเป็นปัญหาสำคัญที่ทวีความรุนแรงขึ้นตามความก้าวหน้าของเทคโนโลยีสารสนเทศและการใช้งานอินเทอร์เน็ตอย่างแพร่หลายในประเทศไทย บทความฉบับนี้มีวัตถุประสงค์เพื่อศึกษาความหมาย แนวคิด รูปแบบ สาเหตุ และผลกระทบของอาชญากรรมทางเทคโนโลยีในบริบทของประเทศไทย รวมถึงการวิเคราะห์บทบาทของกฎหมายและหน่วยงานที่เกี่ยวข้อง ตลอดจนเสนอแนวทางการป้องกันและแก้ไขปัญหาอย่างเป็นระบบ ผลการศึกษาพบว่า รูปแบบอาชญากรรมทางเทคโนโลยีที่พบมากในประเทศไทย ได้แก่ การฉ้อโกงออนไลน์ การฟิชชิง การโจมตีระบบคอมพิวเตอร์ และการละเมิดข้อมูลส่วนบุคคล ซึ่งส่งผลกระทบต่อประชาชน องค์กร และความมั่นคงของประเทศอย่างกว้างขวาง ดังนั้น การพัฒนาความรู้เท่าทันดิจิทัล การเสริมสร้างความปลอดภัยไซเบอร์ และการบังคับใช้กฎหมายอย่างมีประสิทธิภาพจึงเป็นปัจจัยสำคัญในการลดปัญหาอาชญากรรมทางเทคโนโลยีในประเทศไทย

ในปัจจุบันเทคโนโลยีสารสนเทศและการสื่อสารได้เข้ามามีบทบาทสำคัญต่อการดำเนินชีวิตของประชาชนในประเทศไทย ไม่ว่าจะเป็นการติดต่อสื่อสาร การทำธุรกรรมทางการเงิน การศึกษา หรือการดำเนินกิจกรรมทางธุรกิจ การพัฒนาเศรษฐกิจดิจิทัลช่วยเพิ่มประสิทธิภาพและความสะดวกสบายให้กับสังคม อย่างไรก็ตามการใช้เทคโนโลยีอย่างแพร่หลายได้ก่อให้เกิดปัญหาอาชญากรรมทางเทคโนโลยี ซึ่งมีแนวโน้มเพิ่มขึ้นทั้งในด้านจำนวนและความซับซ้อน

อาชญากรรมทางเทคโนโลยีไม่เพียงส่งผลกระทบต่อทรัพย์สินหรือข้อมูลส่วนบุคคลของประชาชนเท่านั้น แต่ยังส่งผลต่อความเชื่อมั่นในระบบดิจิทัล และอาจกระทบต่อความมั่นคงของประเทศ จึงมุ่งเน้นการศึกษาอาชญากรรมทางเทคโนโลยีในบริบทประเทศไทย เพื่อสร้างความเข้าใจและเสนอแนวทางการรับมืออย่างเหมาะสม

---

[1] อาชญากรรมทางเทคโนโลยีในบริบทประเทศไทย : สถานการณ์ ผลกระทบ และแนวทางการรับมือโดยมีที่ปรึกษา คือ รองศาสตราจารย์พัฒนะ เรือนใจดี และคณะกรรมการสอบ คือ รองศาสตราจารย์ ดร.ปวริศร เลิศธรรมเทวี และรองศาสตราจารย์ ดร.ปรีดา โชติมานนท์

[2] นักศึกษาปริญญาโท หลักสูตรนิติศาสตรมหาบัณฑิต (ส่วนภูมิภาค) คณะนิติศาสตร์ มหาวิทยาลัยรามคำแหง

อาชญากรรมทางเทคโนโลยี หมายถึง การกระทำความผิดที่เกี่ยวข้องกับการใช้คอมพิวเตอร์ ระบบเครือข่าย หรือเทคโนโลยีดิจิทัลเป็นเครื่องมือ หรือเป็นเป้าหมายของการกระทำผิด การกระทำดังกล่าวอาจก่อให้เกิดความเสียหายต่อข้อมูล ระบบ หรือทรัพย์สินของผู้อื่น

ในบริบทประเทศไทย อาชญากรรมทางเทคโนโลยีถูกกำหนดและควบคุมโดยกฎหมายหลายฉบับ โดยเฉพาะพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งเป็นกฎหมายหลักในการกำกับดูแลการใช้งานระบบคอมพิวเตอร์และอินเทอร์เน็ต

รูปแบบอาชญากรรมทางเทคโนโลยีในประเทศไทย

1 การฉ้อโกงทางออนไลน์ หมายถึง การกระทำความผิดฐานฉ้อโกงตามประมวลกฎหมายอาญา โดยใช้อินเทอร์เน็ตเป็นช่องทางหลักในการหลอกลวงผู้เสียหาย เพื่อให้ได้มาซึ่งทรัพย์สินหรือข้อมูลส่วนบุคคล อาชญากรรมประเภทนี้จัดอยู่ในกลุ่ม Cyber-enabled Crime หรืออาชญากรรมที่ใช้เทคโนโลยีสนับสนุน ซึ่งแตกต่างจากการแฮ็กระบบตรงที่อาชญากรรมประเภทนี้มุ่งเน้นการโจมตีที่ "จุดอ่อนของมนุษย์" (Human Vulnerability) มากกว่าจุดอ่อนของซอฟต์แวร์ จากการวิเคราะห์สถิติของศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ (PCT) สำนักงานตำรวจแห่งชาติ สามารถจำแนกรูปแบบการฉ้อโกงที่มีนัยสำคัญได้ดังนี้:

1.1 การหลอกลวงซื้อขายสินค้า (E-Commerce Fraud) ถือเป็นคดีที่มีปริมาณการแจ้งความสูงสุด (Volume Crime) รูปแบบพฤติการณ์คือการเปิดเพจร้านค้าปลอม หรือสวมรอยเป็นร้านค้าที่มีชื่อเสียง โพสต์ขายสินค้าในราคาที่ต่ำกว่าท้องตลาดเพื่อดึงดูดใจ (Lure) เมื่อเหยื่อโอนเงิน ผู้กระทำผิดจะปิดเพจหนี หรือส่งสินค้าที่ไม่ตรงปกมาให้

1.2 การหลอกลงทุนแบบไฮบริด (Hybrid Investment Scam / Pig Butchering)

นี่คือรูปแบบที่สร้างมูลค่าความเสียหายสูงสุด (Value Crime) รู้จักกันในชื่อ "Pig Butchering Scam" หรือ "การฆ่าหมู" กระบวนการทำงานมีลักษณะเป็นระบบขั้นสูง:

1.2.1 การขุน (Fattening): คนร้ายเข้ามาตีสนิทผ่านแอปหาคู่หรือโซเชียลมีเดีย (Romance Scam) สร้างความเชื่อใจเสมือนคนรัก หรือที่ปรึกษาทางการเงิน

1.2.2 การหลอกล่อ: ชักชวนให้ลงทุนในแพลตฟอร์มเทรดคริปโทเคอร์เรนซีปลอม (Fake Crypto Exchange) ที่คนร้ายเขียนโปรแกรมควบคุมกราฟได้

1.2.3 การเชือด (Slaughter): ช่วงแรกเหยื่อจะได้รับผลกำไรและถอนเงินได้จริงเพื่อสร้างความตายใจ เมื่อเหยื่อทุ่มเงินก้อนใหญ่ (Life Savings) ระบบจะแจ้งว่าไม่สามารถถอนเงินได้ ต้องจ่ายภาษีหรือค่าธรรมเนียมค้ำประกัน จนกว่าเหยื่อจะหมดตัว

1.3 การหลอกโอนเงินเพื่อหารายได้พิเศษ (Ponzi Scheme & Task Scams)

มักมาในรูปแบบ SMS หรือโฆษณาชวนทำงานง่ายๆ เช่น "กดไลก์ กดแชร์ ได้เงินจริง" หรือ "แพ็กสบู่ที่บ้าน" ในช่วงแรกจะมีการโอนเงินค่าตอบแทนให้จริง (Micro-payment) เพื่อล่อให้เหยื่อโอนเงินวางมัดจำหรือลงทุนในระดับที่สูงขึ้น (VIP Level) ซึ่งแท้จริงแล้วคือรูปแบบหนึ่งของ แชร์ลูกโซ่ดิจิทัล

1.4 การหลอกกู้เงินออนไลน์ (Loan Scams) อาชญากรอาศัยภาวะความเดือดร้อนทางการเงินของประชาชน สร้างแอปพลิเคชันกู้เงินปลอม หรือส่ง SMS อนุมัติวงเงินกู้ เมื่อเหยื่อกดลิงก์เข้าไป จะถูกหลอกให้โอนเงินค่าธรรมเนียม ค่าปลดล็อกรหัส หรือค่าค้ำประกันสัญญา สุดท้ายไม่ได้เงินกู้และเสียเงินที่มีอยู่ไป

2.การฟิชชิง การฟิชชิงเป็นการส่งข้อความหรืออีเมลปลอมเพื่อหลอกให้ผู้เสียหายเปิดเผยข้อมูลส่วนบุคคลหรือข้อมูลทางการเงิน ซึ่งมักแฝงมาในรูปแบบของลิงก์เว็บไซต์ปลอม เป็นรูปแบบหนึ่งของวิศวกรรมสังคม (Social Engineering) ที่ผู้กระทำความผิดส่งข้อความสื่อสารโดยปลอมแปลงเป็นบุคคลหรือองค์กรที่น่าเชื่อถือ (Trustworthy Entity) ไปยังเหยื่อ เพื่อหลอกลวงให้เหยื่อเปิดเผยข้อมูลสำคัญ เช่น รหัสผ่าน เลขบัตรเครดิต หรือข้อมูลส่วนบุคคล ความอันตรายของ Phishing คือการที่แฮกเกอร์ไม่ได้พยายาม "เจาะระบบคอมพิวเตอร์" ที่มี Firewall หนาแน่น แต่เลือกที่จะ "เจาะจิตใจมนุษย์" ซึ่งมักเป็นจุดที่เปราะบางที่สุดในระบบรักษาความปลอดภัย (The Weakest Link)

3.การโจมตีระบบคอมพิวเตอร์ ความพยายามในการบุกรุก ทำลาย เปลี่ยนแปลง หรือเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ เครือข่าย หรืออุปกรณ์สารสนเทศโดยมิชอบ เป้าหมายของการโจมตีมักมุ่งไปที่การทำลายองค์ประกอบสำคัญ 3 ประการของความมั่นคงปลอดภัยสารสนเทศ หรือที่เรียกว่า CIA Triad:

3.1 Confidentiality (การรักษาความลับ): การแอบดูหรือขโมยข้อมูลที่สำคัญ

3.2 Integrity (ความถูกต้องครบถ้วน): การแก้ไขดัดแปลงข้อมูลเพื่อบิดเบือนข้อเท็จจริง

3.3 Availability (ความพร้อมใช้งาน): การทำให้ระบบล่มจนไม่สามารถให้บริการได้

4. การละเมิดข้อมูลส่วนบุคคล การละเมิดมาตรการรักษาความมั่นคงปลอดภัยที่ทำให้เกิดการสูญหาย การเข้าถึง การใช้ การเปลี่ยนแปลงแก้ไข หรือการเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากความตั้งใจ (การโจมตีทางไซเบอร์) หรือความประมาทเลินเล่อ (อุบัติเหตุทางเทคนิค) ข้อมูลส่วนบุคคล (Personal Data) ครอบคลุมถึง:

4.1 ข้อมูลระบุตัวตน: ชื่อ-นามสกุล, เลขบัตรประชาชน, เลขพาสปอร์ต

4.2 ข้อมูลการติดต่อ: ที่อยู่, เบอร์โทรศัพท์, อีเมล

4.3 ข้อมูลทางการเงิน: เลขบัญชีธนาคาร, ประวัติการทำธุรกรรม

4.4 ข้อมูลอ่อนไหว (Sensitive Data): ประวัติการรักษาพยาบาล, ข้อมูลชีวภาพ (ลายนิ้วมือ/ใบหน้า), ความเห็นทางการเมือง

สาเหตุของอาชญากรรมทางเทคโนโลยีในประเทศไทย สาเหตุสำคัญของการเกิดอาชญากรรมทางเทคโนโลยี ได้แก่ อาชญากรรมทางเทคโนโลยีในประเทศไทยเป็นปัญหาที่มีความซับซ้อนและเปลี่ยนแปลงรูปแบบตลอดเวลา การแก้ไขปัญหาอย่างยั่งยืนจึงต้องอาศัยการบูรณาการ 3 ส่วนคือ "กฎหมายที่เข้มงวด" (พ.ร.ก. มาตรการป้องกันฯ 2566), "เทคโนโลยีที่ปลอดภัย" (MFA, Zero Trust) และ "ประชาชนที่เท่าทัน" (Digital Literacy) หากขาดส่วนใดส่วนหนึ่งไป ประเทศไทยจะยังคงเป็นเป้าหมายสำคัญของอาชญากรไซเบอร์ทั่วโลก

ผลกระทบของอาชญากรรมทางเทคโนโลยี อาชญากรรมทางเทคโนโลยีไม่ได้ส่งผลเสียเพียงแค่ตัวเงินที่สูญหายไปเท่านั้น แต่ยังมีผลกระทบที่ซับซ้อนและแผ่ขยายไปถึงโครงสร้างสังคมและความเชื่อมั่นในระดับสากล โดยสามารถจำแนกผลกระทบออกเป็น 4 มิติหลัก ดังนี้:

1. ผลกระทบด้านเศรษฐกิจ (Economic Impact) มิตินี้เป็นผลกระทบที่สามารถวัดมูลค่าเป็นตัวเลขได้ชัดเจนที่สุด แต่ความเสียหายจริงมักสูงกว่าที่รายงานไว้:

- **ความเสียหายโดยตรง (Direct Financial Loss):** เงินที่ถูกโอนออกจากบัญชีเหยื่อผ่านการฉ้อโกง หรือค่าไถ่ที่ต้องจ่ายให้กับกลุ่ม Ransomware เพื่อกู้คืนข้อมูล
- **ต้นทุนในการกู้คืนและปรับปรุงระบบ (Recovery Costs):** องค์กรที่ถูกโจมตีต้องเสียค่าใช้จ่ายมหาศาลในการจ้างผู้เชี่ยวชาญด้านนิติวิทยาศาสตร์ดิจิทัล (Digital Forensics) เพื่อสืบสวนหาสาเหตุ รวมถึงการลงทุนในระบบความปลอดภัยใหม่ทั้งหมด

- **การสูญเสียโอกาสทางธุรกิจ (Opportunity Cost):** เมื่อระบบล่ม (Downtime) ธุรกิจไม่สามารถดำเนินการได้ ส่งผลให้สูญเสียรายได้ตามช่วงเวลาที่หยุดชะงัก และอาจเสียลูกค้าให้แก่คู่แข่ง

2. ผลกระทบด้านจิตวิทยาและสังคม (Psychological and Social Impact)

เป็นผลกระทบที่เยียวยาได้ยากที่สุด เนื่องจากส่งผลต่อความรู้สึกและความสัมพันธ์ในสังคม:

- **ภาวะวิกฤตทางจิตใจของเหยื่อ:** ผู้เสียหายหลายรายประสบภาวะซึมเศร้า วิตกกังวล หรือเสียความมั่นใจในการใช้เทคโนโลยี บางรายอาจสูญเสียเงินเก็บทั้งชีวิตนำไปสู่ปัญหาครอบครัวหรือการตัดสินใจจบชีวิตตนเอง
- **การสูญเสียความเชื่อมั่น (Loss of Trust):** เมื่อเกิดเหตุข้อมูลรั่วไหลหรือการหลอกลวงบ่อยครั้ง ประชาชนจะเริ่มขาดความเชื่อมั่นในระบบสถาบันการเงิน ระบบรัฐบาลดิจิทัล (E-Government) และธุรกรรมออนไลน์ ซึ่งเป็นอุปสรรคสำคัญต่อการขับเคลื่อนเศรษฐกิจดิจิทัลของประเทศ
- **การบิดเบือนข้อมูลทางสังคม (Social Manipulation):** การใช้ Fake News หรือ Deepfake เพื่อสร้างความแตกแยกทางการเมืองหรือสร้างความเกลียดชัง (Hate Speech) ส่งผลต่อความสงบสุขและสันติภาพในสังคม

3. ผลกระทบด้านความมั่นคงระดับชาติ (National Security Impact)

ในยุคสงครามไซเบอร์ (Cyber Warfare) อาชญากรรมทางเทคโนโลยีถูกใช้เป็นเครื่องมือทำลายล้างคู่ต่อสู้:

- **การโจมตีโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure):** หากระบบจ่ายไฟฟ้า ประปา หรือการควบคุมการบินถูกแฮ็ก จะส่งผลกระทบต่อความปลอดภัยสาธารณะอย่างรุนแรง
- **การจารกรรมข้อมูลความลับ (Espionage):** การขโมยข้อมูลลับทางราชการหรือความลับทางการทหาร ส่งผลต่อขีดความสามารถในการแข่งขันและความมั่นคงของประเทศในเวทีโลก
- **การฟอกเงินและการสนับสนุนการก่อการร้าย:** เงินที่ได้จากอาชญากรรมไซเบอร์มักถูกแปลงเป็นคริปโทเคอร์เรนซีเพื่อใช้สนับสนุนกิจกรรมผิดกฎหมายอื่นๆ ต่อไป

4. ผลกระทบด้านกฎหมายและสิทธิมนุษยชน (Legal and Human Rights Impact)

- **การละเมิดสิทธิส่วนบุคคล:** การนำข้อมูลส่วนตัวไปเผยแพร่หรือขายต่อ ถือเป็นการละเมิดศักดิ์ศรีความเป็นมนุษย์และสิทธิขั้นพื้นฐาน

- **ภาระของกระบวนการยุติธรรม:** ปริมาณคดีออนไลน์ที่เพิ่มขึ้นนับแสนคดีต่อปี สร้างภาระมหาศาลให้แก่พนักงานสอบสวน อัยการ และศาล ทำให้การดำเนินคดีในภาพรวมล่าช้าลง

กฎหมายและหน่วยงานที่เกี่ยวข้องในประเทศไทย

ประเทศไทยมีกฎหมายที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยีหลายฉบับ เช่น

- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

หน่วยงานที่มีบทบาทสำคัญ ได้แก่ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงานตำรวจแห่งชาติ และสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

การแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีควรดำเนินการในหลายระดับ หัวข้อ "การแก้ไขปัญหาอาชญากรรมทางเทคโนโลยี" (Solutions and Mitigation Strategies) เป็นส่วนสุดท้ายที่จะเติมเต็มให้บทความวิชาการของคุณสมบูรณ์และครบถ้วนทั้ง 10 หน้า โดยเนื้อหาในส่วนนี้จะมุ่งเน้นไปที่การตอบโต้ภัยคุกคามในเชิงโครงสร้างและเชิงปฏิบัติครับ

การแก้ไขปัญหาอาชญากรรมทางเทคโนโลยี: แนวทางบูรณาการเพื่อความยั่งยืน

(Solutions to Technology Crime: Integrated Approaches for Sustainability)

การแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีไม่สามารถอาศัยเพียงเครื่องมือใดเครื่องมือหนึ่งได้ แต่จำเป็นต้องใช้วิธีการแบบองค์รวม (Holistic Approach) ที่ผสมผสานทั้งด้านกฎหมาย เทคโนโลยี และทรัพยากรมนุษย์ ดังนี้:

1. การตอบโต้ด้วยกลไกทางกฎหมายและนโยบาย (Legal and Policy Framework)

กฎหมายต้องมีความยืดหยุ่นและก้าวทันเล่ห์เหลี่ยมของอาชญากร:

การบังคับใช้กฎหมายข้ามพรมแดน: การทำข้อตกลงความร่วมมือระหว่างประเทศ (Mutual Legal Assistance Treaty - MLAT) เพื่อให้การขอข้อมูลการจราจรทางคอมพิวเตอร์และการส่งผู้ร้ายข้ามแดนทำได้รวดเร็วขึ้น

การปรับปรุงบทลงโทษ: การกำหนดโทษที่รุนแรงขึ้นสำหรับกลุ่มอาชญากรที่เป็นองค์กร (Organized Crime) และผู้ที่ให้การสนับสนุน เช่น เจ้าของบัญชีม้า หรือผู้ให้บริการระบบอินเทอร์เน็ตที่จงใจละเลยการตรวจสอบ

การบังคับใช้มาตรการเชิงรุก: เช่น พ.ร.ก. มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 ที่อนุญาตให้ระงับธุรกรรมได้ทันทีโดยไม่ต้องรอแจ้งความ ซึ่งเป็นการตัดวงจรการฟอกเงิน

2. การใช้มาตรการทางเทคโนโลยีขั้นสูง (Technological Solutions)

เทคโนโลยีที่ถูกนำมาใช้โจมตี ก็สามารถนำมาใช้ป้องกันได้เช่นกัน:

การนำ AI และ Machine Learning มาใช้: หน่วยงานภาครัฐและสถาบันการเงินควรใช้ระบบ AI ในการตรวจจับความผิดปกติ (Anomaly Detection) ของธุรกรรมทางการเงินหรือพฤติกรรมการใช้งานในระบบเครือข่าย เพื่อสกัดกั้นก่อนเกิดความเสียหาย

สถาปัตยกรรมแบบ Zero Trust: องค์กรควรเปลี่ยนแนวคิดจากการป้องกันขอบเขต (Perimeter Defense) มาเป็น Zero Trust หรือ "การไม่ไว้วางใจสิ่งใดเลย" ซึ่งต้องมีการยืนยันตัวตนในทุกขั้นตอนการเข้าถึงข้อมูล

การยืนยันตัวตนหลายชั้น (MFA): การรณรงค์ให้ใช้การยืนยันตัวตนแบบชีวมาตร (Biometrics) หรือ Token แทนการใช้รหัสผ่านเพียงอย่างเดียว ซึ่งจะลดโอกาสการถูก Phishing ได้มากกว่า 90%

3. การสร้างภูมิคุ้มกันทางดิจิทัล (Cyber Immunity and Literacy)

มนุษย์คือจุดอ่อนที่สุดและเป็นจุดแข็งที่สุดในเวลาเดียวกัน:

การเพิ่มทักษะ Digital Literacy: บรรจุวิชาความรู้เท่าทันภัยไซเบอร์ลงในหลักสูตรการศึกษาตั้งแต่ระดับประถมศึกษา เพื่อให้พลเมืองดิจิทัลรุ่นใหม่มี "ภูมิคุ้มกัน" ต่อกลโกง

การสร้างวัฒนธรรมความปลอดภัย (Cybersecurity Culture) : ในระดับองค์กร ต้องมีการฝึกซ้อมรับมือเหตุการณ์จำลอง (Cyber Drill) เป็นประจำเพื่อให้พนักงานรู้วิธีการตอบโต้ที่ถูกต้องเมื่อเผชิญกับการโจมตีจริง

แคมเปญสร้างความตระหนักรู้: รัฐต้องประชาสัมพันธ์รูปแบบกลโกงใหม่ๆ ผ่านทุกช่องทางสื่อสารอย่างต่อเนื่อง เพื่อให้ประชาชน "ไม่เชื่อ ไม่รีบ ไม่โอน"

4. ความร่วมมือระหว่างภาครัฐและภาคเอกชน (Public-Private Partnership)

การแบ่งปันข้อมูลภัยคุกคาม (Threat Intelligence Sharing): ภาคธนาคาร ผู้ให้บริการโทรคมนาคม และตำรวจ ต้องมีการเชื่อมโยงฐานข้อมูลอาชญากรและหมายเลขโทรศัพท์ต้องสงสัยร่วมกันแบบ Real-time เพื่อระงับภัยได้ทันท่วงที

การควบคุมซิมการ์ดและบัญชีธนาคาร: เพิ่มความเข้มงวดในการยืนยันตัวตน (KYC) สำหรับการเปิดบัญชีหรือจดทะเบียนซิมจำนวนมาก เพื่อลดจำนวนบัญชีม้าและซิมผีในระบบ

อาชญากรรมทางเทคโนโลยีเป็นปัญหาที่ท้าทายต่อสังคมไทยในยุคดิจิทัล การป้องกันและแก้ไขปัญหาดังกล่าวจำเป็นต้องอาศัยความร่วมมือจากทุกภาคส่วน การส่งเสริมความรู้ด้านดิจิทัล การพัฒนาระบบความปลอดภัย และการบังคับใช้กฎหมายอย่างจริงจัง จะช่วยลดความเสี่ยงและสร้างสังคมดิจิทัลที่ปลอดภัยยิ่งขึ้น

เอกสารอ้างอิง

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (2565). *รายงานสถานการณ์อาชญากรรมทางเทคโนโลยีในประเทศไทย*.

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2566). *แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์*.

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม.

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562.

Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press.