ภัยคุกคามทางไซเบอร์ที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต*

Cyber Threats Affecting Internet Users' Cyber Threat Awareness

[1]กฤชณัท เหล่ากอ, สมบูรณ์ สุขสำราญ
[1]Kritchanat Laoko, Somboon Suksamran
[1]วิทยาลัยการเมืองและการปกครอง มหาวิทยาลัยราชภัฏสวนสุนันทา
[1]Department of Politics and Governance, Suan Sunandha Rajabhat University
[1]Corresponding Author's E-mail: nawaphorn.1818@gmail.com

บทคัดย่อ

ภัยคุกคามทางไซเบอร์ที่มีผลต่อการตระหนักรู้ของผู้ใช้อินเทอร์เน็ต เมื่อกล่าวถึงประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต กล่าวคือการโจมตีทางไซเบอร์ ที่มีรูปแบบการพัฒนาการโจมตี เพื่อเปิดช่องโหว่ทางอินเทอร์เน็ตหลากหลายรูปแบบทำให้ผู้ใช้อินเทอร์เน็ตไม่สามารถระวังหรือป้องกันการโจมตีทางไซเบอร์ได้และได้รับความเสียหายที่ไม่คาดคิด ปัจจุบันผู้ใช้งานอินเทอร์เน็ตไม่สามารถประเมินสถานการณ์หรือความเสียหายที่เกิดขึ้นได้และผู้ใช้งานอินเทอร์เน็ตส่วนใหญ่ขาดความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ซึ่งส่งผลกระทบต่อความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต ดังนั้นการตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตจะทำให้ผู้ใช้อินเทอร์เน็ตมีความรู้ และทราบถึงภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อตนเอง รวมถึงเข้าใจถึงปัญหาที่เกิดความเสียหายจากภัยคุกคามทางไซเบอร์ ไม่ว่าจะเป็นการเปิดเผยข้อมูลบนสาธารณะ การทำธุรกรรมออนไลน์ การป้องกันให้ไม่ผู้อื่นทราบข้อมูลส่วนตัว และการติดตามข้อมูลข่าวสารการโจมตีรูปแบบใหม่ ๆ การดาวโหลดโปรแกรมที่ถูกต้องมาจากผู้ผลิตโดยตรงป้องกันความเสี่ยงการฝังไวรัสที่ไม่คาดคิดติดมากับโปรแกรมและสามารถป้องกันภัยคุกคามจากผู้ที่ไม่หวังดีที่จะเกิดผลกระทบความเสียหายโดยไม่คาดคิดได้

คำสำคัญ: ภัยคุกคามทางไซเบอร์; การตระหนัก; ผู้ใช้อินเทอร์เน็ต

ABTRACT

Cyber threats affecting the awareness of Internet users When talking about the experience of cyber threats of Internet users, it is cyber attacks that have various forms of attack development to open vulnerabilities in the Internet, causing Internet users to be unable to be careful or prevent cyber attacks and receive unexpected damage. Currently, Internet users cannot assess the situation or damage that occurs and most Internet users lack knowledge about cyber threats, which affects the awareness of cyber threats of Internet users. Therefore, cyber threat awareness of Internet users will make Internet users have knowledge and be aware of cyber threats that affect them, including understanding the problems caused by cyber threats, whether it is disclosing information to the public, making online transactions, preventing others from knowing personal information, and

* Received March 28, 2025; Revised July 27, 2025; Accepted July 28, 2025

following up on news of new forms of attacks. Downloading legitimate programs directly from the manufacturer prevents the risk of unexpected viruses attached to the program and can prevent threats from ill-wishers that will cause unexpected damage.

Keywords: Cyber Threats; Awareness; Internet Users

บทนำ

ปัจจุบันอินเทอร์เน็ต (Internet) เป็นเสมือนปัจจัยที่ 5 ของการดำเนินชีวิตของมนุษย์ทั่วโลกไม่เว้นแม้แต่คนไทย โดยในประเทศไทยได้มีการสำรวจการมีการใช้เทคโนโลยีสารสนเทศและการสื่อสารในครัวเรือน พ.ศ. 2567 (ไตรมาส 4) พบว่าประชาชนอายุ 6 ปีขึ้นไป ประมาณ 66.1 ล้านคน พบว่า มีผู้ใช้อินเทอร์เน็ต 60.0 ล้านคน (ร้อยละ 90.9) ใช้โทรศัพท์มือถือ 63.2 ล้านคน (ร้อยละ 95.7) และมีโทรศัพท์มือถือ 58.8 ล้านคน (ร้อยละ 89.0) และเมื่อพิจารณาแนวโน้มการใช้อินเทอร์เน็ต ระหว่างปี 2566 (ไตรมาส 4) – 2567 (ไตรมาส 4) พบว่า ผู้ใช้อินเทอร์เน็ตมีแนวโน้มเพิ่มขึ้น จากร้อยละ 89.5 ในปี 2566 (ไตรมาส 4) เป็นร้อยละ 90.9 ในปี 2567 (ไตรมาส 4) แสดงให้เห็นว่าความแพร่หลายของเทคโนโลยีอินเทอร์เน็ตในสังคมไทยยังคงเพิ่มขึ้นอย่างต่อเนื่อง (สำนักงานสถิติและสังคมแห่งชาติ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, 2567) อย่างไรก็ตาม แม้การเข้าถึงอินเทอร์เน็ตจะส่งผลให้ประชาชนสามารถเชื่อมโยงกับโลกดิจิทัลได้อย่างสะดวกและรวดเร็ว แต่อีกด้านหนึ่งก็ทำให้ปัญหาอาชญากรรมทางเทคโนโลยีเพิ่มสูงขึ้นตามไปด้วย โดยเมื่อวันที่ 15 ธันวาคม 2567 เว็บไซต์รัฐบาลไทยรายงานว่า นายคารม พลพรกลาง รองโฆษกประจำสำนักนายกรัฐมนตรี ได้เปิดเผยยอดการแจ้งความออนไลน์สะสมผ่านเว็บไซต์ของกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี ตั้งแต่วันที่ 1 มีนาคม 2565 ถึงวันที่ 30 พฤศจิกายน 2567 ว่ามีจำนวนทั้งสิ้น 739,494 เรื่อง มูลค่าความเสียหายรวม 77,360,070,295 บาท หรือเฉลี่ยวันละประมาณ 77 ล้านบาท และมีผลการอายัดบัญชีที่เกี่ยวข้องได้ถึง 560,412 บัญชี คิดเป็นยอดเงินที่สามารถอายัดได้ 8,627,715,890 บาท เฉพาะในช่วงเดือนพฤศจิกายน 2567 เพียงเดือนเดียว พบการแจ้งความออนไลน์จำนวน 31,353 เรื่อง มูลค่าความเสียหายรวม 2,540,251,400 บาท หรือเฉลี่ยวันละประมาณ 85 ล้านบาท โดยสามารถอายัดบัญชีได้ 16,229 บัญชี มียอดขออายัดเงินรวม 1,864,371,518 บาท และสามารถอายัดได้จริงจำนวน 383,933,622 บาท ทั้งนี้ ประเภทคดีออนไลน์ที่มีการแจ้งมากที่สุด 5 อันดับแรก ได้แก่ (1) การหลอกลวงซื้อขายสินค้า/บริการทั่วไป มูลค่าความเสียหาย 146.8 ล้านบาท (2) การหลอกให้โอนเงินเพื่อทำงานหารายได้พิเศษ มูลค่า 526.7 ล้านบาท (3) การข่มขู่ทางโทรศัพท์หรือ Call Center มูลค่า 444.3 ล้านบาท (4) การหลอกให้กู้เงิน มูลค่า 99.8 ล้านบาท และ (5) การหลอกให้โอนเงินเพื่อรับรางวัลหรือเพื่อวัตถุประสงค์อื่น มูลค่า 221.7 ล้านบาท (ประชาไท, 2567) จากข้อมูลนี้เราจะเห็นได้ว่าแม้การเข้าถึงอินเทอร์เน็ตจะเป็นเรื่องที่ง่ายและรวดเร็วและมีประโยชน์อย่างมาก แต่ในทางกลับกันสื่ออินเทอร์เน็ตก็สามารถสร้างความเสียหายต่อตนเองและผู้อื่นได้อีกด้วย โดยความเสียหายที่เกิดขึ้นมักจะเกิดจากพฤติกรรมของผู้ใช้อินเทอร์เน็ตเองหรือเกิดจากาถูกโจมตี การจารกรรมข้อมูลทางคอมพิวเตอร์ของผู้ไม่ประสงค์ดี โดยเป็นอาชญากรมทางคอมพิวเตอร์ที่เป็นภัยคุกคามทางด้านเทคโนโลยีสารสนเทศได้เช่นกัน

จากสภาพการณ์ในปัจจุบันจะเห็นได้ว่าคดีอาชญากรรมทางคอมพิวเตอร์เกิดขึ้นอยู่บ่อยครั้ง สำนักงานตำรวจแห่งชาติจึงได้ปรับปรุงโครงสร้างองค์กร โดยการจัดตั้งหน่วยงานระดับ "กองบัญชาการ" ขึ้นใหม่ คือ "กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.)" หรือเป็นที่รู้จักในชื่อ "กองบัญชาการตำรวจไซเบอร์" เพื่อเพิ่มศักยภาพในการวิเคราะห์สาเหตุ รูปแบบ เครือข่ายการกระทำอาชญากรรมทางเทคโนโลยีสารสนเทศได้อย่างเป็นระบบ ทำหน้าที่เป็นหน่วยงานหลักในการสืบสวนสอบสวน

คดีอาชญากรรมทางเทคโนโลยีที่มีความสลับซับซ้อน มีประชาชนได้รับความเสียหายจำนวนมาก และมีมูลค่าความเสียหายสูง ให้การสนับสนุนสถานีตำรวจในการป้องกันปราบปรามคดีอาชญากรรมทางเทคโนโลยีในเบื้องต้นหากเป็นคดีที่ไม่สลับซับซ้อน และเป็นศูนย์กลางประสานความร่วมมือกับหน่วยงานต่าง ๆ ในการสืบสวนสอบสวนคดีอาชญากรรมทางเทคโนโลยี อีกทั้งได้มีการปรับปรุงโครงสร้างและกำหนดอำนาจหน้าที่ของกองบังคับการและศูนย์ที่เกี่ยวข้องกับการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีที่มีอยู่เดิมเพื่อให้สอดคล้องกับสถานการณ์ปัจจุบันด้วย (สุภาพิชญ์ ถิระวัฒน์, 2564) โดยตำรวจไซเบอร์จะมีหน้าที่สืบสวนสอบสวน และปราบปรามอาชญากรรมทางเทคโนโลยี หรืออาชญากรรมที่กระทำผ่านเครือข่ายคอมพิวเตอร์และอินเทอร์เน็ต เช่น การโจรกรรมข้อมูล การเผยแพร่ข้อมูลเท็จ การล่วงละเมิดทางเพศบนอินเทอร์เน็ต โดยเฉพาะพฤติกรรมการฉ้อโกงผ่านเครือข่ายอินเทอร์เน็ตในลักษณะของการชักชวนให้ลงทุน ซึ่งผู้กระทำผิดใช้เทคโนโลยีและช่องทางออนไลน์เป็นเครื่องมือในการล่อลวงเหยื่อ โดยเน้นไปที่วิธีการสร้างความน่าเชื่อถือ การโน้มน้าวใจ และการจัดการกับข้อมูลเท็จหรือบิดเบือนที่เผยแพร่ผ่านสื่อออนไลน์ เพื่อดึงดูดให้เหยื่อหลงเชื่อและโอนเงินให้ผู้กระทำผิด (ธีระ กุลสวัสดิ์, 2567) จะเห็นได้ว่าในปัจจุบัน ปัญหาอาชญากรรมทางเทคโนโลยีมีแนวโน้มเพิ่มสูงขึ้นอย่างต่อเนื่องและมีความซับซ้อนมากยิ่งขึ้น ส่งผลให้เกิดความเสียหายต่อประชาชนจำนวนมาก ด้วยเหตุนี้ รัฐบาลจึงมีการปรับปรุงโครงสร้างหน่วยงานภายในสำนักงานตำรวจแห่งชาติ โดยอาศัยพระราชกฤษฎีกาแบ่งส่วนราชการสำนักงานตำรวจแห่งชาติ (ฉบับที่ 5) พ.ศ. 2563 เพื่อยกระดับขีดความสามารถในการรับมือกับภัยคุกคามจากอาชญากรรมไซเบอร์อย่างเป็นระบบ โดยจัดตั้งหน่วยงานเฉพาะทางคือ “ตำรวจไซเบอร์” หรือ กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี เพื่อทำหน้าที่วางแผน ควบคุม ตรวจสอบ และให้คำแนะนำเชิงยุทธศาสตร์ในการดำเนินการเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีทั่วประเทศ (ราชกิจจานุเบกษา, 2563) ตำรวจไซเบอร์จึงมีภารกิจหลักในการสืบสวนสอบสวนคดีอาชญากรรมที่เกิดจากการใช้เทคโนโลยี โดยเฉพาะคดีที่มีความซับซ้อนและมีมูลค่าความเสียหายสูง หน่วยงานนี้มีหน้าที่ดำเนินการตามกฎหมายที่เกี่ยวข้อง เช่น กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และกฎหมายอาญาอื่น ๆ ที่เกี่ยวเนื่อง โดยใช้เทคโนโลยีสารสนเทศและเครื่องมือพิเศษสนับสนุนการสืบสวนสอบสวน รวมถึงการรวบรวม ตรวจสอบ วิเคราะห์หลักฐานดิจิทัล และการพัฒนาบุคลากรให้มีความรู้ความสามารถในการรับมือกับอาชญากรรมในยุคดิจิทัล ทั้งนี้ ตำรวจไซเบอร์จะเน้นรับผิดชอบเฉพาะคดีที่มีลักษณะซับซ้อน ส่วนคดีทั่วไปที่เกี่ยวข้องกับการกระทำผิดผ่านเครือข่ายอินเทอร์เน็ต เช่น การหลอกลวงออนไลน์ จะเน้นการสนับสนุนข้อมูลเชิงเทคนิคและประสานงานกับหน่วยงานอื่นเพื่อสืบหาตัวผู้กระทำผิดอย่างมีประสิทธิภาพ

จากทั้งหมดที่กล่าวมานี้เราจะเห็นได้ว่าในประเทศไทย ปัญหาอาชญากรรมทางเทคโนโลยีเริ่มทวีความรุนแรงมากขึ้น โดยเฉพาะในยุคที่เทคโนโลยีสารสนเทศพัฒนาอย่างรวดเร็ว การกระทำความผิดผ่านเครือข่ายคอมพิวเตอร์และอินเทอร์เน็ตจึงเกิดขึ้นอย่างต่อเนื่อง เช่น การโจรกรรมข้อมูล การเผยแพร่ข้อมูลเท็จ การล่วงละเมิดทางเพศในโลกออนไลน์ และการฉ้อโกงผ่านระบบอินเทอร์เน็ต ด้วยเหตุนี้ หน่วยงานภาครัฐจึงได้ปรับโครงสร้างเพื่อรับมือกับภัยคุกคามดังกล่าว โดยจัดตั้ง “กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี” หรือ “ตำรวจไซเบอร์” ขึ้นตามพระราชกฤษฎีกาแบ่งส่วนราชการสำนักงานตำรวจแห่งชาติ พ.ศ. 2563 เพื่อให้สามารถรับมือกับปัญหาอาชญากรรมทางเทคโนโลยีได้อย่างเป็นระบบและมีประสิทธิภาพยิ่งขึ้น โดยมีเป้าหมายเพื่อวิเคราะห์รูปแบบและเครือข่ายของอาชญากรรม ตลอดจนยกระดับกระบวนการสืบสวนสอบสวนให้สามารถรองรับความซับซ้อนของคดีที่มีความเสียหายสูง และส่งผลกระทบต่อประชาชนจำนวนมาก บทบาทของตำรวจไซเบอร์ไม่ได้จำกัดเพียงการดำเนินคดีเท่านั้น หากแต่ยังครอบคลุมถึงการวางยุทธศาสตร์ระดับชาติ การควบคุม ตรวจสอบ ให้คำแนะนำ และเสนอแนะแนวทางการดำเนินงานแก่

หน่วยงานต่าง ๆ ภายใต้กรอบของกฎหมายที่เกี่ยวข้อง เช่น กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายความมั่นคงทางไซเบอร์ และกฎหมายอาญาอื่น ๆ ที่เกี่ยวข้อง ตำรวจไซเบอร์ยังทำหน้าที่ในการรวบรวม ตรวจสอบ และวิเคราะห์ข้อมูลการกระทำความผิดทางเทคโนโลยี รวมถึงการพิสูจน์หลักฐานดิจิทัล และการตรวจสถานที่เกิดเหตุ เพื่อสนับสนุนกระบวนการสืบสวนสอบสวนของหน่วยงานต่าง ๆ ให้มีความแม่นยำและทันต่อสถานการณ์

ดังนั้นผู้วิจัยจึงสนใจที่จะศึกษาเรื่อง ภัยคุกคามทางไซเบอร์ที่มีผลต่อการตระหนักรู้ของผู้ใช้อินเทอร์เน็ต เพื่อความมั่นคงปลอดภัยทางไซเบอร์ และนำไปใช้ประโยชน์ในการวางแผนในการสร้างการตระหนักถึงภัยคุกคามทางไซเบอร์ให้กับผู้ใช้อินเทอร์เน็ตต่อไป

แนวคิดเกี่ยวกับความตระหนัก (Awareness)

แนวคิดเกี่ยวกับความตระหนักมีความสำคัญต่อการวิเคราะห์บทความนี้ เนื่องจากเป็นพื้นฐานในการทำความเข้าใจพฤติกรรมของผู้ใช้อินเทอร์เน็ตต่อภัยคุกคามทางไซเบอร์ นักวิชาการได้ให้คำนิยามความตระหนักไว้หลากหลาย ดังนี้

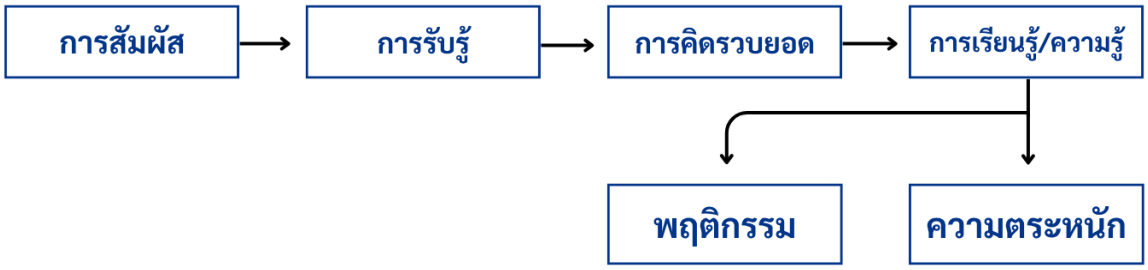
ความหมายของความตระหนัก

พจนานุกรมราชบัณฑิตสถาน พ.ศ. 2554 ได้ให้ความหมายของคำว่า ความตระหนัก ซึ่งผู้วิจัยสรุปได้ว่า ความตระหนักเป็นการรู้ประจักษ์ชัดรู้ชัดแจ้ง จึงสอดคล้องกับพจนานุกรม ของ Good (1973, p. 54) ที่ผู้วิจัยสรุปใจความได้ว่า หมายถึง การแสดงออกจากการระลึกได้หรือจดจำได้ และยังมีผู้นิยามความหมายของความตระหนักไว้อีก ดังนี้

Bloom (1971, p. 271 อ้างถึงใน สุพัตรา ถนอมวงค์, 2551, น.10) ได้ให้นิยามของคำว่า ความตระหนัก ซึ่งผู้วิจัยสรุปใจความได้ว่าภาพจำสุดทางภาคอารมณ์ ซึ่งความตระหนักนั้นคล้ายกับอารมณ์ความรู้สึก (Affective Domain) แต่ความตระหนักต่างกับความรู้สึกตรงที่ความตระหนักไม่จำเป็นต้องเน้นปรากฏการณ์หรือสิ่งหนึ่งสิ่งใด แต่ความตระหนักจะเกิดขึ้นเมื่อมีสิ่งเร้าให้เกิดความตระหนัก

ปัจจัยที่ทำให้เกิดความตระหนัก

Good, 1973 (อ้างถึงใน สุธาสินี อินทร์ผูก, 2548) พจนานุกรม ของ Good (1973) ได้ประมวลขั้นตอนของกระบวนการเกิดความตระหนัก ดังนี้



แผนภาพที่ 1 ขั้นตอนของกระบวนการเกิดความตระหนัก

ในลักษณะเช่นนี้ความตระหนักจึงเป็นผลของกระบวนการทางปัญญา กล่าวคือ เมื่อบุคคลได้รับการกระตุ้นจากสิ่งเร้า หรือรับสัมผัสจากสิ่งเร้าแล้วเกิดการรับรู้ขึ้นแล้วจะนำไปสู่การเกิดความเข้าใจในสิ่งเร้านั้น และนำไปสู่การเรียนรู้เป็นขั้นตอนต่อไป และเมื่อบุคคลเกิดมีความรู้ในสิ่งนั้นแล้วก็จะมีผลไปสู่ความตระหนักในที่สุด ซึ่งทั้งความรู้และความตระหนักจะนำไปสู่การกระทำหรือพฤติกรรมของบุคคลที่มีต่อสิ่งเร้า

นั้น ๆ ต่อไป และจากการศึกษาของพัฒนศักดิ์ บุบผาสุวรรณ (2546) ได้กล่าวถึง ปัจจัยทางพฤติกรรมศาสตร์ที่มีผลต่อความตระหนัก ประกอบด้วย ประสบการณ์ที่มีต่อการรับรู้ความเคยชินต่อสภาพแวดล้อม ถ้าบุคคลใดไม่เคยชินต่อสภาพแวดล้อมนั้นก็จะทำให้บุคคลนั้นไม่ตระหนักต่อสิ่งที่เกิดขึ้น ความใส่ใจและการให้คุณค่า ถ้ามนุษย์มีความใส่ใจในเรื่องใดมากก็จะมีความตระหนักในเรื่องนั้นมาก ลักษณะและรูปแบบของสิ่งเร้า ถ้าสิ่งเร้านั้นสามารถทำให้ผู้พบเห็นเกิดความสนใจย่อมทำให้ผู้พบเห็นเกิดการรับรู้และความตระหนักขึ้น ระยะเวลาและความถี่ในการรับรู้ถ้ามนุษย์ได้รับรู้บ่อยครั้งเท่าใดก็ยิ่งทำให้มีโอกาสเกิดความตระหนักได้มากขึ้นเท่านั้น

แนวคิดเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)

การคุกคามทางไซเบอร์สามารถเกิดขึ้นได้หลายรูปแบบ แต่ละรูปแบบสามารถสร้างความเสียหายให้แก่บุคคล เศรษฐกิจ ไปจนถึงโครงสร้างพื้นฐานของประเทศต่าง ๆ ภัยคุกคามอาจเป็นการก่อวินาศกรรม การจารกรรมข้อมูลหรือรหัสสำคัญ การปล่อยข้อมูลหลอกลวง การทำลายชื่อเสียงของประเทศ องค์กร หรือบุคคล การเผยแพร่ข่าวสารอันเป็นเท็จ รวมถึงการทำลายระบบปฏิบัติการของเซิร์ฟเวอร์คอมพิวเตอร์ส่วนบุคคล และอุปกรณ์เคลื่อนที่ เช่น แท็บเล็ต หรือโทรศัพท์แบบสมาร์ตโฟนเป็นต้น

ประเภทของการเกิดภัยคุกคามทางไซเมอร์

ภัยคุกคามทางไซเบอร์ สามารถแบ่งออกเป็น 4 กลุ่ม ดังนี้

1. ภัยคุกคามที่เกิดจากการใช้โปรแกรมประยุกต์ โปรแกรมประยุกต์ (application-based threats) ที่ถูกดาวน์โหลดมาเพื่อติดตั้งบนคอมพิวเตอร์ หรืออุปกรณ์เคลื่อนที่ อาจจะถูกแอบแฝงมาด้วยโปรแกรมที่เป็นภัยคุกคาม ภัยคุกคามประเภทนี้เรียกว่ามัลแวร์ (malware) ซึ่งเป็นโปรแกรมที่ถูกออกแบบมาเพื่อทำอันตรายต่อข้อมูลในคอมพิวเตอร์ หรืออุปกรณ์เคลื่อนที่ ทำให้เกิดความขัดข้องหรือเสียหายกับระบบปฏิบัติการ นอกจากนี้โปรแกรมที่ติดมัลแวร์ยังส่งข้อความที่ไม่พึงประสงค์ออกไปยังผู้อื่น หรือขโมยข้อมูลสำคัญออกไปตัวอย่างโปรแกรมในกลุ่มนี้ ได้แก่ Venus, Worm, Trojan, Botnet หรือ spyware เป็นต้น

2. ภัยคุกคามที่เกิดจากการใช้งานเว็บไซต์ ภัยคุกคามที่เกิดจากการใช้งานเว็บไซต์ (web-based threats) เป็นภัยคุกคามที่เกิดจากการที่ผู้ใช้คอมพิวเตอร์ หรืออุปกรณ์พกพา เปิดเว็บไซต์ขึ้นมาใช้งาน ซึ่งเว็บไซต์ที่เรียกมาใช้อาจเป็นเว็บไซต์ฟิชชิ่ง (Phishing) ซึ่งถูกออกแบบให้มีลักษณะคล้ายคลึงกับเว็บไซต์จริงเพื่อหลอกให้ผู้ใช้กรอกข้อมูลเข้าสู่ระบบของผู้ไม่หวังดี เช่น หลอกให้ผู้ใช้งานล็อกอินเข้าอีเมล เฟซบุ๊ก หรือเว็บไซต์ที่เกี่ยวข้องกับธุรกรรมทางการเงิน ซึ่งจะคอยตักจับรหัสล็อกอินของผู้ใช้งานนั้น ๆ ทำให้ข้อมูลหรือบัญชีการใช้งานนั้น ๆ มีความเสี่ยงที่จะโดนขโมยข้อมูลออก

3. ภัยคุกคามจากการใช้งานเครือข่ายไร้สาย ภัยคุกคามจากการใช้งานเครือข่ายไร้สาย (Consideration of wireless network usage) อินฟราเรดผ่านอากาศในการสื่อสารข้อมูล โดยปัจจุบันเป็นเทคโนโลยีสำหรับการสื่อสาร นิยมใช้เพื่อตรวจสอบการทำงานในฟังก์ชั่นต่าง ๆ รวมถึงอุปกรณ์คอมพิวเตอร์ที่เน้นในรัศมีการใช้งานไดร์เวอร์การติดตั้งก็เหนือกว่าแบบเครือข่ายแบบมีสาย แต่ส่วนใหญ่จะเป็นส่วนที่ต้องใช้นั่นคือเรื่องของความปลอดภัยมักจะใช้ตัวกลางเป็นอากาศดังนั้นจึงมีการดักข้อมูลและเรื่องของประสิทธิภาพเพราะใช้ตัวกลางโดยรวมคือช่วงของการไหลของวิทยุ

4. ภัยคุกคามที่เกิดจากการถูกโจมตีแบบเจาะจงเป้าหมาย ภัยคุกคามที่เกิดการโจมตีแบบเจาะจงเป้าหมาย (targeted attack) ที่มาจากหลายประเทศมีมากขึ้น ผู้โจมตี หรือแฮกเกอร์ (hackers) ในประเทศต่าง ๆ จะใช้การโจมตีแบบเจาะจงเป้าหมายอย่างต่อเนื่อง สร้างความเสียหายให้แก่โครงสร้างพื้นฐาน สถาบันการเงิน และองค์กร อื่น ๆ ของภาครัฐ และภาคเอกชนในหลายประเทศ อาชญากรไซเบอร์เหล่านี้จะใช้

มาตรการที่รวดเร็วและรุนแรงในการโจรกรรมข้อมูล ภัยคุกคามประเภทนี้จัดว่า เป็นภัยคุกคามที่กระทบต่อความมั่นคงของประเทศเป็นอย่างยิ่ง

ประเภทของภัยคุกคามทางไซเบอร์

หน่วยงาน The European Computer Security Incident Response Team (ECSIRT) ซึ่งเป็นเครือข่ายความร่วมมือของหน่วยงาน CSIRT ในสหภาพยุโรปได้จำแนกตามประเภทของภัยคุกคามทางไซเบอร์ออกเป็น 10 ประเภท ซึ่งผู้วิจัยสรุปได้ดังนี้

บอตเน็ต (Botnet) คือ โปรแกรมไม่พึงประสงค์ติดตั้งอยู่ในคอมพิวเตอร์ซึ่งสามารถโจมตีได้โดยอัตโนมัติหรือรับคำสั่งจากผู้ควบคุมผ่านเครือข่ายอินเทอร์เน็ตได้จากระยะไกล

1. สแปม (Spam) คือ การส่งจดหมายอิเล็กทรอนิกส์ออกไปยังผู้รับจำนวนมากโดยผู้ที่ได้รับจดหมายเหล่านั้น ไม่ได้มีความประสงค์ที่จะได้รับ ส่วนมากเป็นการโฆษณาสินค้าและบริการ

2. โอเพ่นดีเอ็นเอสรีโซลเวอร์ (Open DNS Resolver) คือ การตั้งค่าเครื่องให้บริการ ดีเอ็นเอส (DNS) อย่างไม่เหมาะสม ทำให้ผู้อื่นสามารถส่งข้อมูลโดเมนเนมหลอกลวงให้กับเครื่องบริการดีเอ็นเอส เพื่อใช้หลอกลวงผู้ใช้งาน

3. บรูตฟอร์ซ (Brute Force) คือ โปรแกรมที่เจาะระบบเป้าหมายด้วยวิธีการสุ่มข้อมูลตามอัลกอริทึมที่ผู้โจมตีคิดค้นเพื่อให้ได้ข้อมูลสำคัญหรือข้อมูลลับของระบบเป้าหมาย เช่นบัญชีชื่อผู้ใช้งาน และรหัสผ่าน

4. มัลแวร์ยูอาร์แอล (Malware URL) คือ การที่ผู้ไม่ประสงค์ดีบุกรุกเข้าไปยังเว็บไซต์ของผู้อื่นและใช้พื้นที่ของเว็บไซต์นั้นในการเผยแพร่โปรแกรมไม่พึงประสงค์

5. สแกนนิ่ง (Scanning) คือ การตรวจสอบข้อมูลของบริการของเครื่องแม่ข่ายโดยใช้วิธีส่งข้อมูลไปสู่ระบบที่เป็นเป้าหมาย และรวบรวมข้อมูลที่ได้จากการสแกนนิ่ง เพื่อใช้เป็นข้อมูลในการเจาะระบบ

6. โอเพ่นพร็อกซี่เซิร์ฟเวอร์ (Open Proxy Server) คือ การตั้งค่าบริการเว็บพร็อกซี่ (web proxy) ไม่เหมาะสมที่ยินยอมให้ผู้ใช้งานทั่วไปเรียกใช้งาน เพื่อเข้าถึงบริการเว็บในเครือข่ายอินเทอร์เน็ตได้โดยไม่มีระบบยืนยันตัวตน (authentication)

7. ฟิชชิ่ง (Phishing) คือ เว็บไซต์ปลอมที่ต้องการหลอกลวงเพื่อขโมยข้อมูลสำคัญของผู้ใช้งาน เช่น บัญชีผู้ใช้หรือรหัสผ่าน เป็นต้น

8. สตอร์มเวิร์ม (Storm Worm) คือ โปรแกรมไม่พึงประสงค์ในลักษณะเวิร์ม (Worm) ซึ่งสามารถแพร่กระจายได้ด้วยตัวเอง สตอร์มเวิร์มมีลักษณะการทำงานในรูปแบบบอตเน็ต ต่างกันที่ บอตเน็ตทั่วไปมีโครงสร้างการทำงานที่มีเครื่องที่ทำหน้าที่ควบคุม

9. ดีดอส (DDoS) คือ โปรแกรมที่โจมตีสภาพความพร้อมใช้งานของระบบเพื่อทำให้บริการต่าง ๆ ของระบบไม่สามารถให้บริการได้ตามปกติจนกระทั่งระบบไม่สามารถให้บริการต่อไปได้

แนวคิดเกี่ยวกับอาชญากรรมไซเบอร์

อาชญากรรม : ความหมายแนวคิดของนักวิชาการ

ซีซาร์ เบ็คคาเรีย (Cesare Beccria, 2009) ได้ให้ความหมายของคำว่าอาชญากรรม ซึ่งผู้วิจัยสรุปใจความได้ว่า อาชญากรรม หมายถึง พฤติกรรมหรือการกระทำใด ๆ ที่ก่อให้เกิดอันตรายต่อสังคมจนเป็นผลที่ทำให้สังคมต้องการแก้ไขพฤติกรรมเหล่านั้น ด้วยการออกกฎหมายห้ามมิให้กระทำพร้อมกับกำหนดบทลงโทษผู้ฝ่าฝืนไว้

ซัทเธอร์แลนด์ และเครสซี (Sutherland and Cressey 1992) ได้ให้ความหมายของคำว่าอาชญากรรม ซึ่งผู้วิจัยสรุปใจความได้ว่า อาชญากรรม คือ การกระทำที่ละเมิดกฎหมายอาญา การกระทำใด ๆ ไม่ว่าจะน่าประณาม น่าลงโทษมากสักเพียงใด ไม่ว่าจะผิดศีลธรรมมากน้อยแค่ไหน หรือเลวทรามต่ำช้ามากแค่ไหน ก็ไม่ถือว่าเป็นอาชญากรรมถ้าไม่มีบทบัญญัติของกฎหมายห้ามไว้

พอล แท็ปแพ็น (Paul Tappan 1960) ได้ให้ความหมายของคำว่าอาชญากรรม ซึ่งผู้วิจัยสรุปใจความได้ว่า อาชญากรรม คือ การกระทำโดยมีเจตนาละเมิดกฎหมาย หรือ เจตนาละเว้นไม่กระทำสิ่งที่กฎหมายอาญาบังคับให้กระทำโดยไม่มีข้อแก้ตัวที่สมเหตุสมผล ซึ่งทำให้รัฐต้องดำเนินการลงโทษในฐานะที่เป็นความผิดอุกฉกรรจ์ หรือ ความผิดลหุโทษ

ประเภทของอาชญากรรม การแบ่งประเภทอาชญากรรมตามหลักอาชญาวิทยา

การแบ่งประเภทอาชญากรรมตามหน้าที่การป้องกันและปราบปรามอาชญากรรมตามแนวคิดของมาแชล บี คลิน นาร์ด (Marshll B. Clonard) และริดชาด ควินนี่ (Richard Quinney) ,1973 ได้มีการกำหนดและจำแนกประเภทของอาชญากรรมตามหน้าที่ในการป้องกันและปราบปรามของตำรวจออกเป็น 8 ประเภท เพื่อใช้เป็นกรอบแนวทางในการวิเคราะห์และจัดการกับอาชญากรรมอย่างเป็นระบบ ดังนี้

1. อาชญากรรมประเภทประทุษร้ายต่อชีวิตและร่างกายขั้นรุนแรง
2. อาชญากรรมประเภทประทุษร้ายต่อทรัพย์เป็นครั้งคราว (Occasional Property Crime)
3. อาชญากรรมประเภทใช้หน้าที่การงานเป็นเครื่องมือ (Occupational Crime)
4. อาชญากรรมทางการเมือง (Political Crime)
5. อาชญากรรมประเภทขัดต่อความสงบเรียบร้อยของสังคม (Public Order Crime)
6. อาชญากรรมทั่วไป (Conventional Crime)
7. อาชญากรรมประเภทองค์การหรือองค์การอาชญากรรม (Organized Crime)
8. อาชญากรรมมืออาชีพ (Professional Crime)

แนวคิดทฤษฎีเกี่ยวกับความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์

Wayuparb (2018) ได้กำหนดรายละเอียดความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์ หมายถึงองค์ความรู้ ทักษะ และประสบการณ์ที่มีต่ออาชญากรรมไซเบอร์ โดยประกอบไปด้วยรายละเอียดดังต่อไปนี้

1. ความรู้ความเข้าใจในการโจมตีด้วยมัลแวร์ คือ องค์ความรู้ ทักษะ และประสบการณ์เกี่ยวกับโปรแกรมประสงค์ร้ายต่าง ๆ ที่เรียกว่ามัลแวร์ โดยมัลแวร์ทำงานในลักษณะที่เป็นการโจมตีระบบ การทำให้ระบบเสียหาย รวมไปถึงการโจรกรรมข้อมูล มัลแวร์ แบ่งออกได้หลากหลายประเภท อาทิเช่น ไวรัส (Virus) เวิร์มหรือหนอนอินเทอร์เน็ต (Worm) ม้าโทรจัน (Trojan Horse) การแอบดักจับข้อมูล (Spyware) คีย์ล็อกเกอร์ (Key Logger) ตลอดจนโปรแกรมประเภทขโมยข้อมูล (Cookie) และการฝัง Malicious Mobile Code (MMC) ผ่านทางช่องโหว่ต่าง ๆ

2. ความรู้ความเข้าใจในการโกงและหลอกลวงบนโซเชียลมีเดีย คือ องค์ความรู้ ทักษะ และประสบการณ์เกี่ยวกับภัยจากผู้ไม่หวังดีที่พยายามเข้ามาหลอกล่อ พูดคุย โน้มน้าว ฉ้อโกงหลอกลวงให้ผู้เสียให้กระทำบางอย่างที่เสียผลประโยชน์ เช่น โอนเงิน ส่งรูปภาพ หรือ ส่งข้อมูลส่วนตัวให้กับคนร้าย และคนร้ายนำเอาข้อมูลเหล่านั้นไปใช้ประโยชน์ต่อ

3. ความรู้ความเข้าใจในการเจาะระบบ คือ องค์ความรู้ ทักษะ และประสบการณ์เกี่ยวกับการเจาะเข้าโปรแกรมคอมพิวเตอร์อย่างผิดกฎหมาย ซึ่งเป็นระบบที่มีการป้องกันด้วยรหัสผ่าน แต่มีผู้ไม่หวังดีทำการเจาะเข้าใช้ระบบโดยไม่ได้รับอนุญาต

4. ความรู้ความเข้าใจในการดักจับข้อมูล คือ องค์ความรู้ ทักษะ และประสบการณ์เกี่ยวกับโปรแกรมที่เอาไว้ดักจับข้อมูล บนระบบเครือข่ายคอมพิวเตอร์ เนื่องจากเครือข่ายคอมพิวเตอร์เป็นระบบการสื่อสารที่ใช้ร่วมกัน ทำให้ผู้ไม่หวังดีสามารถรับข้อมูลที่คอมพิวเตอร์เครื่องหนึ่งส่งไปยังเครื่องคอมพิวเตอร์อีกเครื่องหนึ่งได้ โดยการดักจับข้อมูลที่วิ่งไปมาระหว่างเครือข่าย

5. ความรู้ความเข้าใจในการโจมตีเพื่อเรียกค่าไถ่ คือ องค์ความรู้ ทักษะ และประสบการณ์เกี่ยวกับการเรียกค่าไถ่บนอินเทอร์เน็ต โดยผู้ไม่หวังดีทำการเข้าถึงข้อมูลของผู้เสียหาย และทำการเข้ารหัสข้อมูลเหล่านั้นไว้จนไม่สามารถใช้งานได้ และจะทำการเรียกค่าไถ่โดยให้ผู้เสียหายจ่ายเงินเพื่อถอดรหัสข้อมูลที่ถูกเข้ารหัสไว้

6. ความรู้ความเข้าใจในการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต คือ องค์ความรู้ ทักษะ และประสบการณ์เกี่ยวกับการแอบเข้าไปใช้งานข้อมูลส่วนบุคคล หรือแอบเข้าไปใช้งานในระบบที่เจ้าของไม่ได้อนุญาตให้เข้าถึง

แนวคิดการปฏิบัติหน้าที่ พ.ร.ก. อาชญากรรมทางเทคโนโลยี 2566

อาชญากรรมทางเทคโนโลยี" หมายความว่า การกระทำหรือพยายามกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เพื่อฉ้อโกง กรรโชก หรือรีดเอาทรัพย์บุคคลหนึ่งบุคคลใด หรือโดยประการที่น่าจะทำให้บุคคลอื่นเสียหาย หรือกระทำความผิดฐานฉ้อโกงกรรโชก หรือรีดเอาทรัพย์ โดยใช้ระบบคอมพิวเตอร์เป็นเครื่องมือ

"สถาบันการเงิน" หมายความว่า ธนาคารพาณิชย์และสถาบันการเงินของรัฐที่มีกฎหมายเฉพาะจัดตั้งขึ้น ทั้งนี้ ตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน

"ผู้ประกอบธุรกิจ" หมายความว่า ผู้ประกอบธุรกิจตามกฎหมายว่าด้วยระบบการชำระเงิน

พ.ร.ก.อาชญากรรมทางเทคโนโลยี ฯ พ.ศ. 2566 ประกอบด้วย 5 ด้าน ได้แก่

ด้านความพร้อมในการปฏิบัติหน้าที่ตาม พ.ร.ก. อาชญากรรมทางเทคโนโลยี มาตรา 4, 5

มาตรา 4 เพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ในกรณีที่มีเหตุอันควรสงสัยว่ามีหรืออาจมีการกระทำความผิดอาชญากรรมทางเทคโนโลยี ให้สถาบันการเงินและผู้ประกอบธุรกิจมีหน้าที่เปิดเผยหรือแลกเปลี่ยนข้อมูลเกี่ยวกับบัญชีและธุรกรรมของลูกค้าที่เกี่ยวข้องในระหว่างสถาบันการเงินและผู้ประกอบธุรกิจนั้นผ่านระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูลที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษสำนักงานป้องกันและปราบปรามการฟอกเงิน และธนาคารแห่งประเทศไทยเห็นชอบร่วมกัน

เพื่อดำเนินการตามวัตถุประสงค์ตามวรรคหนึ่ง ให้ผู้ให้บริการเครือข่ายโทรศัพท์ ผู้ให้บริการโทรคมนาคมอื่น หรือผู้ให้บริการอื่นที่เกี่ยวข้องมีหน้าที่เปิดเผยหรือแลกเปลี่ยนข้อมูลการให้บริการที่เกี่ยวข้องระหว่างกันผ่านระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูลที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมและสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ เห็นชอบร่วมกัน เมื่อมีการเปิดเผยหรือแลกเปลี่ยนข้อมูลตามวรรคหนึ่งหรือวรรคสองแล้ว ให้ผู้เปิดเผยหรือแลกเปลี่ยนข้อมูลแจ้งให้สำนักงานตำรวจแห่งชาติหรือกรมสอบสวนคดีพิเศษ แล้วแต่กรณีและสำนักงานป้องกันและปราบปรามการฟอกเงิน ทราบโดยทันที และเมื่อได้รับแจ้งแล้วให้สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดี

พิเศษ หรือสำนักงานป้องกันและปราบปรามการฟอกเงินแล้วแต่กรณี มีอำนาจนำข้อมูลดังกล่าวไปใช้ประโยชน์เพื่อป้องกัน ปราบปราม หรือระงับอาชญากรรมทางเทคโนโลยีได้

มาตรา 5 ในกรณีที่มีเหตุอันควรสงสัยว่ามีการกระทำความผิดอาชญากรรมทางเทคโนโลยีและมีความจำเป็นต้องทราบข้อมูลการลงทะเบียนผู้ใช้งานหรือข้อมูลจราจรทางคอมพิวเตอร์ให้สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ หรือสำนักงานป้องกันและปราบปรามการฟอกเงินแล้วแต่กรณี มีอำนาจสั่งให้ผู้ให้บริการเครือข่ายโทรศัพท์ ผู้ให้บริการโทรคมนาคมอื่น หรือผู้ให้บริการอื่นที่เกี่ยวข้องกับการกระทำดังกล่าวเปิดเผยข้อมูลที่เกี่ยวข้องเท่าที่จำเป็น และเมื่อได้รับคำสั่งแล้วให้ผู้ให้บริการเครือข่ายโทรศัพท์ ผู้ให้บริการโทรคมนาคมอื่น หรือผู้ให้บริการอื่นที่เกี่ยวข้องกับการกระทำนั้น มีหน้าที่ส่งข้อมูลดังกล่าวให้แก่ผู้สั่งภายในระยะเวลาที่ผู้สั่งกำหนด

ด้านความพร้อมในการปฏิบัติหน้าที่ตาม พ.ร.ก. อาชญากรรมทางเทคโนโลยี มาตรา 7, 8

มาตรา 7 ในกรณีที่สถาบันการเงินหรือผู้ประกอบธุรกิจได้รับแจ้งจากผู้เสียหาย ซึ่งเป็นผู้ถือบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ว่า ได้มีการทำธุรกรรมโดยบัญชีเงินฝากหรือ บัญชีเงินอิเล็กทรอนิกส์ดังกล่าวและเข้าข่ายเกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี ให้สถาบันการเงิน หรือผู้ประกอบธุรกิจดังกล่าวมีหน้าที่ระงับการทำธุรกรรมนั้นไว้ชั่วคราว พร้อมทั้งนำข้อมูลเข้าสู่ระบบ หรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูลตามมาตรา 4 เพื่อให้สถาบันการเงินและผู้ประกอบธุรกิจ ผู้รับโอนทุกทอดทราบและระงับการทำธุรกรรมดังกล่าวไว้ทันที และแจ้งให้ผู้เสียหายไปร้องทุกข์ ต่อพนักงานสอบสวนภายในเจ็ดสิบสองชั่วโมงเมื่อมีการร้องทุกข์แล้ว ให้พนักงานสอบสวนแจ้งให้ สถาบันการเงินหรือผู้ประกอบธุรกิจที่ได้รับการทำธุรกรรมไว้ทราบ และให้พนักงานสอบสวนพิจารณา ดำเนินการเกี่ยวกับบัญชีเงินฝากและบัญชีเงินอิเล็กทรอนิกส์ดังกล่าวภายในเจ็ดวันนับแต่วันที่ได้รับ แจ้งความร้องทุกข์ หากไม่มีคำสั่งให้ระงับการทำธุรกรรมไว้ต่อไปภายในเวลาดังกล่าว ให้สถาบันการเงิน หรือผู้ประกอบธุรกิจยกเลิกการระงับการทำธุรกรรมนั้น

มาตรา 8 การแจ้งข้อมูลหรือหลักฐานตามมาตรา 6 และมาตรา 7 จะกระทำทางโทรศัพท์ หรือวิธีการทางอิเล็กทรอนิกส์ก็ได้ ในกรณีที่กระทำทางโทรศัพท์ ให้ผู้ได้รับแจ้งบันทึกไว้เป็นลายลักษณ์อักษร ลงลายมือชื่อผู้รับแจ้ง และวันเวลาที่ได้รับไว้เป็นหลักฐาน พร้อมทั้งส่งสำเนาให้ผู้แจ้งเก็บไว้เป็นหลักฐานด้วย

การร้องทุกข์ในความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีจะกระทำต่อพนักงานสอบสวน ณ สถานีตำรวจแห่งใดในราชอาณาจักรหรือต่อกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยีก็ได้ และจะร้องทุกข์โดยวิธีการทางอิเล็กทรอนิกส์ก็ได้ โดยให้ถือว่าเป็นการร้องทุกข์โดยชอบด้วยประมวลกฎหมายวิธีพิจารณาความอาญา และในการสอบสวนหรือดำเนินการเกี่ยวกับการกระทำความผิดดังกล่าว ให้พนักงานสอบสวนที่รับคำร้องทุกข์ไม่ว่าประจำอยู่ที่ใดหรือพนักงานสอบสวนที่ผู้บัญชาการตำรวจแห่งชาติกำหนด เป็นพนักงานสอบสวนผู้รับผิดชอบมีอำนาจสอบสวนและดำเนินการเกี่ยวกับการกระทำความผิดดังกล่าวได้ไม่ว่าความผิดนั้นจะเกิดขึ้น ณ ที่ใดในราชอาณาจักร

ด้านความพร้อมในการปฏิบัติหน้าที่ตาม พ.ร.ก. อาชญากรรมทางเทคโนโลยี มาตรา 9, 10, 11

มาตรา 9 ผู้ใดเปิดหรือยินยอมให้บุคคลอื่นใช้บัญชีเงินฝาก บัตรอิเล็กทรอนิกส์หรือบัญชีเงินอิเล็กทรอนิกส์ของตน โดยมิได้มีเจตนาใช้เพื่อตนหรือเพื่อกิจการที่ตนเกี่ยวข้องหรือยินยอมให้บุคคลอื่นใช้หรือยืมใช้เลขหมายโทรศัพท์สำหรับบริการโทรศัพท์เคลื่อนที่ของตน ทั้งนี้โดยประการที่รู้หรือควรรู้ว่าจะนำไปใช้ใน

การกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีหรือความผิดทางอาญาอื่นใด ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินสามแสนบาทหรือทั้งจำทั้งปรับ

มาตรา 10 ผู้ใดเป็นธุระจัดหา โฆษณา หรือไขข่าวโดยประการใด ๆ เพื่อให้มีการซื้อขาย ให้เช่า หรือให้ยืม บัญชีเงินฝาก บัตรอิเล็กทรอนิกส์ หรือบัญชีเงินอิเล็กทรอนิกส์ เพื่อใช้ในการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีหรือความผิดทางอาญาอื่นใด ต้องระวางโทษจำคุกตั้งแต่สองปีถึงห้าปี หรือปรับตั้งแต่สองแสนบาทถึงห้าแสนบาท หรือทั้งจำทั้งปรับ

มาตรา 11 ผู้ใดเป็นธุระจัดหา โฆษณา หรือไขข่าวโดยประการใด ๆ เพื่อให้มีการซื้อหรือขายเลขหมายโทรศัพท์สำหรับบริการโทรศัพท์เคลื่อนที่ ซึ่งลงทะเบียนผู้ใช้บริการในนามของบุคคลหนึ่งบุคคลใดแล้ว แต่ไม่สามารถระบุตัวผู้ใช้บริการได้ ต้องระวางโทษจำคุกตั้งแต่สองปีถึงห้าปีหรือปรับตั้งแต่สองแสนบาทถึงห้าแสนบาท หรือทั้งจำทั้งปรับ

ด้านความพร้อมในการปฏิบัติหน้าที่ตาม พ.ร.ก. อาชญากรรมทางเทคโนโลยี มาตรา 12

มาตรา 12 การเปิดเผยการแลกเปลี่ยน การเข้าถึง ตลอดจนการเก็บ การรวบรวมหรือการใช้ข้อมูลส่วนบุคคลตามพระราชกำหนดนี้ ไม่อยู่ภายใต้บังคับของกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล แต่ผู้ได้รับหรือครอบครองข้อมูลจะเปิดเผยให้บุคคลอื่นซึ่งไม่มีหน้าที่เกี่ยวข้องทราบมิได้

ด้านความพร้อมในการปฏิบัติหน้าที่ตาม พ.ร.ก. อาชญากรรมทางเทคโนโลยี มาตรา 13

มาตรา 13 ในวาระเริ่มแรกให้นายกรัฐมนตรีแต่งตั้งคณะกรรมการขึ้นคณะหนึ่ง มีจำนวนตามที่เห็นสมควร เพื่อกำหนดแนวทางในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีและให้ข้อเสนอแนะเกี่ยวกับเหตุอันควรสงสัยตามพระราชกำหนดนี้ รวมทั้งให้คำแนะนำและคำปรึกษาเกี่ยวกับการปฏิบัติงานของเจ้าหน้าที่ของรัฐและหน่วยงานที่เกี่ยวข้องในการปฏิบัติการตามพระราชกำหนดนี้โดยให้สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมทำหน้าที่หน่วยธุรการของคณะกรรมการดังกล่าวและให้ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมแต่งตั้งข้าราชการของสำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นเลขานุการและผู้ช่วยเลขานุการ โดยผู้บัญชาการตำรวจแห่งชาติจะต่างตั้งข้าราชการจากสำนักงานตำรวจแห่งชาติเป็นผู้ช่วยเลขานุการด้วยก็ได้

เมื่อครบห้าปีหลังจากที่พระราชกำหนดนี้ใช้บังคับ ให้สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมประเมินความจำเป็นในการให้มีคณะกรรมการตามวรรคหนึ่งปฏิบัติหน้าที่ต่อไปเสนอคณะรัฐมนตรีเพื่อพิจารณาอนุมัติ โดยในกรณีมีความจำเป็นต้องมีคณะกรรมการต่อไปให้เสนอแนะหน่วยงานที่จะทำหน้าที่หน่วยธุรการของคณะกรรมการต่อไปด้วย ในกรณีที่เห็นว่าไม่มีความจำเป็นที่จะต้องมีคณะกรรมการดังกล่าวต่อไป และคณะรัฐมนตรีมีมติเห็นชอบด้วยให้คณะกรรมการดังกล่าวสิ้นสุดลงนับแต่วันที่คณะรัฐมนตรีมีมติหรือวันที่คณะรัฐมนตรีกำหนด แล้วแต่กรณี

ในกรณีที่เห็นควรมีคณะกรรมการตามวรรคหนึ่งต่อไป คณะรัฐมนตรีจะกำหนดให้มีคณะกรรมการเพื่อปฏิบัติหน้าที่ต่อไปเป็นคราว ๆ หรือตลอดไปก็ได้ ในกรณีเช่นนั้นการแต่งตั้งและวาระการดำรงตำแหน่งให้เป็นไปตามระเบียบที่คณะรัฐมนตรีกำหนดการประกาศใช้พระราชกำหนดฉบับนี้ คือ โดยที่ปัจจุบันมีการใช้วิธีการทางเทคโนโลยีหลอกลวงประชาชนทั่วไปผ่านอุปกรณ์เทคโนโลยีต่าง ๆ จนทำให้ประชาชนสูญเสียทรัพย์สินเป็นจำนวนมากและผู้หลอกลวงได้โอนทรัพย์สินที่ได้จากการกระทำความผิดดังกล่าวนั้นผ่านบัญชีเงินฝาก บัตรอิเล็กทรอนิกส์หรือบัญชีเงินอิเล็กทรอนิกส์ของบุคคลอื่นต่อไปเป็นทอด ๆ อย่างรวดเร็ว เพื่อปกปิด

หรืออำพรางการกระทำความผิดซึ่งแต่ละวันประชาชนผู้สุจริตถูกหลอกลวงจำนวนมากและมีมูลค่าความเสียหายสูงมาก และการหลอกลวงดังกล่าวซึ่งเป็นการกระทำความผิดได้เพิ่มมากขึ้น ส่งผลกระทบต่อประชาชนในวงกว้างและเป็นอันตรายร้ายแรงต่อระบบเศรษฐกิจของประเทศ เป็นกรณีฉุกเฉินที่มีความจำเป็นรีบด่วนอันมิอาจจะหลีกเลี่ยงได้ เพื่อประโยชน์ในอันที่จะต้องมีมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีดังกล่าว เพื่อรักษาความปลอดภัยของประเทศ ความปลอดภัยสาธารณะ และความมั่นคงในทางเศรษฐกิจของประเทศ จึงจำเป็นต้องตราพระราชกำหนดนี้

จากการวิเคราะห์ผลกระทบของกฎหมายต่อความตระหนักของผู้ใช้อินเทอร์เน็ต การประกาศใช้ พ.ร.ก. อาชญากรรมทางเทคโนโลยี 2566 มีผลกระทบต่อความตระหนักของผู้ใช้อินเทอร์เน็ตในหลายมิติ :

1. มิติการป้องกัน : มาตรา 7 ที่กำหนดให้สถาบันการเงินระงับการทำธุรกรรมเมื่อได้รับแจ้งจากผู้เสียหาย ทำให้ผู้ใช้มีความมั่นใจมากขึ้นในการทำธุรกรรมออนไลน์ อย่างไรก็ตาม ความมั่นใจนี้อาจทำให้บางคนลดการระมัดระวัง (moral hazard) เพราะรู้ว่ามีระบบป้องกัน

2. มิติการลงโทษ : มาตรา 9-11 ที่กำหนดโทษผู้ที่ให้ยืมบัญชีหรือเบอร์โทรศัพท์ ทำให้ผู้ใช้ตระหนักถึงความรับผิดชอบมากขึ้น การรู้ว่าอาจต้องรับผิดทางกฎหมายทำให้ผู้ใช้ระมัดระวังในการแชร์ข้อมูลส่วนตัวมากขึ้น

3. มิติการรายงาน : การที่กฎหมายกำหนดให้สามารถแจ้งความผ่านระบบอิเล็กทรอนิกส์ได้ (มาตรา 8) ทำให้ผู้เสียหายแจ้งเหตุได้ง่ายขึ้น ความสะดวกในการแจ้งเหตุนี้อาจเพิ่มสถิติการรายงาน ซึ่งส่งผลให้สังคมมีความตระหนักต่อปัญหามากขึ้น

แนวทางการสร้างความตระหนักรู้และรับมือกับภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ

จากการศึกษาในหลักแนวคิดและทฤษฎีที่ผ่านมา ทำให้เกิดความตระหนักรู้ถึงความสำคัญของการเสริมสร้างความตระหนักรู้และแนวทางรับมือภัยคุกคามทางไซเบอร์ในสังคมดิจิทัล ซึ่งในยุคที่เทคโนโลยีดิจิทัลเข้ามามีบทบาทในทุกมิติของชีวิต ภัยคุกคามทางไซเบอร์ได้กลายเป็นหนึ่งในปัญหาสำคัญที่ต้องให้ความสนใจอย่างจริงจัง ผู้ใช้อินเทอร์เน็ตจำนวนมากยังขาดความตระหนักรู้เกี่ยวกับรูปแบบและผลกระทบของภัยเหล่านี้ ซึ่งไม่เพียงส่งผลต่อบุคคล แต่ยังอาจลุกลามสู่ระดับองค์กรหรือประเทศได้ การสร้างระบบความปลอดภัยทางไซเบอร์ที่เข้มแข็งจึงต้องอาศัยการมีส่วนร่วมจากทุกภาคส่วน โดยเฉพาะประชาชนในฐานะ "ผู้ใช้อินเทอร์เน็ต" ที่ต้องได้รับการเสริมสร้างความรู้ ความเข้าใจ และแนวทางปฏิบัติที่ชัดเจน เพื่อให้สามารถป้องกันและรับมือกับความเสี่ยงทางไซเบอร์ได้อย่างมีประสิทธิภาพ

ประการแรกคือ แนวทางการสร้างความตระหนักรู้ของผู้ใช้อินเทอร์เน็ต ซึ่งเริ่มจากการเสริมความรู้พื้นฐานเกี่ยวกับภัยคุกคามทางไซเบอร์ ไม่ว่าจะเป็นมัลแวร์ ฟิชชิ่ง การดักจับข้อมูล หรือการเจาะระบบ เพื่อให้ผู้ใช้สามารถรู้เท่าทันกลลวงและหลีกเลี่ยงพฤติกรรมที่เสี่ยงต่อการถูกโจมตี ทั้งนี้ การพัฒนาทักษะการรับรู้และจดจำสิ่งเร้าก็มีความสำคัญ โดยอิงตามแนวคิดของ Good และ Bloom ที่ชี้ว่าความตระหนักรู้จะเกิดขึ้นเมื่อมีการรับรู้ซ้ำ การมีประสบการณ์ตรง และการเรียนรู้จากสถานการณ์จริง เช่น การจำลองเหตุการณ์ฟิชชิ่งหรือการโจมตีไซเบอร์จะช่วยเสริมการเรียนรู้เชิงลึกได้เป็นอย่างดี นอกจากนี้ การคำนึงถึงปัจจัยทางพฤติกรรมศาสตร์ยังช่วยให้การส่งเสริมความตระหนักรู้มีประสิทธิภาพยิ่งขึ้น กล่าวคือ ผู้ใช้จะมีพฤติกรรมที่ปลอดภัยมากขึ้นหากมีความคุ้นเคยกับโลกดิจิทัล เข้าใจคุณค่าของข้อมูลส่วนตัว และตระหนักถึงผลกระทบของการละเลย

ความปลอดภัย เช่น การตั้งค่าความเป็นส่วนตัวบนโซเชียลมีเดียหรือการไม่แชร์ข้อมูลส่วนบุคคลในพื้นที่สาธารณะ

ต่อมา คือ แนวทางการรับมือกับภัยคุกคามทางไซเบอร์ ที่ต้องเริ่มจากการจำแนกประเภทภัยอย่างชัดเจน ไม่ว่าจะเป็นมัลแวร์ ฟิชชิ่ง การดักจับข้อมูล หรือการโจมตีแบบเฉพาะเจาะจง (targeted attack) ซึ่งแต่ละประเภทต้องการมาตรการป้องกันที่แตกต่างกัน เช่น การติดตั้งโปรแกรมป้องกันมัลแวร์ หลีกเลี่ยงการใช้ Wi-Fi สาธารณะโดยไม่มี VPN หรือการอัปเดตระบบซอฟต์แวร์อย่างสม่ำเสมอ ล้วนเป็นแนวทางพื้นฐานที่ช่วยลดความเสี่ยงได้อย่างมีประสิทธิภาพ นอกจากนี้ ควรส่งเสริมให้ประชาชนสามารถแจ้งเหตุภัยไซเบอร์ได้สะดวก เช่น ผ่านระบบอิเล็กทรอนิกส์หรือแพลตฟอร์มออนไลน์ที่เข้าถึงง่าย เพราะเมื่อประชาชนสามารถรายงานเหตุการณ์ได้ทันที จะช่วยให้ระบบสามารถเฝ้าระวังและตอบสนองต่อภัยคุกคามได้รวดเร็วและทั่วถึงมากยิ่งขึ้น

สุดท้าย คือ แนวทางการใช้กฎหมายเพื่อส่งเสริมความปลอดภัยและความตระหนักรู้ทางไซ**เบอร์** ซึ่งถือเป็นกลไกสำคัญในการกำกับพฤติกรรมและสร้างความรับผิดชอบในโลกดิจิทัล ตัวอย่างเช่น พระราชกำหนดว่าด้วยการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 ที่กำหนดบทลงโทษชัดเจนในมาตรา 9–11 สำหรับผู้ที่ให้ยืมบัญชีหรือเบอร์โทรศัพท์ไปใช้ในทางที่ผิด ถือเป็นมาตรการที่กระตุ้นให้ประชาชนตระหนักถึงการรักษาข้อมูลส่วนตัวอย่างเคร่งครัด นอกจากนี้ การสนับสนุนให้เจ้าหน้าที่บังคับใช้กฎหมายสามารถเข้าถึงข้อมูลจากผู้ให้บริการโทรคมนาคมตามมาตรา 5 ยังช่วยให้การสอบสวนและดำเนินคดีมีประสิทธิภาพมากขึ้น อีกทั้ง การเปิดโอกาสให้ประชาชนแจ้งความผ่านระบบออนไลน์ตามมาตรา 8 ยังช่วยให้ประชาชนเข้าถึงกระบวนการยุติธรรมได้ง่ายขึ้น สร้างแรงจูงใจให้เข้ามามีส่วนร่วมในการสอดส่องภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง

กล่าวโดยสรุป การเสริมสร้างความตระหนักรู้ การกำหนดแนวทางการรับมือ และการใช้กฎหมายเป็นเครื่องมือสนับสนุน ล้วนเป็นองค์ประกอบสำคัญของการจัดการภัยคุกคามทางไซเบอร์ในยุคดิจิทัล หากดำเนินการอย่างเป็นระบบและมีส่วนร่วมจากทุกภาคส่วน ย่อมจะนำไปสู่การสร้างสังคมไซเบอร์ที่ปลอดภัยและยั่งยืนในระยะยาว

บทสรุป

ภัยคุกคามทางไซเบอร์ที่มีผลต่อการตระหนักรู้ของผู้ใช้อินเทอร์เน็ต เมื่อกล่าวถึงประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต กล่าวคือการโจมตีทางไซเบอร์ที่มีรูปแบบการพัฒนาการโจมตีเพื่อหาช่องโหว่ทางอินเทอร์เน็ตหลากหลายรูปแบบ เพื่อทำให้ผู้งานอินเทอร์เน็ตไม่สามารถระวังได้ถึงภัยคุกคามทางไซเบอร์และไม่สามารถป้องกันการโจมตีที่ไม่เหมือนเดิมและได้รับความเสียหายไม่คาดคิดแตกต่างจากครั้งก่อนทำให้ไม่สามารถประเมินสถานการณ์ที่จะเกิดความเสียหายขึ้นได้หรือในทางด้านความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต กล่าวคือ ทำให้ทราบถึงผู้ที่มีความรู้ และทราบถึงภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อตนเอง สามารถเข้าใจถึงปัญหาที่จะเกิดความเสียหาย จากภัยคุกคามทางไซเบอร์ขึ้นล่วงหน้า ไม่ว่าจะเป็นการเปิดเผยข้อมูลบนสาธารณะ การทำธุรกรรมออนไลน์ การป้องกันให้ไม่ผู้อื่นทราบข้อมูลส่วนตัว และการติดตามข้อมูลข่าวสารการโจมตีรูปแบบใหม่ๆ การดาวโหลดโปรแกรมที่ถูกต้องมาจากผู้ผลิตโดยตรงป้องกันความเสี่ยงการฝังไวรัสที่ไม่คาดคิดติดมากับโปรแกรมและสามารถป้องกันภัยคุกคามจากผู้ที่ไม่หวังดีที่จะเกิดผลกระทบความเสียหายโดยไม่คาดคิดได้ และความตระหนักถึงภัยคุกคามและอาชญากรรมไซเบอร์สามารถนำไปใช้ในออกแบบการเรียนรู้ที่เหมาะสมเพื่อ

ป้องกันภัยคุกคามและอาชญากรรมไซเบอร์ที่สอดคล้องเหมาะสมกับปัจจุบัน ตามรูปแบบการใช้อินเทอร์เน็ตที่เปลี่ยนแปลงไปอย่างรวดเร็วเพื่อให้ผู้ใช้งานอินเทอร์เน็ตในสถานศึกษารู้เท่าทันและป้องกันตนเองได้ก่อนที่จะเกิดความไม่ปลอดภัยกับชีวิตและทรัพย์สินจากภัยและอาชญากรรมไซเบอร์ต่อไป

บรรณานุกรม

กองสถิติเศรษฐกิจ สำนักงานสถิติแห่งชาติ. (2567). *สำรวจการมีการใช้เทคโนโลยีสารสนเทศและการสื่อสารในครัวเรือน พ.ศ. 2567 (ไตรมาส 4).* กรุงเทพมหานคร: กองสถิติพยากรณ์ สำนักงานสถิติแห่งชาติ.

ประชาไท. (2567). *สถิติ 3 ปี มูลค่าความเสียหายภัยออนไลน์จากมิจฉาชีพสูงกว่า 7 หมื่นล้านบาท.* สืบค้น 25 มีนาคม 2568, จาก https://prachatai.com/journal/2024/12/111710?utm_source=chatgpt.com

พัฒนศักดิ์ บุบผาสุวรรณ. (2546). *ความตระหนักของนิสิตมหาวิทยาลัยเกษตรศาสตร์ ต่ออาชญากรรมบนอินเทอร์เน็ต*. (วิทยานิพนธ์ปริญญามหาบัณฑิต). มหาวิทยาลัยเกษตรศาสตร์.

กฎกระทรวง แบ่งส่วนราชการเป็นกองบังคับการหรือส่วนราชการอย่างอื่น ในสำนักงานตำรวจแห่งชาติ (ฉบับที่ 17. (2563, 9 กันยายน). *ราชกิจจานุเบกษา*. เล่ม 137 ตอนที่ 72 ก หน้า 1–6.

ราชบัณฑิตยสถาน. (2554). *พจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ. 2554.* (พิมพ์ครั้งที่ 2). กรุงเทพมหานคร: ราชบัณฑิตยสถาน.

สุธาสินี อินทร์ผูก. (2548). *ความตระหนักในปัญหาการจัดการมูลฝอยกับพฤติกรรมการนำมูลฝอยแห้งกลับมาใช้ซ้ำของประชาชนเขตเทศบาลนครลำปาง*. (การค้นคว้าแบบอิสระ ศิลปะศาสตร์มหาบัณฑิต สาขาวิชาการจัดการมนุษย์กับสิ่งแวดล้อม). มหาวิทยาลัยเชียงใหม่.

สุพัตรา ถนอมวงค์. (2551). *ความตระหนักต่อการจัดการขยะของผู้อยู่อาศัยบริเวณริมคลองรังสิต ประยูรศักดิ์ : ศึกษากรณี ตำบลบึงยี่โถ อำเภอธัญบุรี จังหวัดปทุมธานี*. (ภาคนิพนธ์ ปริญญามหาบัณฑิต). สถาบันบัณฑิตพัฒนบริหารศาสตร์.

สุภาพิชญ์ ถิระวัฒน์. (2564). *รายการร้อยเรื่อง...เมืองไทย เรื่อง “กองบัญชาการตำรวจไซเบอร์”*. กรุงเทพมหานคร: สำนักงานเลขาธิการสภาผู้แทนราษฎร

Beccaria, C. (2009). *On Crimes and Punishments* (5th ed.). London: Routledge.

Bloom, B.S. (Ed.). Engelhart, M.D., Furst, E.J., Hill, W.H., Krathwohl, D.R. (1971). *Taxonomy Of Educational Objectives, Handbook I: The Cognitive Domain*. New York: David McKay Co Inc.

Clonard, M. B., & Quinney, R. (1973). *Criminal Behavior Systems: A Typology.* (2nd ed.). New York: Holt, Rinehart and Winston.

Good, C.V. (1973). *Dictionary of education*. New York: McGraw-Hill.

Sutherland, E. H., & Cressey, D. R. (1992). *Principles of criminology* (11th ed.). New York: Bloomsbury Publishing.

Tappan, Paul J. (1960). *Psychology of Crime Problem*. New York: The Macmilan Company.

Wayuparb, S. (2018). *Thailand Internet User Profile 2018*. (รายงานภาษาไทย). Electronic Transactions Development Agency Publication.