เอกสารวิชาการ

เรื่อง

มาตรการทางกฎหมายและนโยบายในการแก้ไขปัญหา

อาชญากรรมทางเทคโนโลยีของประเทศไทย

จัดทำโดย
นางสาวบูชิตา ไวทยานนท์
วิทยากรชำนาญการพิเศษ กลุ่มงานวิจัยและพัฒนา
สำนักวิชาการ สำนักงานเลขาธิการสภาผู้แทนราษฎร

คำนำ

เอกสารวิชาการ เรื่อง มาตรการทางกฎหมายและนโยบายในการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีของประเทศไทย จัดทำขึ้นเพื่อ (๑) ศึกษารูปแบบของกลยุทธ์และประเภทของอาชญากรรมทางเทคโนโลยี ตลอดจนวิเคราะห์สภาพปัญหาและรูปแบบการกระทำผิดอาชญากรรมทางเทคโนโลยีในประเทศไทย (๒) ศึกษากรอบและการบังคับใช้กฎหมายหลัก กฎหมายรอง และนโยบายในการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีของหน่วยงานที่เกี่ยวข้องทั้งในระดับประเทศและสากล และ (๓) ศึกษาบทเรียนความสำเร็จการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีของประเทศสิงคโปร์ เพื่อเป็นแนวทางการพัฒนาและปรับปรุงการบังคับใช้กฎหมายเพื่อแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีของประเทศไทย ด้วยวิธีการศึกษาเชิงคุณภาพโดยการทบทวนเอกสารวิชาการ กฎหมายหลัก กฎหมายรอง และนโยบายที่เกี่ยวข้องกับปัญหาอาชญากรรมทางเทคโนโลยีทั้งในประเทศไทยและต่างประเทศ

ผลจากการศึกษา พบว่าประเทศไทยและสิงคโปร์ต่างมีมาตรการทางกฎหมายเพื่อป้องกันและปราบปรามทางเทคโนโลยี ประเทศไทยได้ตราพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ ๒) พ.ศ. ๒๕๖๘ เพื่อคุ้มครองประชาชนจากภัยทางการเงิน ขณะที่สิงคโปร์มีแนวทางที่เข้มงวดโดยกำหนดให้สถาบันการเงินและผู้ให้บริการด้านการสื่อสารมีบทบาทในการร่วมรับผิดชอบแก่ผู้เสียหาย โดยผู้จัดทำมีข้อเสนอแนะจากการศึกษาในส่วนของแนวทางการพัฒนาและปรับปรุงการบังคับใช้กฎหมายเพื่อแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีของประเทศไทย คือ ๑) รัฐควรเร่งดำเนินการออกกฎหมายที่เกี่ยวข้องเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีให้มีความทันสมัยสอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป ๒) รัฐควรมีมาตรการหน่วงเงินมาใช้เพื่อเพิ่มความปลอดภัยให้กับประชาชน และ ๓) รัฐควรส่งเสริมวัฒนธรรมแห่งการป้องกันโดยการใช้เทคโนโลยีเป็นสื่อรณรงค์เพื่อสร้างความตระหนักรู้ให้แก่ประชาชน

ผู้จัดทำขอขอบคุณผู้บังคับบัญชาที่สนับสนุนให้คำแนะนำองค์ความรู้อันเป็นประโยชน์ต่อเอกสารวิชาการนี้จนครบถ้วนสมบูรณ์ รวมทั้งผู้มีส่วนเกี่ยวข้องทุกท่าน และหวังว่าเอกสารวิชาการฉบับนี้จะเป็นประโยชน์แก่สมาชิกรัฐสภา คณะกรรมาธิการและผู้ที่สนใจศึกษาต่อไป

บูชิตา ไวทยานนท์
เมษายน ๒๕๖๘

สารบัญ

สารบัญภาพ

ภาพที่ **หน้า**

สารบัญตาราง

บทที่ ๑
บทนำ

๑.๑ ความเป็นมาและความสำคัญของปัญหา

โลกไร้พรมแดนในยุคโลกาภิวัตน์ส่งผลให้มนุษย์ ทุน ความรู้ เทคโนโลยี สินค้า และบริการ สามารถเชื่อมโยงกันทั่วโลก ทำให้เกิดการเปลี่ยนแปลงทางด้านเศรษฐกิจ สังคม การเมือง ประชากร การรักษาสิ่งแวดล้อม ตลอดจนเทคโนโลยีการเชื่อมโยงข้อมูลข่าวสาร ซึ่งการเปลี่ยนแปลงดังกล่าว ก่อให้เกิดทั้งโอกาสและอุปสรรคอันส่งผลต่อการพัฒนาประเทศ ทั้งในด้านที่เกิดประโยชน์และไม่เกิดประโยชน์ นอกจากนี้ ยังนำมาซึ่งปัญหาอาชญากรรมในรูปแบบใหม่ ๆ ที่มีความสลับซับซ้อนรุนแรง และมีแนวโน้มของปัญหาเพิ่มมากยิ่งขึ้น ส่งผลต่อแนวโน้มอัตราการเกิดอาชญากรรมเพิ่มสูงขึ้นตามลำดับ เช่น การก่อการร้ายสากล อาชญากรรมข้ามชาติ การลักลอบค้ายาเสพติด การค้ามนุษย์ อาชญากรรมทางเศรษฐกิจ อาชญากรรมคอมพิวเตอร์ และการละเมิดทรัพย์สินทางปัญญา เป็นต้น สถานการณ์ดังกล่าวย่อมส่งผลกระทบโดยตรงอันนำไปสู่ปัญหาความปลอดภัยในชีวิตและทรัพย์สินของประชาชนที่มีความซับซ้อนและเพิ่มความรุนแรงมากขึ้น ผลลัพธ์ของความทันสมัยจึงไม่ได้มีเพียงด้านบวกเท่านั้น แต่ยังมีประชาชนจำนวนมากที่อาจใช้เทคโนโลยีในทางที่ผิด สร้างอันตรายและก่อให้เกิดความเสียหายต่อทรัพย์สินและสภาพจิตใจในระดับบุคคล หรือทำลายโครงสร้างพื้นฐานที่สำคัญของรัฐเพื่อผลประโยชน์ของตนเอง อาทิ การหลอกลวงให้โอนเงินบนแพลตฟอร์มออนไลน์ การหลอกลงทุนผ่านระบบออนไลน์ หรือการหลอกซื้อขายสินค้าและบริการผ่านสื่อออนไลน์ ซึ่งปัญหาดังกล่าวกลายเป็นภัยคุกคามรายวันของผู้คนในประเทศไทย โดยมีมูลค่าความเสียหายเพิ่มสูงขึ้นในทุก ๆ ปี สะท้อนให้เห็นว่าเทคโนโลยีหรือวิธีการหลอกลวงที่ล้ำสมัยเป็นเรื่องยากในการแก้ปัญหา เนื่องจากปัญหาเหล่านี้มีความซับซ้อนเมื่อเกิดขึ้นบนพื้นที่ไซเบอร์ซึ่งยังไม่มีกฎหมายบังคับใช้เป็นการเฉพาะประกอบกับความไร้พรมแดนของเทคโนโลยี จึงเป็นภัยร้ายแรงที่สร้างผลกระทบต่อเศรษฐกิจและความมั่นคงในระดับชาติและระดับโลก

ในปี ๒๕๖๗ ประเทศไทยเผชิญกับอาชญากรรมทางเทคโนโลยีและภัยคุกคามทางไซเบอร์ที่เพิ่มขึ้นอย่างต่อเนื่อง ข้อมูลจากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ระบุว่า มีการโจมตีทางไซเบอร์ที่สำคัญหลายประเภท โดยเฉพาะการโจมตีด้วยแรนซัมแวร์ (Ransomware) ที่มุ่งเป้าไปยังองค์กรทั้งภาครัฐและภาคเอกชน ส่งผลให้ข้อมูลที่มีการเข้ารหัสไฟล์และเรียกค่าไถ่เพื่อแลกกับการกู้คืนการเข้าถึงไฟล์ที่เข้ารหัส สร้างความเสียหายทางเศรษฐกิจอย่างมาก นอกจากนี้ การหลอกลวงทางออนไลน์ เช่น การหลอกลวงลงทุนและการซื้อขายสินค้าผิดกฎหมาย ยังคงเป็นปัญหาที่พบอย่างแพร่หลายและมีผู้เสียหายจำนวนมาก ส่งผลกระทบต่อความเชื่อมั่นของประชาชนในการใช้บริการออนไลน์ ซึ่งสอดคล้องกับข้อมูลจากสำนักงานตำรวจแห่งชาติที่ระบุว่าในปี ๒๕๖๗ อาชญากรรมทางเทคโนโลยีในประเทศไทยมีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง โดยระหว่างวันที่ ๑ มีนาคม ๒๕๖๕ ถึง ๓๑ ธันวาคม ๒๕๖๗ มีการแจ้งความออนไลน์เกี่ยวกับอาชญากรรมทางเทคโนโลยี จำนวน ๗๗๓,๑๑๘ เรื่อง มูลค่าความเสียหายรวม ๗๙,๕๖๙,๔๑๒,๖๐๘ บาท และที่ผ่านมา พบว่าคดีที่มีจำนวนการแจ้งความมากที่สุดอันดับ ๑ คือ

การหลอกซื้อขายสินค้าหรือบริการทางออนไลน์ มีจำนวน ๓๖๕,๐๗๕ คดี และยังเป็นคดีที่มีความเสียหายรวมสูงที่สุดอันดับ ๑ ด้วย โดยมีความเสียหายรวม ๕,๐๓๕,๗๙๓,๐๐๙ บาท สำหรับคดีในรูปแบบอื่น ๆ อาทิ การหลอกให้โอนเงิน การหลอกให้ลงทุน การหลอกให้กู้เงิน และการข่มขู่ทางโทรศัพท์ ยังคงเป็นรูปแบบคดีที่มีผู้เสียหายและสร้างความเสียหายในอันดับต้น ๆ เช่นเดียวกัน[๑]

ข้อมูลรายงานและสถิติคดีดังกล่าวสะท้อนให้เห็นถึงปัญหาในการบังคับใช้กฎหมาย คือ พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๖[๒] โดยมีผลบังคับใช้แล้วตั้งแต่วันที่ ๑๗ มีนาคม ๒๕๖๖ แต่กลับพบว่ายังไม่สามารถนำมาปฏิบัติและบังคับใช้ให้เกิดประสิทธิผลในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีได้ ซึ่งยังไม่สามารถแก้ปัญหาบรรเทาความเดือดร้อนของประชาชนและแก้ไขข้อขัดข้องในการปฏิบัติของสถาบันการเงิน รวมทั้งผู้ประกอบธุรกิจที่เกี่ยวข้องได้อย่างครบถ้วน อาทิ ปัญหานิยามศัพท์ไม่ครอบคลุมครบถ้วนในการกระทำที่ใช้เทคโนโลยีเป็นเครื่องมือในการกระทำความผิด และการกระทำความผิดที่เกิดขึ้นนอกราชอาณาจักร และยังไม่ครอบคลุมสถาบันการเงิน ผู้ประกอบธุรกิจ และผู้ให้บริการที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี ข้อจำกัดเกี่ยวกับการดำเนินคดีอาญา ข้อจำกัดเกี่ยวกับกระบวนการคุ้มครองผู้เสียหายจากการกระทำความผิด ตลอดจนเจ้าหน้าที่ของรัฐที่มีอำนาจหน้าที่ที่เกี่ยวข้องยังมีข้อจำกัดในการบังคับใช้กฎหมายอยู่หลายประการ และยังไม่มีบทบัญญัติให้นำกฎหมายอื่น ๆ ที่เกี่ยวข้องมาปฏิบัติเพื่อสนับสนุนการบังคับใช้กฎหมายตามพระราชกำหนดฉบับดังกล่าวได้ สาเหตุของปัญหาเนื่องมาจากพระราชกำหนดฉบับดังกล่าวมีความจำเป็นเร่งด่วนอันมิอาจหลีกเลี่ยงได้ จึงจำเป็นต้องตราเป็นพระราชกำหนด ทำให้มีข้อขัดข้องไม่สามารถนำมาปฏิบัติหรือบังคับใช้ให้เกิดประสิทธิผลได้

ประเด็นปัญหาการบังคับใช้พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๖ จากรายงานการพิจารณาศึกษาเรื่อง “การบังคับใช้และแก้ไขกฎหมายว่าด้วยการป้องกันปราบปรามอาชญากรรมทางเทคโนโลยี” ของคณะอนุกรรมาธิการศึกษาการบังคับใช้และแก้ไขกฎหมายว่าด้วยการป้องกันปราบปรามอาชญากรรมทางเทคโนโลยี ในคณะกรรมาธิการการป้องกันปราบปรามการฟอกเงินและยาเสพติด สภาผู้แทนราษฎร (๒๕๖๗)[๓] ระบุว่า การบังคับใช้กฎหมายว่าด้วยการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีเป็นกระบวนการที่สำคัญและซับซ้อน เนื่องจากการกระทำผิดในโลกดิจิทัลมีลักษณะที่เปลี่ยนแปลงรวดเร็วและขยายตัวอย่างต่อเนื่อง กระบวนการสืบสวนอาชญากรรมทางเทคโนโลยีมีความเฉพาะเจาะจงและท้าทาย เนื่องจากต้องอาศัยทักษะและความรู้ในด้านเทคโนโลยีขั้นสูง เจ้าหน้าที่ที่ปฏิบัติงานในด้านนี้จำเป็นต้องมีความเชี่ยวชาญในการใช้เครื่องมือและซอฟต์แวร์ที่เกี่ยวข้องในการ

---

[๑] ไทยพีบีเอส, *พิษอาชญากรรมออนไลน์ปี ๖๘ เกือบ ๒ เดือนสูญ ๓.๔ พันล้าน*, สืบค้นเมื่อวันที่ ๑ มีนาคม ๒๕๖๘. จาก https://www.thaipbs.or.th/news/content/๓๔๙๒๔๘

[๒] พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๖ (๑๗ มีนาคม ๒๕๖๖). *ราชกิจจานุเบกษา*, เล่ม ๑๔๐ ตอนที่ ๑๘ ก, น. ๑-๗.

[๓] สภาผู้แทนราษฎร. (๒๕๖๗). *รายงานผลการพิจารณาศึกษาของคณะอนุกรรมาธิการบังคับใช้และแก้ไขกฎหมายว่าด้วยการป้องกันปราบปรามอาชญากรรมทางเทคโนโลยี*. กรุงเทพฯ : สำนักงานเลขาธิการสภาผู้แทนราษฎร.

เก็บรวบรวมและวิเคราะห์หลักฐานทางดิจิทัล การเก็บหลักฐานในโลกไซเบอร์จะต้องทำอย่างรวดเร็ว เนื่องจากข้อมูลอาจถูกลบหรือเปลี่ยนแปลงได้ง่าย และหน่วยงานที่เกี่ยวข้องในการบังคับใช้กฎหมายในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีโดยเฉพาะ เช่น กองบังคับการปราบปรามอาชญากรรมทางเทคโนโลยี (Cyber Crime Division) ซึ่งมีหน้าที่สืบสวนและดำเนินคดีในกรณีที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ โดยการทำงานของหน่วยงานจำเป็นต้องร่วมมือกับหน่วยงานอื่นทั้งในประเทศและต่างประเทศ เนื่องจากการกระทำความผิดเหล่านี้ส่วนใหญ่เกิดขึ้นในประเทศใกล้เคียงและมีความซับซ้อนในระดับนานาชาติ ซึ่งทำให้การบังคับใช้กฎหมายในระดับประเทศเพียงอย่างเดียวไม่เพียงพอ จำเป็นต้องมีการประสานงานและความร่วมมือกับหน่วยงานบังคับใช้กฎหมายในประเทศอื่น ๆ หรือองค์กรระหว่างประเทศ เช่น อินเตอร์โพล (Interpol) หรือยูโรโปล (Europol) เพื่อการแลกเปลี่ยนข้อมูลและร่วมมือในการสืบสวนและดำเนินคดีเพื่อตอบสนองภัยคุกคามทางเทคโนโลยีบนโลกไซเบอร์

นอกจากการปราบปรามอาชญากรรมทางเทคโนโลยีแล้ว การป้องกันเป็นสิ่งสำคัญ ซึ่งการให้ความรู้และการสร้างความตระหนักในสังคมเกี่ยวกับภัยคุกคามจากการใช้งานเทคโนโลยีอย่างไม่ระมัดระวังเป็นมาตรการหนึ่งที่สามารถลดความเป็นไปได้ในการตกเป็นเหยื่อของอาชญากรรม อีกทั้งการส่งเสริมให้หน่วยงานและองค์กรต่าง ๆ ใช้มาตรการรักษาความปลอดภัยทางไซเบอร์ที่เข้มงวด และการสนับสนุนการวิจัยและพัฒนานวัตกรรมด้านความปลอดภัยทางไซเบอร์เป็นปัจจัยสำคัญในการป้องกัน จะเห็นได้ว่าหน่วยงานบังคับใช้กฎหมายมีความท้าทายในการบังคับใช้กฎหมายว่าด้วยการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีหลายประการ ด้วยเทคโนโลยีมีการพัฒนาอย่างรวดเร็ว รวมทั้งเครือข่ายอาชญากรรมทางเทคโนโลยีมีรูปแบบการหลอกลวงที่เปลี่ยนแปลงอย่างรวดเร็วเช่นกัน ทำให้กฎหมายและกระบวนการบังคับใช้ต้องมีการทบทวนและปรับปรุงอยู่เสมอ นอกจากนี้ การติดตามการกระทำความผิดในโลกดิจิทัลมีความซับซ้อนและมีผู้กระทำผิดอยู่ในประเทศต่าง ๆ ทั่วโลก ทำให้การสืบสวนและดำเนินคดีกับผู้กระทำผิดเป็นไปอย่างยากลำบาก

ด้วยเหตุผลข้างต้น สำนักวิชาการ สำนักงานเลขาธิการสภาผู้แทนราษฎร จึงได้ดำเนินการศึกษาการปฏิบัติและการบังคับใช้กฎหมายการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี โดยการศึกษาและวิเคราะห์สภาพปัญหาการบังคับใช้กฎหมายและข้อจำกัดของกฎหมายทั้งในมิติของตัวบทกฎหมาย หลักและแนวทางปฏิบัติของหน่วยงานที่อยู่ในบังคับใช้ของกฎหมาย รวมทั้งการศึกษาด้านเทคโนโลยีสารสนเทศในการสนับสนุนการป้องกันและปราบปรามทางเทคโนโลยี เพื่อให้เกิดประสิทธิภาพและประสิทธิผลในการปฏิบัติและบังคับใช้กฎหมายต่อไป

๑.๒ วัตถุประสงค์ของการศึกษา

๑.๒.๑ เพื่อศึกษารูปแบบของกลยุทธ์และประเภทของอาชญากรรมทางเทคโนโลยี ตลอดจนวิเคราะห์สภาพปัญหาและรูปแบบการกระทำผิดอาชญากรรมทางเทคโนโลยีในประเทศไทย

๑.๒.๒ เพื่อศึกษากรอบและการบังคับใช้กฎหมายหลัก กฎหมายรอง และนโยบายในการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีของหน่วยงานที่เกี่ยวข้องทั้งในระดับประเทศและสากล

๑.๒.๓ เพื่อศึกษาบทเรียนความสำเร็จการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีของประเทศสิงคโปร์ เพื่อเป็นแนวทางการพัฒนาและปรับปรุงการบังคับใช้กฎหมายเพื่อแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีของประเทศไทย

๑.๓ ขอบเขตการศึกษา

เอกสารวิชาการ เรื่อง **มาตรการทางกฎหมายและนโยบายในการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีของประเทศไทย** เป็นการศึกษาและวิเคราะห์กรอบกฎหมายหลัก กฎหมายรอง ตลอดจนนโยบายที่เกี่ยวข้องกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี โดยจะศึกษากฎหมายทั้งในระดับประเทศและระดับสากล

๑.๓.๑ ขอบเขตด้านเนื้อหา

มาตรการทางกฎหมายและนโยบายในการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีของประเทศไทย มีขอบเขตการศึกษาเพื่อมุ่งศึกษาการปฏิบัติและการบังคับใช้กฎหมายการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีทั้งในระดับประเทศและสากล ศึกษากรอบกฎหมายหลัก กฎหมายรอง และนโยบายที่เกี่ยวข้อง เช่น กฎหมายป้องกันอาชญากรรมไซเบอร์ กฎหมายคุ้มครองข้อมูลส่วนบุคคล กฎหมายอาชญากรรมทางเทคโนโลยีในประเทศต่าง ๆ และอนุสัญญาระหว่างประเทศ การวิเคราะห์สภาพปัญหาและประเภทของอาชญากรรมทางเทคโนโลยี เช่น การโจรกรรมข้อมูล การหลอกลวงออนไลน์ และการโจมตีระบบคอมพิวเตอร์ ตลอดจนการศึกษาเกี่ยวกับปัญหาหรืออุปสรรคในการบังคับใช้กฎหมาย และการนำเสนอแนวทางในการปรับปรุงการบังคับใช้กฎหมายให้มีประสิทธิภาพ และการศึกษาการใช้เทคโนโลยีในการสนับสนุนการป้องกันและสืบสวนอาชญากรรมทางเทคโนโลยี

๑.๓.๒ ขอบเขตด้านระยะเวลา

การศึกษาครั้งนี้ ผู้จัดทำได้ทำการศึกษาตั้งแต่เดือนกุมภาพันธ์ ๒๕๖๘ ถึงเดือนมีนาคม ๒๕๖๘ รวมใช้ระยะเวลาในการศึกษาทั้งสิ้นโดยประมาณ ๒ เดือน ซึ่งผู้จัดทำได้มีการทบทวนเอกสารวิชาการ กฎหมายหลัก กฎหมายรอง และนโยบายที่เกี่ยวข้องกับปัญหาอาชญากรรมทางเทคโนโลยีในประเทศไทย โดยมุ่งเน้นไปที่การวิเคราะห์และการสรุปผล

๑.๔ วิธีการศึกษา

เอกสารวิชาการฉบับนี้ ผู้จัดทำได้กำหนดระเบียบวิธีการศึกษาด้วยการใช้กระบวนการศึกษาเชิงคุณภาพ โดยการทบทวนเอกสารวิชาการ กฎหมายหลัก กฎหมายรอง และนโยบายที่เกี่ยวข้องกับปัญหาอาชญากรรมทางเทคโนโลยีทั้งในประเทศไทยและต่างประเทศ เพื่อนำมาวิเคราะห์กรณีศึกษาของการปฏิบัติและการบังคับใช้กฎหมายของต่างประเทศ เพื่อให้ได้ข้อเสนอแนะในการปรับปรุงและพัฒนากลไกการบังคับใช้กฎหมายที่มีประสิทธิภาพ ผู้จัดทำจึงได้แบ่งประเด็นการศึกษาเกี่ยวกับมาตรการทางกฎหมายและนโยบายในการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีของประเทศไทยที่ครอบคลุมในหลายมิติ เพื่อให้เข้าใจถึงประสิทธิภาพ อุปสรรค และแนวทางพัฒนาได้อย่างรอบด้าน สามารถแบ่งเป็นประเด็นสำคัญ ดังนี้

๑.๔.๑ สภาพปัญหาอาชญากรรมทางเทคโนโลยีในประเทศไทย

๑) ศึกษารูปแบบของกลยุทธ์และเทคนิคของกลุ่มผู้โจมตี (Tactics)

๒) ศึกษาการโจมตีของแฮกเกอร์

๓) ศึกษาประเภทของอาชญากรรมทางเทคโนโลยี

๔) ศึกษารูปแบบการกระทำผิดอาชญากรรมทางเทคโนโลยี โดยศึกษาลักษณะคดีในรูปแบบการกระทำผิดอาชญากรรมทางเทคโนโลยีและรูปแบบอาชญากรรมทางเทคโนโลยีที่พบมากในสังคมไทยปัจจุบัน

๑.๔.๒ แนวคิดทางกฎหมายและนโยบายในการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยี

๑) ศึกษากฎหมายหลักที่เกี่ยวข้องกับการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยี ประกอบด้วย พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และกฎหมายเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๖ และพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ ๒) พ.ศ. ๒๕๖๘

๒) ศึกษากฎหมายลำดับรองที่เกี่ยวข้องกับการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยี

๓) ศึกษาความร่วมมือระหว่างประเทศที่เกี่ยวข้องกับการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยี

๔) ศึกษากลไกการบังคับใช้กฎหมาย

๕) ศึกษาบทบาทและหน้าที่ของหน่วยงานที่เกี่ยวข้อง

๑.๔.๓ ถอดบทเรียนความสำเร็จการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยี

๑) ศึกษาและวิเคราะห์ผ่านบทเรียนความสำเร็จการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีของประเทศสิงคโปร์ จากการประเมิน Global Cybersecurity Index หรือ GCI ที่มีกรอบปัจจัยจากการพิจารณา ๕ ด้าน ประกอบด้วย ด้านกฎหมาย (Legal Measure) ด้านมาตรการทางเทคนิค (Technical Measure) ด้านหน่วยงาน/นโยบาย (Organizational Measure) ด้านการพัฒนาศักยภาพ (Capacity Development Measure) และด้านความร่วมมือ (Cooperative Measure) โดยการประเมินดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ของสหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union หรือ ITU) มีวัตถุประสงค์เพื่อวัดผลสัมฤทธิ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศต่าง ๆ ซึ่งเป็นองค์กรระหว่างประเทศที่มีหน้าที่ส่งเสริมการพัฒนาเทคโนโลยีโทรคมนาคมและสารสนเทศ

๒) ศึกษาและวิเคราะห์การแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีของประเทศไทยโดยการประเมินดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ของสหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union หรือ ITU)

๑.๔.๔ การสรุปผล แนวทางพัฒนา และข้อเสนอแนะ

๑.๕ ประโยชน์ที่คาดว่าจะได้รับ

๑.๕.๑ ทราบถึงสภาพปัญหา รูปแบบของกลยุทธ์และประเภทของอาชญากรรมทางเทคโนโลยี ตลอดจนรูปแบบการกระทำผิดอาชญากรรมทางเทคโนโลยีในประเทศไทย

๑.๕.๒ ทราบถึงกรอบและการบังคับใช้กฎหมายหลัก กฎหมายรอง และนโยบายในการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีของหน่วยงานที่เกี่ยวข้องทั้งในระดับประเทศและสากล

๑.๕.๓ ทราบถึงแนวทางในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีของประเทศไทยที่มีประสิทธิภาพและเกิดประสิทธิผล

บทที่ ๒
สภาพปัญหาอาชญากรรมทางเทคโนโลยีในประเทศไทย

การพัฒนาของอินเทอร์เน็ตและเทคโนโลยีดิจิทัลที่ทันสมัยได้เข้ามาปรับเปลี่ยนวิถีชีวิตของประชากรทั่วโลกอย่างมีนัยสำคัญ อาจกล่าวได้ว่าสมาร์ทโฟน (Smart phone)[๔] ได้กลายเป็นปัจจัยสำคัญที่ส่งผลต่อการดำเนินชีวิตประจำวันของมนุษย์ ทำให้การสื่อสารและการเข้าถึงข้อมูลเป็นไปอย่างสะดวกและรวดเร็ว นอกจากนี้ เทคโนโลยีดิจิทัลยังมีบทบาทสำคัญในการเพิ่มโอกาสในการพัฒนาเศรษฐกิจและยกระดับคุณภาพชีวิตของประชากรโลก อย่างไรก็ตาม การพึ่งพาพื้นที่ไซเบอร์ในระดับที่มากขึ้นได้นำมาซึ่งผลกระทบเชิงลบควบคู่กันไป ปัจจุบันมีบุคคลจำนวนมากที่ใช้เทคโนโลยีในทางที่มิชอบ ก่อให้เกิดภัยคุกคามต่อทรัพย์สิน สภาพจิตใจของบุคคล ตลอดจนความมั่นคงของรัฐ ตัวอย่างสำคัญ ได้แก่ การฉ้อโกงทางการเงินผ่านแพลตฟอร์มออนไลน์ หรือการลักลอบเข้าถึงบัญชีธนาคารโดยมิชอบ ซึ่งปรากฏให้เห็นอย่างแพร่หลายในช่วงไม่กี่ปีที่ผ่านมา และได้กลายเป็นภัยคุกคามที่ส่งผลกระทบต่อประชากรทั่วโลก ความซับซ้อนของปัญหาดังกล่าวทวีความรุนแรงขึ้น เมื่อพิจารณาถึงลักษณะของพื้นที่ไซเบอร์ซึ่งมีความไร้พรมแดนและอยู่ภายใต้ขอบเขตของกฎหมายที่จำกัด ทำให้การบังคับใช้กฎหมายและการติดตามพฤติกรรมอาชญากรรมในโลกดิจิทัลเป็นไปได้ยากขึ้น อีกทั้งอาชญากรไซเบอร์ยังสามารถปรับเปลี่ยนวิธีการเพื่อหลีกเลี่ยงการถูกดำเนินคดี ส่งผลให้กลโกงและการกระทำผิดในลักษณะดังกล่าวยังคงเกิดขึ้นอย่างต่อเนื่อง ก่อให้เกิดความเสียหายในระดับบุคคลสะสมจนส่งผลกระทบต่อระบบเศรษฐกิจ ความมั่นคงของประเทศ ตลอดจนเสถียรภาพของระบบการเงินในระดับสากล

อาชญากรรมทางเทคโนโลยี[๕] หมายถึง การกระทำผิดที่เกี่ยวข้องกับการใช้คอมพิวเตอร์หรือเครื่องมือทางเทคโนโลยีในการก่อให้เกิดความเสียหายแก่บุคคล องค์กร หรือสังคมโดยรวม ตัวอย่างของอาชญากรรมประเภทนี้ ได้แก่ การลักทรัพย์อุปกรณ์คอมพิวเตอร์ ตลอดจนการกระทำผิดทางอาญาที่ต้องอาศัยความรู้ด้านคอมพิวเตอร์ในการดำเนินการ เช่น การบิดเบือนข้อมูล (Extortion) การเผยแพร่สื่อลามกอนาจารที่เกี่ยวข้องกับผู้เยาว์ (Child Pornography) การฟอกเงิน (Money Laundering) การฉ้อโกง (Fraud) การถอดรหัสซอฟต์แวร์โดยไม่ได้รับอนุญาตและเผยแพร่ให้ผู้อื่นดาวน์โหลดหรือที่เรียกว่า การละเมิดลิขสิทธิ์ซอฟต์แวร์ (Software Piracy) รวมถึงการขโมยข้อมูลความลับทางการค้าของบริษัท (Corporate Espionage) เป็นต้น[๖] ซึ่งอาชญากรรมทางเทคโนโลยีสามารถกระทำต่อบุคคล

---

[๔] สมาร์ตโฟน (Smart phone) คือ โทรศัพท์ที่รองรับระบบปฏิบัติการต่าง ๆ ที่ย่อเอาความสามารถในการรับส่งข้อมูล ดูหนังฟังเพลง การจัดการไฟล์ต่าง ๆ ที่เทียบได้กับคอมพิวเตอร์พื้นฐานย่อม ๆ ตัวหนึ่งมาไว้ในตัว ทำให้โทรศัพท์มือถือเพิ่มความสามารถมากไปกว่าการโทรศัพท์ออกและรับสาย โปรดดู สำนักราชบัณฑิตยสภา, *ประเภทของโทรศัพท์มือถือ*, สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘. จาก https://www.orst.go.th/FILEROOM/CABROYINWEB/DRAWER๐๐๔/GENERAL/DATA๐๐๐๐/๐๐๐๐๐๖๒๔.FLP/html/๕๒/#zoom=z

[๕] อภิชาต บวบขม. อาชญากรรมทางเทคโนโลยี: กฎหมายและแนวทางการป้องกันแบบบูรณาการ, *Journal of Roi Kaensarn Academi*, ๘(๑๒) ธันวาคม ๒๕๖๖: ๗๒๘-๗๒๙.

[๖] Shelly, G. & Vermaat, M., *Discovering Computers ๒๐๑๑*. (Complete: Cengage Learning, ๒๐๑๐).

กลุ่มบุคคลหรือองค์กร โดยมีแรงจูงใจที่มุ่งทำให้เหยื่อได้รับความเสียหาย ไม่ว่าจะเป็นด้านชื่อเสียง สุขภาพจิต หรือร่างกายทั้งทางตรงและทางอ้อม ลักษณะสำคัญของอาชญากรรมประเภทนี้ คือ การอาศัยเครือข่ายโทรคมนาคมสมัยใหม่เป็นช่องทางในการกระทำความผิด เช่น การใช้อินเทอร์เน็ต ผ่านคอมพิวเตอร์หรือโทรศัพท์เคลื่อนที่ (เช่น ห้องสนทนาออนไลน์ อีเมล กระดานประกาศ และกลุ่มข่าว) ตลอดจนการใช้อุปกรณ์โทรศัพท์เคลื่อนที่ในการส่งข้อความสั้น (SMS) หรือข้อความมัลติมีเดีย (MMS) เพื่อดำเนินการทางอาชญากรรม อาชญากรรมทางเทคโนโลยีจึงเป็นความท้าทายสำคัญที่ต้องได้รับการจัดการอย่างเป็นระบบ เพื่อป้องกันและลดผลกระทบที่อาจเกิดขึ้นต่อบุคคลและสังคมโดยรวม

๒.๑ รูปแบบของกลยุทธ์และเทคนิคของกลุ่มผู้โจมตี (Tactics)[๗]

๒.๑.๑ รูปแบบของกลยุทธ์ของกลุ่มผู้โจมตี

MITRE ATT&CK เป็นโครงการที่พัฒนาโดย MITRE Corporation ซึ่งเป็นองค์กรไม่แสวงหาผลกำไรที่ก่อตั้งขึ้นในปี ค.ศ. ๑๙๕๘ โดยมีวัตถุประสงค์เพื่อแก้ไขปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์ และส่งเสริมให้เกิดสภาพแวดล้อมที่ปลอดภัยมากยิ่งขึ้น โครงการดังกล่าวมุ่งเน้นการพัฒนาแนวคิด วิธีการ และกระบวนการ เพื่อปกป้องระบบสารสนเทศให้มีความมั่นคงปลอดภัย ตลอดจนรวบรวมข้อมูลเกี่ยวกับการทดสอบความปลอดภัยของอุปกรณ์และผลิตภัณฑ์ที่เกี่ยวข้องกับ Cybersecurity คำว่า ATT&CK เป็นคำย่อจาก "Adversarial Tactics, Techniques, and Common Knowledge" ซึ่งหมายถึงแพลตฟอร์มที่ใช้ในการบริหารจัดการและจัดหมวดหมู่ กลยุทธ์ (Tactics) เทคนิค (Techniques) และกระบวนการ (Procedures) ที่ผู้ไม่หวังดีใช้ในการโจมตีระบบเครือข่ายและโครงสร้างพื้นฐานทางไซเบอร์ โดยมีวัตถุประสงค์เพื่อช่วยให้องค์กรสามารถเพิ่มประสิทธิภาพในการป้องกันภัยคุกคามทางไซเบอร์ MITRE ATT&CK ทำหน้าที่เป็นฐานข้อมูลความรู้ (Knowledge Sharing Base) ขนาดใหญ่ ซึ่งใช้ในการจำแนกประเภทของการโจมตีทางไซเบอร์ วิธีการที่ใช้ ตลอดจนแพลตฟอร์มที่ได้รับผลกระทบ โดยข้อมูลเหล่านี้ถูกจัดเรียงในรูปแบบ Enterprise Matrix ที่จำแนกพฤติกรรมของกลุ่มผู้โจมตี (Tactics) ในแต่ละขั้นตอนของการโจมตี ปัจจุบัน Enterprise Tactics ถูกแบ่งออกเป็น ๑๔ หมวดหมู่หลัก ดังแสดงในตารางที่ ๑

ตารางที่ ๑ การอธิบายขั้นตอนของการโจมตี (Enterprise Tactics)

ชื่อ	รายละเอียด
Collection	ทำการเตรียมดึงข้อมูลออกจากระบบ หรือเป้าหมาย
Command and Control	การเชื่อมต่อระหว่างระบบที่ถูกโจมตีกับเครือข่ายหรือเซิร์ฟเวอร์ของผู้โจมตี ทำให้สามารถควบคุมระบบจากระยะไกลได้
Credential Access	ขโมยรหัส บัญชีผู้ใช้ และทำการเข้าสู่ระบบ

[๗] ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ, *รายงาน MITRE ATT&CK Matrix ประจำเดือนธันวาคม ปี ๒๕๖๗*, สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘. จาก https://drive.ncsa.or.th/s/eQx๒Y๓yP๓๒oaQpN

ตารางที่ ๑ การอธิบายขั้นตอนของการโจมตี (Enterprise Tactics) (ต่อ)

ชื่อ	รายละเอียด
Defense Evasion	หลบเลี่ยงโปรแกรมตรวจจับหรือโปรแกรมสังเกตความผิดปกติ
Discovery	เป็นขั้นตอนที่ผู้โจมตีใช้ในการตรวจสอบและรวบรวมข้อมูลเกี่ยวกับระบบเป้าหมาย โดยมีเป้าหมายเพื่อหาข้อมูลที่สำคัญ
Execution	สั่งการโปรแกรมที่เตรียมไว้ หรือ Code ที่อันตรายที่เป้าหมาย
Exfiltration	กระบวนการที่ผู้โจมตีใช้เพื่อดึงหรือส่งข้อมูลสำคัญออกจากระบบเป้าหมายไปยังเครือข่ายของผู้โจมตี โดยข้อมูลที่ถูกขโมยอาจรวมถึงข้อมูลที่เป็นความลับ
Impact	เป็นขั้นตอนสุดท้ายที่ผู้โจมตีดำเนินการเพื่อให้บรรลุวัตถุประสงค์ที่ตั้งไว้ ซึ่งอาจรวมถึงการทำลายระบบ การขโมยหรือทำลายข้อมูลที่สำคัญ หรือการลบหลักฐานการโจมตี เพื่อทำให้ยากต่อการตรวจสอบและป้องกัน
Initial Access	เข้าถึงระบบเป้าหมาย หรือเชื่อมกับเครื่องที่ต้องการโจมตี
Lateral Movement	การเคลื่อนที่เข้าควบคุมเครื่องเป้าหมาย หรือหาข้อมูลอื่น ๆ ในเน็ตเวิร์ค
Persistence	ทำให้การควบคุมของผู้โจมตีคงอยู่และไม่ถูกขัด แม้หลังจากการรีบูตระบบ
Privilege Escalation	การยกระดับสิทธิ์การเข้าถึง เป็นเทคนิคที่ผู้โจมตีใช้เพื่อเพิ่มสิทธิ์ในระบบจากระดับที่ต่ำ (เช่น ผู้ใช้งานทั่วไป) ไปเป็นระดับสูง (เช่น ผู้ดูแลระบบ) โดยมีเป้าหมายเพื่อเข้าถึงและควบคุมระบบทั้งหมดได้
Reconnaissance	รวบรวมข้อมูลก่อนการโจมตีของเป้าหมายให้ได้มากที่สุด
Resource Development	เตรียมเครื่องมือเพื่อโจมตีเป้าหมาย ทั้งเขียนเอง ซื้อ หรือขโมยมา

ที่มา : ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ, รายงาน MITRE ATT&CK Matrix ประจำเดือนธันวาคม ปี ๒๕๖๗, สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘. จาก https://drive.ncsa.or.th/s/eQx๒Y๓yP๓๒oaQpN

๑) Collection ประกอบไปด้วยเทคนิคที่ผู้โจมตีใช้ในการรวบรวมข้อมูลที่จำเป็นเพื่อสนับสนุนการโจมตีเป้าหมายหลัก หลังจากการรวบรวมข้อมูลแล้ว ขั้นตอนถัดไปมักจะเกี่ยวข้องกับการขโมยข้อมูล (Exfiltrate) หรือการใช้ข้อมูลที่ได้มาเพื่อหาข้อมูลเพิ่มเติมเกี่ยวกับการตั้งค่าหรือ

ข้อมูลของอุปกรณ์เป้าหมาย โดยทั่วไปแล้ว ผู้โจมตีมักจะมุ่งเป้าไปที่ข้อมูลที่เก็บอยู่ในไดรฟ์เก็บข้อมูลเบราว์เซอร์ ข้อมูลเสียง วิดีโอ และอีเมลในอุปกรณ์ที่ถูกเข้าถึง

๒) Command and Control ประกอบด้วยเทคนิคที่ผู้โจมตีใช้เพื่อสื่อสารและควบคุมระบบที่ถูกเข้าครอบครองภายในเครือข่ายของเหยื่อ ผู้โจมตีมักจะเลียนแบบการรับส่งข้อมูลปกติเพื่อหลีกเลี่ยงการตรวจจับ ความลับและความแนบเนียนของการส่งข้อมูลนั้นขึ้นอยู่กับโครงสร้างเครือข่ายและความมั่นคงของการป้องกันของเหยื่อ

๓) Credential Access ประกอบด้วยทคนิคที่ผู้โจมตีใช้ในการขโมยข้อมูลที่ใช้สำหรับการยืนยันสิทธิ์ เช่น ชื่อบัญชีและรหัสผ่าน เทคนิคที่ใช้ในการขโมยข้อมูลเหล่านี้รวมถึงการบันทึกการกดแป้นพิมพ์ (Keylogging) หรือการดึงข้อมูลการยืนยันสิทธิ์ (Credential Dumping) การใช้ข้อมูลที่ได้จากการเข้าสู่ระบบเหล่านี้สามารถช่วยให้ผู้โจมตีเข้าถึงระบบได้โดยยากต่อการตรวจจับ และอาจมีการสร้างบัญชีใหม่เพื่อใช้ในการสอดแนมเพิ่มเติม

๔) Defense Evasion ประกอบด้วยเทคนิคที่ผู้โจมตีใช้เพื่อหลีกเลี่ยงการตรวจจับโดยเทคนิคที่ใช้ในการหลบเลี่ยงการป้องกันรวมถึงการถอนการติดตั้งหรือปิดการใช้งานซอฟต์แวร์รักษาความปลอดภัย หรือการทำให้หลักฐานยากต่อการตรวจสอบ เช่น การเบลอข้อมูล (Obfuscating) หรือการเข้ารหัส (Encrypting) ผู้โจมตียังอาจใช้กระบวนการที่เชื่อถือได้เพื่อซ่อนหรือปลอมแปลงมัลแวร์ให้เป็นกระบวนการเหล่านั้น

๕) Discovery ประกอบด้วยเทคนิคที่ผู้โจมตีใช้เพื่อให้ได้ข้อมูลเพิ่มเติมเกี่ยวกับระบบและเครือข่ายภายใน การสำรวจและสอดแนมโครงสร้างของเครือข่ายในขั้นตอนนี้ ช่วยให้ผู้โจมตีสามารถตัดสินใจได้ว่าจะดำเนินการอย่างไรในขั้นตอนถัดไป และสามารถควบคุมหรือใช้ประโยชน์จากส่วนใดของระบบเพื่อบรรลุวัตถุประสงค์ของการโจมตี

๖) Execution ประกอบด้วยเทคนิคที่ผู้โจมตีใช้เพื่อให้โค้ดที่เป็นอันตรายทำงานบนระบบที่เข้าถึงได้ทั้งทางกายภาพหรือผ่านอินเทอร์เน็ต เทคนิคในการรันโค้ดมักจะถูกใช้ร่วมกับเทคนิคอื่น ๆ เพื่อช่วยบรรลุเป้าหมายของการโจมตี เช่น การสำรวจเครือข่ายหรือการขโมยข้อมูล โดยอาจใช้สคริปต์ PowerShell

๗) Exfiltration ประกอบด้วยเทคนิคที่ผู้โจมตีใช้เพื่อขโมยข้อมูลจากเครือข่ายของเป้าหมาย เมื่อเข้าถึงข้อมูลที่ต้องการแล้ว ผู้โจมตีมักจะทำการบีบอัดข้อมูล (Compression) เพื่อหลีกเลี่ยงการตรวจจับขณะส่งข้อมูลออกจากระบบ หรืออาจใช้การเข้ารหัส (Encryption) เทคนิคการส่งข้อมูลออกจากเครือข่ายอาจทำผ่านช่องทาง Command and Control (C๒) และรวมถึงการจำกัดขนาดของการส่งข้อมูลโดยการแบ่งข้อมูลเป็นชิ้นส่วนเล็ก ๆ เพื่อหลีกเลี่ยงการตรวจจับ

๘) Impact ประกอบด้วยเทคนิคที่ผู้โจมตีใช้เพื่อสร้างผลกระทบต่อความพร้อมใช้งาน (Availability) ความสมบูรณ์ (Integrity) หรือความลับของข้อมูล (Confidentiality) เทคนิคที่ใช้รวมถึงการทำลายหรือการแก้ไขข้อมูล และการใช้ทรัพยากรของระบบจนหมดเพื่อทำให้ผู้ใช้งานไม่สามารถดำเนินการตามปกติ

๙) Initial Access ประกอบด้วยเทคนิคที่ผู้โจมตีใช้ช่องทางการเข้าถึงที่เปิดอยู่ในระบบเพื่อเริ่มต้นการโจมตีในเครือข่ายของเป้าหมาย เทคนิคในการเข้าถึงเบื้องต้น ได้แก่ การโจมตีแบบ Spear Phishing ซึ่งเป็นการโจมตีที่มุ่งเน้นไปที่บุคคลหรือกลุ่มเป้าหมายเฉพาะ และการใช้ช่องโหว่ที่มีอยู่ในเว็บเซิร์ฟเวอร์ที่สามารถเข้าถึงได้โดยสาธารณะ

๑๐) Lateral Movement ประกอบด้วยเทคนิคที่ผู้โจมตีใช้เพื่อเข้าสู่ระบบระยะไกลภายในเครือข่ายและควบคุมระบบเหล่านั้น โดยมักจะมีการสำรวจเครือข่ายเพื่อค้นหาเป้าหมายที่สำคัญก่อนที่จะเข้าถึงเป้าหมายดังกล่าว ผู้โจมตีอาจเคลื่อนที่ผ่านหลายระบบและบัญชีเพื่อให้ได้มาซึ่งสิทธิ์ที่สูงขึ้น อาจติดตั้งเครื่องมือควบคุมระยะไกล หรือใช้บัญชีผู้ใช้ที่ถูกร่วมกับเครื่องมือในระบบปฏิบัติการและเครือข่ายที่มีอยู่แล้ว ซึ่งทำให้การตรวจจับการกระทำเหล่านี้ยากยิ่งขึ้น

๑๑) Persistence ประกอบด้วยเทคนิคที่ผู้โจมตีใช้เพื่อรักษาการเข้าถึงระบบหลังจากการรีบูต การเปลี่ยนรหัสผ่าน หรือการดำเนินการใด ๆ ที่อาจตัดการเข้าถึง เทคนิคที่ใช้ในการรักษาการเข้าถึงรวมถึงการปรับเปลี่ยนการตั้งค่าของระบบ เช่น การแทนที่หรือปรับปรุงโค้ดของกระบวนการพื้นฐาน หรือการเพิ่มโค้ดที่เริ่มทำงานอัตโนมัติเมื่อระบบทำการบูตใหม่

๑๒) Privilege Escalation เทคนิคที่ผู้โจมตีใช้เพื่อยกระดับสิทธิ์การเข้าถึงในระบบหรือเครือข่าย โดยเริ่มต้นจากการเข้าถึงระบบด้วยบัญชีที่มีสิทธิ์จำกัด แต่เพื่อให้สามารถดำเนินการโจมตีต่อไปได้ พวกเขาจำเป็นต้องได้รับสิทธิ์ที่สูงขึ้น เทคนิคที่ใช้บ่อยในการยกระดับสิทธิ์ คือ การหาประโยชน์จากจุดอ่อนที่มีอยู่ในระบบหรือการตั้งค่าที่ผิดพลาด เทคนิคเหล่านี้มักถูกใช้ร่วมกับเทคนิค Persistence เพื่อให้การเข้าถึงยังคงมีอยู่ในระยะยาว

๑๓) Reconnaissance หรือการสอดแนม ประกอบด้วยเทคนิคที่ผู้โจมตีใช้ในการรวบรวมข้อมูลทั้งในรูปแบบ Passive และ Active ข้อมูลที่รวบรวมได้สามารถนำไปใช้ในการสนับสนุนการเลือกเป้าหมาย เช่น รายละเอียดเกี่ยวกับองค์กรของเหยื่อ โครงสร้างพื้นฐาน หรือพนักงาน/บุคลากร ข้อมูลเหล่านี้สามารถนำไปใช้ในขั้นตอนอื่น ๆ ของการโจมตี เช่น การวางแผนและดำเนินการ Initial Access การกำหนดขอบเขต และการจัดลำดับความสำคัญของเป้าหมายหลังจากการบุกรุก

๑๔) Resource Development ประกอบด้วยเทคนิคที่ผู้โจมตีใช้ในการสร้าง ซื้อ หรือขโมยทรัพยากรที่สามารถใช้สนับสนุนการโจมตีได้ง่ายขึ้น ทรัพยากรเหล่านี้รวมถึงอุปกรณ์ เซิร์ฟเวอร์ บัญชีผู้ใช้จากระบบต่าง ๆ ทรัพยากรเหล่านี้สามารถใช้โดยผู้โจมตีในขั้นตอนอื่น ๆ เช่น การใช้โดเมนที่ซื้อมาเพื่อสนับสนุนการทำ Command and Control Server การใช้บัญชีอีเมลในการโจมตีแบบ Phishing เพื่อสร้าง Initial Access หรือการขโมย Code Signing Signature เพื่อหลีกเลี่ยงการตรวจจับ (Defense Evasion)

๒.๑.๒ เทคนิคในการโจมตีของผู้บุกรุกทางไซเบอร์

๑) การเข้ารหัสข้อมูลเพื่อสร้างผลกระทบ (Data Encrypted for Impact) เป็นกระบวนการเข้ารหัสข้อมูลที่จัดเก็บอยู่ในระบบเป้าหมายหรือในเครือข่าย เพื่อทำลายความสามารถในการเข้าถึงข้อมูล (Availability) ซึ่งส่งผลให้ข้อมูลดังกล่าวไม่สามารถใช้งานได้

โดยการโจมตีนี้มักมีวัตถุประสงค์เพื่อเรียกค่าไถ่จากผู้เสียหาย (Ransomware) โดยแลกกับรหัสถอดรหัส หรืออาจเป็นการทำลายข้อมูลอย่างถาวรหากไม่มีการส่งรหัสถอดรหัสให้แก่เหยื่อ

๒) การปฏิเสธการให้บริการเครือข่าย (Network Denial of Service - DoS) เป็นการโจมตีที่มุ่งลดระดับหรือขัดขวางการให้บริการของระบบเป้าหมาย โดยใช้ทรัพยากรเครือข่ายจนหมดสิ้น ส่งผลให้บริการต่าง ๆ เช่น เว็บไซต์ บริการอีเมล ระบบชื่อโดเมน (DNS) และเว็บแอปพลิเคชันไม่สามารถให้บริการได้ ทั้งนี้ การโจมตีลักษณะนี้อาจมีวัตถุประสงค์ทางการเมือง การขู่กรรโชก หรือเพื่อเบี่ยงเบนความสนใจจากกิจกรรมที่เป็นอันตรายอื่น ๆ

๓) การเปลี่ยนแปลงเนื้อหาในระบบ (Defacement) เป็นการโจมตีที่มุ่งเปลี่ยนแปลงหรือดัดแปลงเนื้อหาภายในหรือภายนอกเครือข่ายขององค์กร ซึ่งเป็นการละเมิดความถูกต้องของข้อมูล (Integrity) โดยการโจมตีลักษณะนี้อาจแสดงข้อความข่มขู่ ส่งสารที่แสดงถึงวัตถุประสงค์ของผู้โจมตี หรือใช้ภาพที่ไม่เหมาะสมเพื่อทำลายชื่อเสียงของบุคคลหรือองค์กร

๔) การปฏิเสธการให้บริการต่ออุปกรณ์ปลายทาง (Endpoint Denial of Service - DoS) เป็นการโจมตีที่ใช้ทรัพยากรของอุปกรณ์ปลายทางเป้าหมายจนหมด ส่งผลให้ระบบไม่สามารถดำเนินการได้ เป้าหมายหลักของการโจมตีลักษณะนี้ ได้แก่ เว็บไซต์ บริการอีเมล ระบบชื่อโดเมน (DNS) และเว็บแอปพลิเคชัน ซึ่งอาจมีวัตถุประสงค์เพื่อขู่กรรโชก หรือสนับสนุนกิจกรรมที่เป็นอันตรายอื่น ๆ

๕) การลักลอบนำข้อมูลออกผ่านบริการเว็บ (Exfiltration Over Web Service) เป็นการลักลอบขโมยข้อมูลโดยใช้บริการจากเว็บไซต์ทั่วไปแทนการควบคุมระบบของเหยื่อโดยตรง ซึ่งทำให้ตรวจสอบได้ยาก เนื่องจากระบบภายในองค์กรมักอนุญาตให้มีการติดต่อกับบริการเว็บเหล่านี้อยู่แล้ว รวมถึงการกำหนดค่าของไฟร์วอลล์ที่อาจไม่สามารถป้องกันพฤติกรรมดังกล่าวได้

๖) การลักลอบนำข้อมูลออกผ่านช่องทางคำสั่งและควบคุม (Exfiltration Over C๒ Channel) เป็นกระบวนการขโมยข้อมูลผ่านเซิร์ฟเวอร์ Command & Control (C๒) โดยข้อมูลที่ถูกขโมยจะถูกเข้ารหัสและส่งผ่านช่องทางการสื่อสารที่ใช้โปรโตคอลเดียวกันกับที่ผู้โจมตีใช้ในการควบคุมระบบของเหยื่อ

๗) การลักลอบนำข้อมูลออกผ่านโปรโตคอลทางเลือก (Exfiltration Over Alternative Protocol) เป็นการขโมยข้อมูลโดยใช้โปรโตคอลที่แตกต่างจากช่องทางการสื่อสารปกติของผู้โจมตีและเหยื่อ โดยอาจมีการส่งข้อมูลไปยังเครือข่ายอื่นก่อนเพื่อปกปิดตำแหน่งที่แท้จริงของผู้กระทำความผิด

๘) การใช้เครื่องมือแปลคำสั่งและสคริปต์เพื่อโจมตี (Command and Scripting Interpreter) เป็นการใช้เครื่องมือที่สามารถรันคำสั่งหรือสคริปต์เพื่อดำเนินกิจกรรมที่เป็นอันตรายต่อระบบเป้าหมาย โดยระบบปฏิบัติการส่วนใหญ่มักรองรับการใช้คำสั่งผ่าน Command-Line Interface (CLI) เช่น ระบบปฏิบัติการ macOS และ Linux ใช้ Unix Shell ขณะที่ Windows ใช้ Command Shell และ PowerShell ซึ่งผู้โจมตีอาจใช้ช่องโหว่ในระบบเหล่านี้เพื่อดำเนินการโจมตี

๙) การหลอกล่อให้เหยื่อดำเนินการเปิดไฟล์ที่เป็นอันตราย (User Execution & Malicious File) เป็นการใช้เทคนิคทางวิศวกรรมสังคม (Social Engineering) เพื่อชักจูงให้เหยื่อเปิดไฟล์ที่มีมัลแวร์แฝงอยู่ เช่น การโจมตีแบบ Spear Phishing Attachment ซึ่งแนบไฟล์อันตรายมากับอีเมล ไฟล์ที่ใช้ในการโจมตีอาจอยู่ในรูปแบบต่าง ๆ เช่น .doc, .pdf, .xls, .rtf, .scr, .exe, .lnk, .pif, .cpl, .reg โดยไฟล์เหล่านี้จำเป็นต้องได้รับการเปิดใช้งานจากผู้ใช้จึงจะสามารถเริ่มต้นการโจมตีได้

๑๐) การโจมตีแบบฟิชชิงและการปลอมแปลงลิงก์เพื่อหลอกลวงเหยื่อ (Phishing & Spear Phishing Link) เป็นการส่งข้อความฟิชชิง (Phishing) ในรูปแบบต่าง ๆ เช่น อีเมลหรือข้อความ เพื่อชักจูงให้เหยื่อคลิกลิงก์ที่เป็นอันตราย ซึ่งอาจนำไปสู่การติดตั้งมัลแวร์ หรือการนำเหยื่อไปยังเว็บไซต์ปลอมเพื่อหลอกให้ป้อนข้อมูลสำคัญ โดย Spear Phishing เป็นรูปแบบเฉพาะของการโจมตีที่มีเป้าหมายไปยังบุคคลหรือองค์กรโดยเฉพาะ โดยอาจมีการปลอมตัวเป็นบุคคลที่น่าเชื่อถือเพื่อเพิ่มโอกาสในการหลอกลวงสำเร็จ

๒.๒ ประเภทของอาชญากรรมทางเทคโนโลยี

อาชญากรรมทางเทคโนโลยี (Cybercrime) คือ การกระทำความผิดทางกฎหมายโดยใช้คอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์เป็นเครื่องมือในการก่อให้เกิดความเสียหาย และ/หรือแสวงหาผลประโยชน์ส่วนตัวโดยมิชอบด้วยกฎหมาย อาชญากรรมทางไซเบอร์สามารถเกิดขึ้นในหลายรูปแบบ อาทิ การโจมตีระบบคอมพิวเตอร์ การทำลาย แก้ไข ขโมยข้อมูล การหลอกลวงให้เสียทรัพย์ การรู้เท่าทันอาชญากรรมทางไซเบอร์ที่เข้ามาเกี่ยวข้องกับชีวิตการทำงานและชีวิตประจำวันจึงเป็นสิ่งจำเป็นอย่างยิ่ง[๘] โดยรูปแบบของอาชญากรรมทางเทคโนโลยีนั้นมีหลายรูปแบบ ปัจจุบันทั่วโลกจัดแบ่งลักษณะของอาชญากรรมทางคอมพิวเตอร์ ออกเป็น ๙ ประเภทใหญ่[๙] ดังนี้

๑) การโจรกรรมข้อมูลและการลักลอบใช้บริการทางอินเทอร์เน็ตโดยมิชอบ การขโมยข้อมูลที่จัดเก็บอยู่ในระบบคอมพิวเตอร์ หรือการใช้บริการอินเทอร์เน็ตโดยไม่ได้รับอนุญาต ซึ่งอาจรวมถึงการเข้าถึงระบบเพื่อใช้ทรัพยากรของผู้อื่นโดยมิชอบ

๒) การปกปิดร่องรอยการกระทำความผิดโดยใช้ระบบคอมพิวเตอร์ การใช้เทคโนโลยีสารสนเทศเพื่อปกปิดตัวตนหรือความผิดของตนเอง เช่น การตั้งค่ารหัสผ่านหรือใช้เครื่องมือเข้ารหัสข้อมูลเพื่อป้องกันไม่ให้บุคคลอื่นสามารถตรวจสอบหรือเข้าถึงข้อมูลได้

๓) การละเมิดลิขสิทธิ์และการปลอมแปลงซอฟต์แวร์ การทำซ้ำ คัดลอก หรือลอกเลียนแบบซอฟต์แวร์โดยไม่ได้รับอนุญาตจากเจ้าของสิทธิ์ หรือการดัดแปลงโปรแกรมเพื่อใช้ประโยชน์โดยมิชอบ

---

[๘] รุ่งโรจน์ กิตติถาวรกุล, *รู้ เข้าใจและตระหนัก "อาชญากรรมทางไซเบอร์" (Cybercrime) ป้องกันภัยคุกคามใกล้ตัว*, สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘. จาก https://www.chula.ac.th/news/๑๓๘๒๙๑/

[๙] ราชกิจจานุเบกษา, *พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐*, สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘. จาก https://ratchakitcha.soc.go.th/documents/๒๑๗๕๕๓.pdf

๔) การเผยแพร่เนื้อหาลามกอนาจารและข้อมูลที่ไม่เหมาะสม การนำเสนอหรือเผยแพร่ภาพ เสียง หรือข้อความที่มีลักษณะลามก อนาจาร หรือขัดต่อศีลธรรมและจริยธรรมของสังคม

๕) การใช้คอมพิวเตอร์เพื่อกระทำความผิดเกี่ยวกับการฟอกเงิน การใช้ระบบคอมพิวเตอร์หรือธุรกรรมทางอิเล็กทรอนิกส์เพื่ออำพรางหรือแปลงสภาพเงินที่ได้จากการกระทำความผิดให้ดูเหมือนเป็นเงินที่ได้มาโดยชอบด้วยกฎหมาย

๖) การก่อกวนระบบคอมพิวเตอร์และระบบโครงสร้างพื้นฐาน การเจาะระบบเพื่อทำลายหรือขัดขวางการทำงานของระบบคอมพิวเตอร์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานที่สำคัญ เช่น ระบบสาธารณูปโภค ระบบจ่ายน้ำ ระบบจ่ายไฟฟ้า และระบบควบคุมการจราจร

๗) การหลอกลวงเพื่อชักชวนให้ลงทุนหรือทำธุรกิจโดยมิชอบด้วยกฎหมาย การใช้แพลตฟอร์มออนไลน์เพื่อหลอกลวงให้ผู้อื่นลงทุนในธุรกิจที่ไม่มีอยู่จริง หรือชักชวนให้ร่วมลงทุนในโครงการที่ผิดกฎหมาย

๘) การดัดแปลงข้อมูลเพื่อนำไปใช้ประโยชน์โดยมิชอบ การเข้าถึงหรือเปลี่ยนแปลงข้อมูลภายในระบบคอมพิวเตอร์เพื่อแสวงหาประโยชน์ส่วนตน เช่น การขโมยข้อมูลบัตรเครดิตหรือข้อมูลทางการเงินของบุคคลอื่น

๙) การโอนย้ายเงินจากบัญชีผู้อื่นเข้าสู่บัญชีของตนเองโดยมิชอบ การเข้าถึงระบบธนาคารออนไลน์หรือระบบธุรกรรมทางการเงิน เพื่อดำเนินการโอนเงินจากบัญชีของบุคคลอื่นมายังบัญชีของตนเองโดยไม่ได้รับอนุญาต

นอกจากนี้ ยังมีการแบ่งลักษณะของอาชญากรรมคอมพิวเตอร์ออกเป็นกลุ่ม[๑๐] โดยจำแนกไว้ดังนี้

๑) บุคคลที่มีประสบการณ์ด้านคอมพิวเตอร์ในระดับเริ่มต้น บุคคลที่เพิ่งเริ่มใช้งานคอมพิวเตอร์และอาจกระทำผิดโดยไม่รู้ตัว หรือมีเจตนาทดสอบความสามารถของตนเองในระบบคอมพิวเตอร์

๒) บุคคลที่มีแนวโน้มพฤติกรรมรุนแรงและเป็นอันตราย (Darned Person) บุคคลที่มีพฤติกรรมรุนแรงและใช้เทคโนโลยีในการกระทำผิดที่ส่งผลเสียต่อผู้อื่นหรือสังคม

๓) กลุ่มอาชญากรที่มีการจัดตั้งเป็นองค์กร (Organized Crime) กลุ่มบุคคลที่มีการวางแผนและดำเนินการกระทำผิดทางคอมพิวเตอร์ในรูปแบบองค์กรขนาดใหญ่ โดยมีโครงสร้างการทำงานที่ซับซ้อน

---

[๑๐] ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC), *ปัญหาคอมพิวเตอร์*, สืบค้นเมื่อวันที่ ๑๙ มกราคม ๒๕๖๘. จาก https://www.nectec.or.th/schoolnet/library/create-web/๑๐๐๐๐/technology
/๑๐๐๐๐-๑๒๓๗๙.html

๔) อาชญากรมืออาชีพ (Career Criminal) บุคคลที่มีทักษะสูงในด้านคอมพิวเตอร์และใช้ความสามารถของตนเพื่อกระทำความผิดเป็นอาชีพ

๕) บุคคลที่มีความเชี่ยวชาญด้านคอมพิวเตอร์และใช้ความสามารถเพื่อการฉ้อโกง (Con Artist) บุคคลที่มีความรู้ความสามารถทางเทคโนโลยีและใช้ทักษะดังกล่าวเพื่อดำเนินกิจกรรมที่ผิดกฎหมาย

๖) บุคคลที่มีความเชื่อมั่นในอุดมการณ์หรือแนวคิดบางอย่างอย่างสุดโต่ง (Dreamer) บุคคลที่ใช้เทคโนโลยีในการกระทำผิดโดยอ้างอุดมการณ์หรือความเชื่อส่วนบุคคล เช่น กลุ่มที่แฮ็กระบบเพื่อแสดงออกทางการเมืองหรือศาสนา

๗) กลุ่มแครกเกอร์ (Cracker) บุคคลที่มีทักษะสูงทางด้านคอมพิวเตอร์ โดยเฉพาะในด้านการเจาะระบบและการดัดแปลงข้อมูล ซึ่งอาจมีเจตนาในการก่อกวน ทำลาย หรือแสวงหาผลประโยชน์จากการโจมตีทางไซเบอร์

๒.๓ รูปแบบการกระทำผิดอาชญากรรมทางเทคโนโลยี

๒.๓.๑ ลักษณะคดีในรูปแบบการกระทำผิดอาชญากรรมทางเทคโนโลยี[๑๑]

ลักษณะคดีดังต่อไปนี้ เป็นการกำหนดรูปแบบการกระทำผิดในกรณีอาชญากรรมทางเทคโนโลยีที่เกี่ยวข้องกับการฉ้อโกง การกรรโชก การรีดเอาทรัพย์ หรือการกระทำใด ๆ ที่อาจทำให้ผู้อื่นได้รับความเสียหาย ซึ่งมีวัตถุประสงค์เพื่อให้สอดคล้องกับพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๖ และคำสั่งสำนักงานตำรวจแห่งชาติที่ ๑๘๒/๒๕๖๖ ลงวันที่ ๑๗ มีนาคม ๒๕๖๖ โดยกำหนดให้ใช้ในการมอบหมายหน้าที่ให้กับพนักงานสอบสวนที่รับผิดชอบ รวมถึงการให้สิทธิในการสืบสวนสอบสวนเกี่ยวกับความผิดตามลักษณะดังกล่าวแก่หน่วยงานต่าง ๆ ภายในสำนักงานตำรวจแห่งชาติ ดังนี้

๑) คดีหลอกลวงการซื้อขายสินค้าหรือบริการที่ไม่มีลักษณะเป็นขบวนการ ได้แก่ คดีที่มีการกระทำผิดโดยทุจริตและหลอกลวงตั้งแต่ต้นผ่านการประกาศหรือโฆษณาขายสินค้าหรือบริการผ่านสื่อสังคมออนไลน์ โดยเชิญชวนให้ผู้เสียหายเข้ามาซื้อสินค้าหรือใช้บริการ เมื่อผู้เสียหายได้ชำระเงินแล้ว แต่ไม่ได้รับสินค้า หรือบริการตามที่สัญญาไว้ หรือได้รับสินค้าและบริการในลักษณะที่มีเจตนาฉ้อโกง หรือได้รับสินค้าไม่ตรงตามที่ได้โฆษณา ทั้งในแง่ของแหล่งกำเนิด สภาพ คุณภาพ หรือปริมาณสินค้า ซึ่งเป็นข้อมูลที่ไม่เป็นจริง รวมถึงการหลอกลวงให้ผู้ขายในระบบออนไลน์ส่งสินค้าผ่านช่องทางออนไลน์ โดยมีเจตนาแต่แรกที่จะไม่ชำระค่าสินค้า

๒) คดีหลอกลวงโดยการใช้บุคคลอื่นเพื่อขอยืมเงิน ได้แก่ คดีที่กระทำผิดโดยการนำภาพของบุคคลอื่นมาใช้สร้างบัญชีสื่อสังคมออนไลน์ปลอมหรือเข้าถึงบัญชีสื่อสังคมออนไลน์ของบุคคลอื่น โดยการแอบอ้างตนเป็นเจ้าของบัญชีสื่อสังคมออนไลน์ดังกล่าว เพื่อหลอกให้ผู้เสียหาย

---

[๑๑] คำอธิบายลักษณะคดี ออกตามความใน ข้อ ๕ ของคำสั่งสำนักงานตำรวจแห่งชาติ ที่ ๑๘๒/๒๕๖๖ ลงวันที่ ๑๗ มีนาคม ๒๕๖๖, สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘. จาก https://www.gcc.go.th/wp-content/uploads/๒๐๒๔/๐๓/๖๗_cybercrime_๑๔type.pdf

หลงเชื่อและขอยืมเงิน หรือให้โอนเงินไปตามเหตุผลที่หลอกลวง เช่น การสร้างลิงก์ปลอมเพื่อขโมยรหัสล็อกอินของแอปพลิเคชันไลน์จากผู้อื่น แล้วนำไลน์ของผู้นั้นไปส่งข้อความขอยืมเงินจากผู้เสียหายที่เป็นเพื่อนในไลน์ของบุคคลดังกล่าว

๓) คดีหลอกลวงในลักษณะการสร้างความรักเพื่อขอเงิน (Romance Scam) ได้แก่ คดีที่กระทำผิดโดยการปลอมแปลงภาพถ่ายประจำตัว (Profile Picture) เป็นบุคคลอื่น แล้วสุ่มเข้ามาพูดคุยและตีสนิทกับผู้เสียหายในระบบออนไลน์ เพื่อสร้างความรัก ความน่าสนใจ หรือความน่าเชื่อถือ จากนั้นผู้กระทำความผิดจะสร้างเรื่องราวหลอกลวงให้ผู้เสียหายหลงเชื่อและโอนเงินให้ เช่น การปลอมแปลงโปรไฟล์เป็นทหารอเมริกันติดต่อมาผ่านเฟซบุ๊กหรือเว็บไซต์หาคู่ พูดคุยจนเกิดความสัมพันธ์และหลอกว่าจะส่งของมีค่ามาให้ผู้เสียหาย โดยมีผู้ร่วมขบวนการแอบอ้างตนเป็นเจ้าหน้าที่กรมศุลกากรหรือบริษัทขนส่งแจ้งผู้เสียหายให้โอนเงินเพื่อชำระภาษี หรืออ้างว่าเจ็บป่วยและต้องการเงินเพื่อช่วยเหลือ หรืออ้างว่าจำเป็นต้องใช้เงินจ้างทนายความเพื่อฟ้องร้องแบ่งมรดก เป็นต้น

๔) คดีหลอกลวงให้โอนเงินเพื่อรับรางวัลหรือวัตถุประสงค์อื่น ๆ ได้แก่ คดีที่มีการกระทำผิดโดยการสร้างเว็บไซต์ปลอมในสื่อสังคมออนไลน์หรือการส่งข้อความอันเป็นเท็จให้ผู้เสียหายทางโทรศัพท์ หรือช่องทางอื่น ๆ โดยทำให้ผู้เสียหายหลงเชื่อว่าตนเป็นผู้โชคดีได้รับรางวัลหรือสิทธิประโยชน์ต่าง ๆ แต่ต้องชำระค่าใช้จ่ายล่วงหน้าภายใต้ข้ออ้างต่าง ๆ เช่น ค่าสมาชิก ค่าธรรมเนียม ภาษี หรือค่าใช้จ่ายอื่น ๆ เมื่อผู้เสียหายได้โอนเงินแล้ว กลับไม่สามารถรับรางวัลดังกล่าวได้ และรวมถึงการกระทำผิดที่เกี่ยวข้องกับการฉ้อโกง กรรโชก หรือรีดเอาทรัพย์ผ่านระบบคอมพิวเตอร์ในรูปแบบอื่น เช่น การหลอกให้โอนเงินเพื่อทำบุญโดยไม่ได้นำไปทำบุญจริง หรือการข่มขู่โดยการใช้ข้อมูลส่วนตัวของผู้เสียหาย เช่น การตัดต่อภาพแล้วข่มขู่ให้โอนเงิน มิฉะนั้นจะนำข้อมูลไปเผยแพร่ในเพจเฟซบุ๊กที่เปิดให้สาธารณชนเข้าถึง

๕) คดีหลอกลวงให้กู้เงิน ได้แก่ คดีที่มีการกระทำผิดโดยการส่งข้อความ ประกาศหรือโฆษณาผ่านสื่อสังคมออนไลน์ เชิญชวนให้ประชาชนกู้ยืมเงิน เมื่อผู้เสียหายหลงเชื่อและดำเนินการขอกู้ยืมเงิน คนร้ายจะอ้างว่าเงินกู้ได้รับการอนุมัติแล้ว แต่จำเป็นต้องชำระเงินค้ำประกันหรือเงินที่แสดงถึงความสามารถในการผ่อนชำระ จากนั้นจะอ้างเหตุผลต่าง ๆ เช่น ข้อมูลผิด หรือการต้องแก้ไขสัญญา หรือเครดิตไม่เพียงพอ เพื่อหลอกให้ผู้เสียหายจ่ายเงินเพิ่มเติมในแต่ละขั้นตอน จนกระทั่งผู้เสียหายไม่ได้ทั้งเงินกู้และเงินที่โอนให้คนร้าย รวมถึงการให้กู้ยืมเงินที่ผิดกฎหมายผ่านระบบออนไลน์ โดยการหักดอกเบี้ยเกินอัตราที่กฎหมายกำหนด และมีการทวงหนี้ในลักษณะที่เข้าข่ายการกรรโชกหรือรีดเอาทรัพย์ เช่น การส่งข้อความสั้น (SMS) ให้ผู้เสียหายเข้าร่วมการกู้เงินโดยการหลอกให้โอนเงินค้ำประกันล่วงหน้า

๖) คดีหลอกลวงให้โอนเงินเพื่อทำงานหารายได้พิเศษ ได้แก่ คดีที่มีการประกาศหรือโฆษณาผ่านสื่อสังคมออนไลน์ หรือการส่งข้อความชักชวนให้ผู้เสียหายทำงานพิเศษหรือกิจกรรมต่าง ๆ ในระบบออนไลน์เพื่อสร้างรายได้หรือค่าตอบแทน แต่ผู้เสียหายจะต้องซื้อแพ็กเกจค้ำประกันการทำงานหรือชำระค่าใช้จ่ายอื่น ๆ ล่วงหน้า เมื่อผู้เสียหายได้ซื้อแพ็กเกจและทำกิจกรรมแล้ว ในระยะแรกอาจได้รับผลตอบแทนจริง แต่เมื่อจ่ายเงินเพิ่มเพื่อรับผลตอบแทนที่สูงขึ้นกลับไม่ได้รับค่าตอบแทนและไม่สามารถขอคืนเงินได้ เช่น การชักชวนให้ทำงานเพียงกดไลก์ (Like) หรือแชร์

(Share) หรือเพิ่มยอดผู้ชม (View) ในเว็บไซต์ขายสินค้า โดยต้องซื้อสินค้าและจ่ายเงินหลายครั้ง เพื่อเพิ่มผลตอบแทนที่คาดหวัง

๗) คดีข่มขู่ทางโทรศัพท์ให้เกิดความกลัวแล้วหลอกให้โอนเงิน (Call Center) ได้แก่ คดีที่มีการใช้สื่อสังคมออนไลน์ โทรศัพท์ หรือโทรผ่านระบบอินเทอร์เน็ต (VoIP) สุ่มติดต่อไปยังผู้เสียหาย โดยการสร้างเรื่องหลอกลวงอ้างตัวเป็นเจ้าหน้าที่รัฐ ข่มขู่ให้เกิดความกลัวเกี่ยวกับการกระทำผิดต่าง ๆ และให้ผู้เสียหายโอนเงินไปเพื่อช่วยเหลือหรือหลีกเลี่ยงการถูกดำเนินคดี เช่น การอ้างว่าเจ้าหน้าที่ตำรวจจับกุมผู้ค้ายาเสพติดได้แล้วให้การว่าผู้เสียหายเกี่ยวข้องกับการรับโอนเงินจากผู้ค้ายาเสพติดและขอตรวจสอบทางการเงินโดยการให้โอนเงินไปตรวจสอบ

๘) คดีที่กระทำต่อระบบหรือข้อมูลคอมพิวเตอร์โดยมิชอบ (Hacking) เพื่อให้ได้มาซึ่งทรัพย์สิน ได้แก่ คดีที่มีการเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ล่วงรู้รหัสผ่านบัญชีของผู้อื่นและนำข้อมูลเหล่านั้นไปเปิดเผย หรือการเข้าถึงข้อมูลคอมพิวเตอร์ การส่งสแปมเมล (Spam mail) การแก้ไข ดัดแปลง หรือก่อกวนระบบข้อมูลคอมพิวเตอร์ของผู้อื่น รวมถึงการเผยแพร่ชุดคำสั่งหรือข้อมูลคอมพิวเตอร์โดยมิชอบ ทำให้เกิดความเสียหาย อันมีลักษณะเป็นการฉ้อโกง กรรโชก หรือรีดเอาทรัพย์ หรือทำให้ผู้อื่นเสียหายทางทรัพย์สิน เช่น การเข้าถึงข้อมูลอีเมลของบริษัทแล้วส่งอีเมลหลอกลวงให้บุคคลอื่นโอนเงินไปยังบัญชีของคนร้าย

๙) คดีที่มีการเข้ารหัสข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบเพื่อกรรโชกหรือรีดเอาทรัพย์ (Ransomware) ได้แก่ คดีที่มีการส่งซอฟต์แวร์ที่เป็นอันตราย หรือมัลแวร์ (Malware) เข้ามาในเครื่องคอมพิวเตอร์ของผู้เสียหาย ซึ่งอาจส่งมาทางอีเมล ลิงก์ URL ผ่านสื่อสังคมออนไลน์ หรือการติดตั้งผ่านอุปกรณ์เก็บข้อมูลแบบพกพา (Flash Drive) ซอฟต์แวร์อันตรายดังกล่าวจะทำการคัดลอกข้อมูลจากเครื่องคอมพิวเตอร์ของผู้เสียหายและเข้ารหัสหรือปิดกั้นไฟล์ข้อมูลเอกสาร รูปภาพ หรือวิดีโอ ทำให้ผู้เสียหายไม่สามารถเข้าถึงข้อมูลเหล่านั้นได้ ยกเว้นต้องจ่ายค่าไถ่เพื่อรับคีย์ (Key) หรือซอฟต์แวร์ในการปลดล็อก

๑๐) คดีหลอกลวงให้ติดตั้งโปรแกรมควบคุมระบบในเครื่องโทรศัพท์เพื่อให้ได้มาซึ่งทรัพย์สิน ได้แก่ คดีที่คนร้ายสุ่มโทรศัพท์มาอ้างเป็นเจ้าหน้าที่รัฐ ข่มขู่ให้เกิดความกลัวเกี่ยวกับการกระทำผิดต่าง ๆ โดยหลอกว่าเป็นเจ้าหน้าที่รัฐที่จะช่วยเหลือด้านภาษี หรือการจดทะเบียนพาณิชย์ หรืออ้างเป็นเจ้าหน้าที่บริษัทเอกชนที่จะให้สิทธิประโยชน์ต่าง ๆ หรือสร้างข้อมูลเท็จในระบบคอมพิวเตอร์แล้วหลอกลวงให้ผู้เสียหายดาวน์โหลดลิงก์เพื่อให้ติดตั้งโปรแกรมควบคุมระบบในเครื่องโทรศัพท์จากทางไกล เพื่อติดตามการทำงานหรือเข้าดำเนินการในเครื่องโทรศัพท์ของผู้เสียหาย หรือเอาข้อมูลจากเครื่องของผู้เสียหายไปใช้โดยมิชอบ ซึ่งมีลักษณะเป็นการฉ้อโกง กรรโชก หรือรีดเอาทรัพย์ หรือทำให้บุคคลอื่นเสียหายทางทรัพย์สิน เช่น การหลอกลวงโดยอ้างเป็นเจ้าหน้าที่กรมสรรพากร ข่มขู่ผู้เสียหายให้ดาวน์โหลดแอปพลิเคชันปลอมเพื่อกรอกข้อมูลส่วนตัวและรหัสผ่าน จากนั้นทำการควบคุมเครื่องและถอนเงินจากบัญชีธนาคารของผู้เสียหาย

๑๑) คดีหลอกลวงเกี่ยวกับสินทรัพย์ดิจิทัล ได้แก่ คดีที่มีการหลอกลวงให้โอนสินทรัพย์ดิจิทัลในระบบเทคโนโลยีบล็อกเชน (Blockchain) ทั้งในและนอกศูนย์ซื้อขายสินทรัพย์ดิจิทัล โดยผู้เสียหายถูกหลอกให้ซื้อสินทรัพย์ดิจิทัลและเก็บไว้ในกระเป๋าเงินดิจิทัล (Crypto wallet) ของตนเอง แล้วโอนไปยังบัญชีของคนร้ายทั้งในและนอกศูนย์ซื้อขาย หรือในระบบ Peer to Peer ในตลาดอื่น ๆ เช่น การปลอมโปรไฟล์เป็นบุคคลที่มีความน่าเชื่อถือแล้วสุ่มส่งข้อความมาพูดคุยกับผู้เสียหายจนเกิดความเชื่อใจ หรือความรัก แล้วชักชวนให้ไปลงทุนในตลาดซื้อขายเหรียญสกุลเงินดิจิทัลในต่างประเทศ โดยหลอกให้ซื้อเหรียญสกุลเงินดิจิทัลจาก Bitkub และโอนไปลงทุนในเว็บเทรดที่คนร้ายสร้างขึ้นมา

๑๒) คดีหลอกลวงให้ลงทุนผ่านระบบคอมพิวเตอร์ ได้แก่ คดีที่มีการชักชวนให้ลงทุนในลักษณะธุรกิจเครือข่าย หรือชักชวนเป็นรายบุคคลผ่านสื่อสังคมออนไลน์ในรูปแบบต่าง ๆ โดยปลอมโปรไฟล์เป็นบุคคลที่มีความน่าเชื่อถือ สุ่มส่งข้อความมาพูดคุยกับผู้เสียหายจนเกิดความเชื่อใจหรือความรัก หรือจากบุคคลที่ลงทุนอยู่ก่อนแล้วที่ได้ชักชวนให้ผู้เสียหายลงทุนในรูปแบบต่าง ๆ ผ่านเว็บไซต์ แอปพลิเคชัน หรือแพลตฟอร์มอื่น โดยอ้างว่าจะได้รับผลตอบแทนในอัตราสูง แต่แท้จริงแล้วไม่มีธุรกิจหรือกิจการที่ให้ผลตอบแทนเช่นนั้นจริง และผู้เสียหายไม่ได้รับผลตอบแทนและเงินทุนคืน เช่น การหลอกลวงว่าเป็นเจ้าหน้าที่การตลาดของบริษัทให้ผู้เสียหายติดตั้งแอปพลิเคชันและโอนเงินไปลงทุน หรือการปลอมโปรไฟล์เป็นบุคคลที่มีอาชีพนักธุรกิจ ชักชวนพูดคุยทางออนไลน์จนเกิดความรักและชักชวนให้ลงทุนกับเว็บไซต์ปลอม

๑๓) คดีหลอกลวงซื้อขายสินค้าหรือบริการที่มีลักษณะเป็นขบวนการ ได้แก่ คดีที่เกี่ยวข้องกับการกระทำผิดในการหลอกขายสินค้าหรือบริการ โดยมีการเชื่อมโยงของคนร้ายในลักษณะขบวนการ หรือการมีผู้เสียหายจำนวนมากหลายพื้นที่ (ตั้งแต่ ๑๐ รายขึ้นไป)

๑๔) คดีหลอกลวงให้ลงทุนที่เป็นความผิดตามพระราชกำหนดการกู้ยืมเงินที่เป็นการฉ้อโกงประชาชน พ.ศ. ๒๕๒๗ ได้แก่ คดีที่กระทำผิดตามกฎหมายว่าด้วยการกู้ยืมเงินที่เป็นการฉ้อโกงประชาชน โดยการชักชวนให้ลงทุนในลักษณะธุรกิจเครือข่ายหรือชักชวนเป็นรายบุคคลด้วยการโฆษณาหรือประกาศให้ปรากฏแก่ประชาชนทั่วไป หรือแก่บุคคลตั้งแต่ ๑๐ คนขึ้นไป ให้เข้าร่วมลงทุน โดยอ้างว่าจะได้รับผลตอบแทนสูงกว่าดอกเบี้ยที่สถาบันการเงินจะจ่ายให้ได้ตามกฎหมาย โดยใช้ระบบคอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด เช่น การเปิดเพจเฟซบุ๊กชักชวนให้ลงทุนทำฟาร์มเห็ด โดยให้ผลตอบแทนสูงแล้วปิดเว็บไซต์หนีไป

๑๕) คดีอาชญากรรมทางเทคโนโลยีลักษณะอื่น ๆ นอกเหนือจากลำดับที่ ๑-๑๔ หมายถึง คดีที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยีตามความหมายของพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๖ ซึ่งไม่ได้กำหนดเป็นลักษณะคดีในข้อ ๑)-๑๔)

ภาพที่ ๑ สถิติความเสียหายจากอาชญากรรมทางเทคโนโลยี

ที่มา: กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี, สถิติความเสียหายสะสม ตั้งแต่วันที่ ๑ มกราคม ๒๕๖๘ ถึงวันที่ ๒๑ มีนาคม ๒๕๖๘, สืบค้นเมื่อวันที่ ๒๒ มีนาคม ๒๕๖๘. จาก https://www.thaipoliceonline.com/

๒.๓.๒ รูปแบบอาชญากรรมทางเทคโนโลยีที่พบมากในสังคมไทยปัจจุบัน[๑๒]

จากสถิติข้อมูลตามประเภทของคดีที่ได้รับการแจ้งจากศูนย์ AOC ๑๔๔๑ ซึ่งอยู่ภายใต้การดูแลของกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี พบว่าประเภทของคดีที่ได้รับการแจ้งมากที่สุดคือการหลอกลวงในการซื้อขายสินค้าหรือบริการ นอกจากนี้ ยังมีการหลอกลวงในลักษณะต่าง ๆ เช่น การหลอกเพื่อรับรางวัล หารายได้พิเศษ การหลอกลงทุน การหลอกกู้เงิน และการหลอกลวงในลักษณะของแก๊งคอลเซ็นเตอร์ ซึ่งการหลอกลวงผ่านโทรศัพท์ไม่ได้จำกัดเพียงแค่การโทรศัพท์เพื่อหลอกลวงเท่านั้น แต่ในปัจจุบันมีการใช้วิธีการหลอกลวงผ่านแชตสนทนาโดยไม่จำเป็นต้องมีการพูดคุยทางโทรศัพท์ การสื่อสารผ่านแอปพลิเคชันต่าง ๆ เช่น ไลน์ หรือแอปพลิเคชันสนทนาในประเทศนั้น ๆ ถูกใช้ในการหลอกลวงแทนการโทรศัพท์ นอกจากนี้ ยังมีการหลอกลวงให้ติดตั้งโปรแกรมควบคุมระบบผ่านลิงก์ต่าง ๆ ซึ่งหากผู้เสียหายคลิกลิงก์ที่ได้รับอาจทำให้ผู้กระทำความผิดสามารถเข้าถึงและควบคุมระบบของผู้เสียหายได้ และยังพบการหลอกลวง

---

[๑๒] เขมชาติ ประกายหงส์มณี, *อาชญากรรมออนไลน์*, สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘. จาก https://www.oscc.consulting/media/๒๗๒

ในลักษณะ Romance scam[๑๓] โดยผู้กระทำผิดปลอมตัวเป็นบุคคลต่างชาติที่มีลักษณะน่าสนใจ เช่น หนุ่มสาวหน้าตาดี เพื่อหลอกลวงผู้เสียหาย

ภาพที่ ๒ รูปแบบการหลอกลวง

ที่มา: เขมชาติ ประกายหงส์มณี, อาชญากรรมออนไลน์, สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘. จาก https://www.oscc.consulting/media/๒๗๒

๑) กลุ่มผู้กระทำความผิดในการหลอกลวงผ่านโทรศัพท์ (แก๊งคอลเซ็นเตอร์)

ปัจจุบันอาชญากรรมทางเทคโนโลยีได้กลายเป็นอาชญากรรมไร้พรมแดน โดยเริ่มต้นจากการกระทำผิดในประเทศไทย แต่ผู้กระทำผิดมักอาศัยอยู่ในประเทศเพื่อนบ้าน เช่น กัมพูชา พม่า ลาว ซึ่งเป็นปัจจัยที่ทำให้การบังคับใช้กฎหมายมีข้อจำกัด เนื่องจากระบบกฎหมายในแต่ละประเทศยังคงมีขอบเขตตามพรมแดนของตน จึงเป็นอุปสรรคในการดำเนินงานเกี่ยวกับอาชญากรรมทางเทคโนโลยีที่ข้ามประเทศ ซึ่งปัจจุบันสามารถเรียกได้ว่าเป็นอาชญากรรมข้ามชาติ โดยมีปัจจัยที่ส่งผลให้เกิดอาชญากรรมดังกล่าว ๓ ประการ ดังนี้

(๑) ผู้กระทำความผิด ในปัจจุบันกลุ่มผู้กระทำผิดมีการพัฒนาและปรับตัวอย่างต่อเนื่อง กรณีการเข้าร่วมกลุ่มในสื่อสังคมออนไลน์ เช่น เฟซบุ๊ก เป็นการแลกเปลี่ยนความรู้กันใน

---

[๑๓] การหลอกให้หลงรัก หลอกให้เชื่อว่ารัก หลอกให้เชื่อใจ ให้ความหวังว่าจะแต่งงาน ใช้ชีวิตอยู่ด้วยกันตลอดไป และใช้ความรักความเชื่อใจหรือความหวังของเหยื่อเพื่อแสวงหาประโยชน์ โดยหลอกให้โอนเงินหรือทรัพย์สินอื่น ๆ ไปให้ หรือหลอกให้กระทำผิดบางอย่าง โปรดดู กรมประชาสัมพันธ์, *Romance Scam คืออะไร รู้จักไว้ก่อนตกเป็นเหยื่อ*, สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘. จาก https://www.prd.go.th/th/content/category/detail/id/๓๑/iid/๒๖๖๒๘๙

กลุ่มที่ผู้ใช้ไม่รู้จักกันมาก่อน กลุ่มเหล่านี้ทำหน้าที่เสมือน "Academy Online" ของผู้กระทำผิด โดยจะมีการอัพเดทข้อมูลเกี่ยวกับวิธีการหลีกเลี่ยงการจับกุมจากเจ้าหน้าที่ตำรวจหรือหน่วยงานที่เกี่ยวข้องและการแลกเปลี่ยนเทคโนโลยีใหม่ ๆ รวมถึงการติดตามความเคลื่อนไหวของเจ้าหน้าที่

(๒) เป้าหมาย ความสามารถในการปกป้องตัวเองของผู้คนมีความแตกต่างกัน การปลูกฝังการป้องกันภัยทางไซเบอร์ในโรงเรียนและชุมชนจึงมีบทบาทสำคัญในการเสริมสร้าง "วัคซีนไซเบอร์" ให้แก่เด็กและประชาชน โดยเฉพาะในกลุ่มเด็กและเยาวชนที่มักใช้แพลตฟอร์ม เช่น TikTok ส่วนกลุ่มผู้สูงอายุมีแนวโน้มที่จะตกเป็นเหยื่อของการหลอกลวงผ่านแอปพลิเคชันไลน์ ดังนั้น การประชาสัมพันธ์ควรใช้แพลตฟอร์มที่ตรงกับกลุ่มเป้าหมายเพื่อเพิ่มประสิทธิภาพในการป้องกัน

(๓) สถานการณ์โรคระบาดโควิด ๑๙ การแพร่ระบาดของไวรัสโคโรนา ๒๐๑๙ ได้เป็นตัวเร่งปฏิกิริยาที่ทำให้เกิดอาชญากรรมทางเทคโนโลยีใหม่ ๆ ในช่วงที่มีการเรียนออนไลน์ผ่านโปรแกรมต่าง ๆ เช่น Zoom ซึ่งทำให้ผู้กระทำผิดสามารถเข้าถึงผู้เสียหายโดยตรง โดยไม่จำเป็นต้องผ่านคนกลางเหมือนในอดีต ทำให้การเข้าถึงกลุ่มเป้าหมายเป็นเรื่องง่ายขึ้น

นอกจากนี้ แก๊งคอลเซ็นเตอร์มีการทำงานในลักษณะเป็นทีม โดยมีการแบ่งหน้าที่ที่ชัดเจน มีทักษะในการโทรและฝึกท่องบทสนทนา เพื่อหลอกลวงเหยื่อได้อย่างมีประสิทธิภาพ โดยได้รับผลตอบแทนเป็นสัดส่วนของรายได้จากยอดที่สามารถหลอกลวงเหยื่อได้ ส่วนกลุ่มที่สองจะรับผิดชอบในการถอนเงินที่ได้จากการหลอกลวง ซึ่งในปัจจุบันพบว่าผู้กระทำผิดได้เปลี่ยนรูปแบบการใช้เงินจากเงินสดมาเป็นเงินดิจิทัลที่ไม่ได้มีการจดทะเบียน ทำให้ไม่สามารถควบคุมได้และมีการไหลออกไปยังบัญชีที่ไม่สามารถตรวจสอบได้

ในส่วนของภาครัฐโดยกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (ตำรวจไซเบอร์) ได้ดำเนินโครงการ Senior’s Community Cyber Police Club เพื่อเสริมสร้างการป้องกันอาชญากรรมไซเบอร์และให้ข้อมูลเกี่ยวกับการแจ้งความออนไลน์ รวมถึงการอายัดบัญชีธนาคารได้ด้วยตนเอง ผ่านเว็บไซต์ที่มีหมายเลขโทรศัพท์ของธนาคารทุกแห่งในประเทศไทย พร้อมทั้งการจัดตั้งศูนย์ปฏิบัติการแก้ไขปัญหาอาชญากรรมออนไลน์ (Anti Online Scam Operation Center: AOC) หรือ AOC ๑๔๔๑ เพื่อให้บริการแก่ประชาชนในการแจ้งเบาะแสภัยออนไลน์ต่าง ๆ เช่น บัญชีธนาคารต้องสงสัย เบอร์โทรศัพท์ที่น่าสงสัย เว็บหรือลิงก์ปลอม รวมถึงข้อความหลอกลวง (SMS) ต่าง ๆ

๒) การข่มขู่คุกคามทางเพศ (Sextortion)

การข่มขู่คุกคามทางเพศผ่านช่องทางออนไลน์เป็นปัญหาที่เกิดขึ้นอย่างแพร่หลายในปัจจุบัน โดยมักเริ่มต้นจากผู้กระทำความผิดที่เข้ามาติดต่อเหยื่อผ่านช่องทางต่าง ๆ และเสนอโอกาสในการเป็นนักแสดง โดยขอให้เหยื่อส่งภาพถ่ายมา ก่อนที่ผู้กระทำความผิดจะข่มขู่ให้เหยื่อถอดเสื้อผ้าและถ่ายภาพในลักษณะที่ไม่เหมาะสมทางเพศ หลังจากนั้นผู้กระทำความผิดจะใช้ภาพเหล่านี้ข่มขู่เหยื่อให้ส่งทรัพย์สินหรือเงินทอง โดยส่วนใหญ่มักจะหลอกกลุ่มวัยรุ่นที่มีความต้องการเข้าวงการบันเทิง โดยการใช้ช่องทางที่เปิดเป็นสาธารณะในแพลตฟอร์มออนไลน์ ซึ่งทำให้ผู้กระทำความผิดสามารถเข้าถึงและติดต่อเหยื่อได้ง่ายขึ้น หนึ่งในมาตรการป้องกันเบื้องต้น คือ

การตั้งค่าความเป็นส่วนตัวในโปรไฟล์ออนไลน์ให้เห็นเฉพาะเพื่อนหรือผู้ที่รู้จัก ซึ่งแม้ไม่สามารถปิดกั้นได้ทั้งหมด ลดความเสี่ยงได้ในระดับหนึ่ง ซึ่งไม่ควรเปิดเป็นสาธารณะให้ทุกคนสามารถเข้าถึงข้อมูลได้ นอกจากนี้ ผู้กระทำความผิดยังสามารถเลือกเหยื่อที่เป็นเด็ก ซึ่งบางครั้งผู้ปกครองอาจตกเป็นเหยื่อในการหลอกลวงด้วย โดยผู้กระทำความผิดมักจะหลอกให้พ่อแม่ส่งภาพลามกของเด็ก โดยเฉพาะในกรณีที่พ่อแม่อาศัยอยู่ในต่างจังหวัดและไม่เข้าใจภาษาต่างประเทศ เช่น ภาษาสเปนหรือโปรตุเกส ซึ่งอาจถูกหลอกให้ใช้คำพูดที่มีเนื้อหาชักชวนทางเพศโดยไม่รู้ตัว สถานการณ์ปัจจุบันทำให้เห็นว่าภาษาไม่เป็นอุปสรรคสำหรับผู้กระทำความผิดอีกต่อไป เนื่องจากเทคโนโลยีแปลภาษาและปัญญาประดิษฐ์ (AI) สามารถแปลและเข้าใจได้ทันที ทำให้ผู้กระทำความผิดสามารถหลอกลวงเหยื่อได้ง่ายขึ้น โดยเริ่มต้นจากการสร้างความสัมพันธ์ในลักษณะโรแมนติกและค่อย ๆ ใช้การขู่กรรโชกจนทำให้เหยื่อต้องถ่ายภาพหรือส่งข้อมูลส่วนตัวที่ไม่เหมาะสมผ่านกล้อง ทั้งนี้ การข่มขู่คุกคามทางเพศในลักษณะนี้ไม่จำกัดเฉพาะกลุ่มวัยรุ่นเท่านั้น ส่วนใหญ่พบมากในกลุ่มผู้ใหญ่ที่อยู่ในวัยทำงาน ซึ่งผู้กระทำความผิดอาจใช้ภาพของเหยื่อจากคดีอื่น ๆ เพื่อหลอกลวงเหยื่อที่เป็นเป้าหมายให้หลงเชื่อว่าเป็นบุคคลที่กำลังพูดคุยด้วยอยู่ สำหรับการดำเนินการทางกฎหมายในกรณีนี้ มักจะเกี่ยวข้องกับผู้ที่เปิดบัญชีม้าและรับโอนเงินจากเหยื่อ นอกจากการฟ้องคดีอาญาแล้ว ยังสามารถดำเนินคดีเรียกค่าเสียหายทางแพ่งได้ โดยผู้ที่ปรากฏในภาพหรือคลิปสามารถเรียกค่าเสียหายได้ แม้ว่าจำเลยจะรับสารภาพแล้ว แต่ศาลจะรอการพิจารณาคดีในเรื่องค่าเสียหายเพิ่มเติม สิ่งที่เผยแพร่ในโลกไซเบอร์สามารถขยายไปได้อย่างรวดเร็วและก่อให้เกิดความเสียหายมากกว่าที่ควรจะเป็น โดยในประเทศไทยยังไม่มีสิทธิในการลบข้อมูลจากอินเทอร์เน็ต (Right to be Forgotten)[๑๔] เช่นเดียวกับในบางประเทศที่สามารถระงับการเผยแพร่ข้อมูลได้ โดยศาลสามารถสั่งห้ามการเผยแพร่ต่อไปได้ ตามที่กำหนดในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มาตรา ๒๔ และมาตรา ๓๓

การขู่กรรโชกทางเพศ (Sextortion) เป็นหนึ่งในอาชญากรรมออนไลน์ที่มีการเกิดขึ้นอย่างแพร่หลาย โดยเฉพาะอย่างยิ่งในกรณีที่เด็กเป็นเหยื่อ เนื่องจากเป็นกลุ่มที่มีความเสี่ยงสูงต่อการถูกแสวงหาประโยชน์ทางเพศผ่านช่องทางออนไลน์ โดยผู้กระทำความผิดจะขู่ว่าจะแพร่เผยภาพหรือวิดีโอที่เกี่ยวข้องกับกิจกรรมทางเพศของเหยื่อ หากเหยื่อไม่ทำตามคำขอที่พวกเขาเรียกร้อง ซึ่งอาจรวมถึงการขอรูปภาพลามกอนาจาร เงิน หรือคำขออื่น ๆ การขู่กรรโชกทางเพศจึงถือเป็นอาชญากรรมที่มีความร้ายแรงและสามารถส่งผลกระทบอย่างมากต่อเหยื่อ การให้ความรู้เกี่ยวกับความเสี่ยงในการแบ่งปันข้อมูลส่วนบุคคลออนไลน์ รวมถึงการระมัดระวังในการสนทนาและสร้างความสัมพันธ์กับบุคคลแปลกหน้าผ่านสื่อสังคมออนไลน์จึงเป็นสิ่งที่สำคัญยิ่งในกรณีที่ตกเป็นเหยื่อการขู่กรรโชกทางเพศ โดยควรดำเนินการตามขั้นตอน ดังนี้

๑) เก็บหลักฐานการโพสต์หรือการแชร์ ผู้เสียหายควรรวบรวมหลักฐานการกระทำความผิดที่เกี่ยวข้อง เช่น เก็บหลักฐานที่แสดงให้เห็นว่าใครเป็นผู้โพสต์หรือเผยแพร่ข้อมูล

---

[๑๔] สิทธิที่จะถูกลืม (Right to be forgotten) หมายถึง สิทธิของปัจเจกบุคคลที่จะขอร้องให้อีกฝ่าย ซึ่งเป็นปัจเจกบุคคลหรือองค์กร ที่มีข้อมูลส่วนบุคคลของเขาไว้ในครอบครอง ทำการลบข้อมูลส่วนบุคคลของเขาออก เนื่องจากไม่ยินยอมให้มีการใช้ข้อมูลของเขาอีกต่อไป เป็นสิทธิที่เกี่ยวข้องกับความเป็นส่วนตัว เกี่ยวข้องกับศักดิ์ศรีความเป็นมนุษย์ที่ครอบคลุมตัวคนมากกว่าคุ้มครององค์กรหรือนิติบุคคล

เหล่านั้นให้ปรากฏชัดเจน และในกรณีที่มีผู้แชร์ข้อมูลดังกล่าว ควรเก็บหลักฐานไว้ด้วย เนื่องจากทั้งผู้โพสต์และผู้แชร์ข้อมูลล้วนมีความผิดตามกฎหมาย

๒) เก็บหลักฐานการข่มขู่ หากมีการข่มขู่หรือแบล็คเมล์จากผู้กระทำความผิดผ่านทางโทรศัพท์ ควรบันทึกเสียงไว้ในขณะที่มีการข่มขู่ เพื่อใช้เป็นหลักฐานในการดำเนินคดี

๓) แจ้งความต่อสถานีตำรวจในท้องที่ที่เกิดเหตุ เมื่อรวบรวมหลักฐานได้ครบถ้วนแล้ว ผู้เสียหายสามารถแจ้งความได้ที่สถานีตำรวจในพื้นที่ที่เกิดเหตุ เนื่องจากสถานีตำรวจมีหน้าที่ในการรับแจ้งความในกรณีดังกล่าว หรือสามารถร้องทุกข์ไปยังกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) ในกรณีที่ผู้เสียหายต้องการความช่วยเหลือในระดับสูงขึ้น สามารถแจ้งความที่กรมสอบสวนคดีพิเศษ (DSI) กองคดีเทคโนโลยีได้ โดย DSI จะมีข้อจำกัดในกระบวนการเริ่มต้นคดี เนื่องจากต้องขออนุมัติจากอธิบดีเพื่อให้ดำเนินการสืบสวนสอบสวนต่อไป อย่างไรก็ตาม หากผู้เสียหายต้องการความช่วยเหลือเร่งด่วน สามารถดำเนินการแจ้งความต่อ บก.ปอท. และ DSI ควบคู่กันไปได้ ซึ่งหาก DSI รับคดีเป็นคดีพิเศษ และสามารถนำสำนวนที่ได้รับจากตำรวจมารวมกับสำนวนของ DSI เพื่อดำเนินการตามกฎหมายต่อไป

๓) การหลอกลวงในลักษณะ SCAM

การหลอกลวงในรูปแบบ SCAM มักเริ่มต้นด้วยการสร้างความไว้วางใจในลักษณะเพื่อนหรือแฟน จนทำให้เหยื่อเกิดความเชื่อมั่นและพร้อมที่จะลงทุนในสกุลเงินดิจิทัล เช่น Bitcoin หรือ Bitcoin Cash ผ่านแอปพลิเคชันที่มาจากประเทศจีน โดยเหยื่ออาจเป็นทั้งชายและหญิง หรืออาจเริ่มต้นด้วยการสร้างความไว้วางใจในลักษณะของความสัมพันธ์เชิงรักใคร่ แล้วตามด้วยการหลอกลวงให้โอนเงินเพื่อค่าธรรมเนียมในการส่งของ หรือหลอกลวงเอาเงินของเหยื่อในลักษณะดังกล่าว ผู้เสียหายจากการหลอกลวงในลักษณะนี้ส่วนใหญ่จะเป็นผู้หญิงในกลุ่มพ่อหม้ายและแม่หม้ายสูงอายุ แต่ปัจจุบันเหยื่อไม่จำกัดเฉพาะกลุ่มนี้เท่านั้น แต่ยังรวมถึงกลุ่มผู้ที่มีรสนิยมเฉพาะ เช่น ผู้ที่มีความชื่นชอบในสาวจีน โดยคนร้ายจะใช้วิธีการสร้างโปรไฟล์ปลอม และนำภาพของบุคคลอื่นมาแอบอ้างเพื่อหลอกลวง เลือกโปรไฟล์ที่ดูดีและมีหน้าตาดึงดูดใจ เพื่อสร้างความน่าเชื่อถือ ซึ่งโปรไฟล์เหล่านี้มักจะมีอายุบัญชีเฟซบุ๊กที่ไม่นานนัก วิธีการหลอกลวงจะเริ่มจากการทักทายผ่านเฟซบุ๊กแล้วพาเหยื่อเข้าสู่ห้องสนทนา หรือหลอกให้โหลดแอปพลิเคชันที่เป็นอันตราย ซึ่งถูกสร้างขึ้นโดยคนร้ายเพื่อหลอกลวงเหยื่อ โดยบางครั้งหากคนร้ายไม่สามารถใช้ภาษาไทยได้ ก็อาจใช้ Google Translate เพื่อสร้างความน่าเชื่อถือในการสนทนา โดยการหลอกลวงเหล่านี้อาจรวมถึงการขอเลขบัญชีเพื่อทำการโอนเงิน ซึ่งสุดท้ายจะนำไปสู่การโอนเงินเข้าบัญชีม้า ข้อสังเกตสำคัญ คือ ชื่อบริษัทที่ปรากฏมักไม่ตรงกับข้อมูลที่จริง และคนร้ายมักจะพยายามหลีกเลี่ยงการใช้บัญชีบุคคลในการรับโอนเงินจำนวนมากโดยการใช้บัญชีของบริษัทแทน เนื่องจากการโอนผ่านบัญชีบริษัทไม่จำเป็นต้องสแกนใบหน้า แต่การใช้บัญชีบุคคลจำเป็นต้องมีการยืนยันตัวตนผ่านการสแกนใบหน้า ในกรณีที่เกิดความสงสัยเกี่ยวกับความน่าเชื่อถือของบริษัทหรือบัญชีธนาคาร ควรตรวจสอบว่าเว็บไซต์หรือหน้าเพจที่เกี่ยวข้องมีความน่าเชื่อถือหรือไม่ และควรตรวจสอบว่าเป็นบัญชีที่เคยมีการหลอกลวงมาก่อนหรือไม่

๔) การหลอกลวงขอแต่งงาน

การหลอกลวงในลักษณะการขอแต่งงานมักเริ่มต้นจากการหลอกลวงให้เหยื่อเชื่อว่าจะมีการส่งของมาให้ โดยการส่งอีเมลหรือข้อความเพื่อให้เหยื่อเชื่อว่ามีเงินจำนวนหนึ่งเตรียมไว้เพื่อเป็นสินสอด การหลอกลวงในลักษณะนี้มีต้นกำเนิดจากกลุ่มอาชญากรในภูมิภาคแอฟริกา เช่น ประเทศไนจีเรีย ไลบีเรีย กานา โดยเริ่มต้นจากการหลอกลวงขายน้ำยาปลอม ซึ่งสามารถเปลี่ยนกระดาษเปล่าให้กลายเป็นธนบัตรดอลลาร์สหรัฐฯ ในภายหลัง เมื่อการหลอกลวงขายน้ำยาปลอมไม่ประสบความสำเร็จ อาชญากรจึงได้พัฒนารูปแบบการหลอกลวงในลักษณะของ Romance Scam โดยจะมีการขอให้เหยื่อโอนเงิน โดยอ้างว่าเป็นการจ่ายเงินสินสอด หรือค่าใช้จ่ายที่เกี่ยวข้องกับการแต่งงาน โดยมักจะใช้เอกสารปลอมที่อ้างถึงการจองตั๋วหรือเอกสารทางการเงินต่าง ๆ เพื่อสร้างความน่าเชื่อถือ

อย่างไรก็ตาม การตระหนักรู้และการป้องกันอาชญากรรมทางเทคโนโลยี การรับรู้ถึงความสำคัญของอาชญากรรมทางเทคโนโลยีและการเตรียมความพร้อมในการรับมือกับการโจมตีทางเทคโนโลยีเป็นสิ่งสำคัญ ซึ่งทุกภาคส่วนควรมีการเตรียมความพร้อมในด้านต่าง ๆ ดังนี้

(๑) การสร้างความรู้ความเข้าใจ (People) การให้ความรู้แก่ประชาชนเกี่ยวกับภัยคุกคามทางเทคโนโลยี

(๒) การมีระบบป้องกันที่มีความปลอดภัย (Process) การพัฒนาและนำระบบการป้องกันที่มีประสิทธิภาพมาใช้

(๓) การอัพเดตเทคโนโลยี (Technology) การอัพเดตและพัฒนาเทคโนโลยีเพื่อเสริมความปลอดภัยอยู่เสมอ

บทที่ ๓
แนวคิดกฎหมายและนโยบายในการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยี

ปัจจุบันทุกประเทศทั่วโลกก้าวเข้าสู่ยุคสังคมดิจิทัล ซึ่งความก้าวหน้าของเทคโนโลยีสารสนเทศมีบทบาทสำคัญอย่างยิ่งต่อวิถีชีวิตและโครงสร้างของสังคมมนุษย์ การพัฒนาด้านเทคโนโลยีดิจิทัลที่ก้าวกระโดด ส่งผลให้เกิดการก่ออาชญากรรมทางคอมพิวเตอร์หรืออาชญากรรมทางเทคโนโลยี (Cybercrime) ซึ่งมีรูปแบบการกระทำผิดที่หลากหลายและซับซ้อนยิ่งขึ้น ในการรับมือกับภัยคุกคามทางไซเบอร์และการป้องกันอาชญากรรมทางคอมพิวเตอร์ในประเทศไทย มีการบังคับใช้กฎหมายที่เกี่ยวข้องหลายฉบับ เพื่อให้มีมาตรการที่มีประสิทธิภาพในการป้องกันและลดความเสี่ยงจากปัญหาดังกล่าว ทั้งในระดับภายในประเทศและภายนอกประเทศ ซึ่งอาจมีผลกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ และความมั่นคงทางทหาร รวมถึงความสงบเรียบร้อยภายในประเทศ

ภัยคุกคามทางไซเบอร์และอาชญากรรมทางเทคโนโลยีมีการวิวัฒนาการในรูปแบบที่หลากหลายและมีผลกระทบอย่างรวดเร็วในวงกว้าง โดยไม่จำเป็นต้องใช้ผู้กระทำเป็นจำนวนมาก รวมถึงปัจจุบันการกระทำผิดทางไซเบอร์ได้พัฒนารูปแบบและเทคนิคที่ซับซ้อนยิ่งขึ้น ภายใต้การพัฒนาเทคโนโลยีที่มีความก้าวหน้ามากขึ้นในทุกปี นอกจากนี้ ระบบกฎหมายในการควบคุมปัญหาอาชญากรรมทางเทคโนโลยีในประเทศไทยยังคงมีการปรับปรุงและบังคับใช้อย่างต่อเนื่อง โดยมีการศึกษาและวิเคราะห์รูปแบบการกระทำผิดทางเทคโนโลยีในประเทศ เพื่อนำไปสู่การพัฒนามาตรการการป้องกันและการรับมือที่มีประสิทธิภาพในอนาคต

๓.๑ กฎหมายหลักที่เกี่ยวข้องกับการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยี

๓.๑.๑ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และกฎหมายเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์[๑๕]

กฎหมายธุรกรรมทางอิเล็กทรอนิกส์เป็นกฎหมายกลางที่รองรับสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ให้มีผลผูกพันและใช้บังคับได้ตามกฎหมาย โดยที่การทำธุรกรรมในปัจจุบันมีแนวโน้มที่จะปรับเปลี่ยนวิธีการในการติดต่อสื่อสารที่อาศัยการพัฒนาการเทคโนโลยีทางอิเล็กทรอนิกส์ซึ่งมีความสะดวก รวดเร็ว และมีประสิทธิภาพ แต่เนื่องจากการทำธุรกรรมทางอิเล็กทรอนิกส์ดังกล่าวมีความแตกต่างจากวิธีการทำธุรกรรมซึ่งมีกฎหมายรองรับอยู่ในปัจจุบันเป็นอย่างมาก อันส่งผลให้ต้องมีการรองรับสถานะทางกฎหมายของข้อมูลทางอิเล็กทรอนิกส์ให้เสมอกับการทำเป็นหนังสือหรือหลักฐานเป็นหนังสือ การรับรองวิธีการส่งและรับข้อมูลอิเล็กทรอนิกส์ การใช้ลายมือชื่ออิเล็กทรอนิกส์ ตลอดจนการรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ เพื่อเป็นการส่งเสริมการทำธุรกรรมทางอิเล็กทรอนิกส์ให้น่าเชื่อถือ และมีผลในทางกฎหมายเช่นเดียวกับการทำธุรกรรมโดยวิธีการทั่วไปที่เคยปฏิบัติอยู่เดิม ควรกำหนดให้มีคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

---

[๑๕] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA), *พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ (ฉบับอัพเดท)*, สืบค้นเมื่อวันที่ ๑ มีนาคม ๒๕๖๘. จาก https://www.etda.or.th/th/Useful-Resource/กฎหมาย-HTML/

ทำหน้าที่วางนโยบายกำหนดหลักเกณฑ์เพื่อส่งเสริมการทำธุรกรรมทางอิเล็กทรอนิกส์ ติดตามดูแลการประกอบธุรกิจเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ รวมทั้งมีหน้าที่ในการส่งเสริมการพัฒนาการทางเทคโนโลยีเพื่อติดตามความก้าวหน้าของเทคโนโลยี ซึ่งมีการเปลี่ยนแปลงและพัฒนาศักยภาพตลอดเวลาให้มีมาตรฐานน่าเชื่อถือ ตลอดจนเสนอแนะแนวทางแก้ไขปัญหาและอุปสรรคที่เกี่ยวข้อง อันจะเป็นการส่งเสริมการใช้ธุรกรรมทางอิเล็กทรอนิกส์ทั้งภายในประเทศและระหว่างประเทศด้วยการมีกฎหมายรองรับในลักษณะที่เป็นเอกรูป และสอดคล้องกับมาตรฐานที่นานาประเทศยอมรับ

กฎหมายฉบับดังกล่าวใช้บังคับแก่ธุรกรรมในทางแพ่งและพาณิชย์ที่ดำเนินการโดยใช้ข้อมูลอิเล็กทรอนิกส์ เว้นแต่ธุรกรรมที่มีพระราชกฤษฎีกากำหนดมิให้นำพระราชบัญญัตินี้ทั้งหมดหรือแต่บางส่วนมาใช้บังคับ รวมถึงให้ใช้บังคับแก่การทำธุรกรรมทางอิเล็กทรอนิกส์ของภาครัฐด้วย เช่น คำขอ การอนุญาต การจดทะเบียน คำสั่งทางปกครอง การชำระเงิน การประกาศ หรือการดำเนินการใด ๆ ตามกฎหมายกับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ ถ้าได้กระทำในรูปของข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์และวิธีการที่กำหนดโดยพระราชกฤษฎีกา ให้ถือว่ามีผลโดยชอบด้วยกฎหมายเช่นเดียวกับการดำเนินการตามหลักเกณฑ์และวิธีการที่กฎหมายในเรื่องนั้นกำหนด

๓.๑.๒ พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐[๑๖] และพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐[๑๗]

พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เป็นกฎหมายฉบับแรกที่ตราขึ้นมาเพื่อป้องกัน ควบคุมการกระทำผิดที่จะเกิดขึ้นได้จากการใช้คอมพิวเตอร์ ทั้งที่เป็นคอมพิวเตอร์ตั้งโต๊ะ โน้ตบุ๊ค สมาร์ตโฟน รวมถึงระบบต่าง ๆ ที่ถูกควบคุมด้วยระบบคอมพิวเตอร์ แต่ที่ผ่านมา พบว่ากฎหมายมีปัญหาในการตีความ จนกระทบกับการบังคับใช้ เช่น นำฐานความผิดที่ใช้กับเรื่องฉ้อโกงปลอมแปลงทางออนไลน์ไปใช้กับการหมิ่นประมาท ทำให้กระทบต่อสิทธิเสรีภาพในการแสดงความคิดเห็น จนทำให้เกิดการโจมตีและเกิดกระแสสังคมเรียกร้องหลักประกันสิทธิเสรีภาพในการแสดงความคิดเห็นขึ้น ประกอบกับบทบัญญัติบางประการที่ไม่เหมาะสมต่อการป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในปัจจุบัน ซึ่งมีรูปแบบการกระทำความผิดที่มีความซับซ้อนมากขึ้น เช่น เพิ่มเติมฐานความผิดและกำหนดโทษผู้ส่งข้อมูลคอมพิวเตอร์ หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่น รวมทั้งการเฝ้าระวังและติดตามสถานการณ์ด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศของประเทศ จึงได้มีตรากฎหมายแก้ไขเพิ่มเติมพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ เพื่อปรับปรุงบทบัญญัติในส่วนที่เกี่ยวกับผู้รักษากฎหมาย และเป็นการปรับปรุงกฎหมายให้เท่าทันกับเทคโนโลยีและภัยคุกคามที่เปลี่ยนแปลงไป

---

[๑๖] กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (MDES), *พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐*, สืบค้นเมื่อวันที่ ๑ มีนาคม ๒๕๖๘, จาก https://www.mdes.go.th/law/detail/๓๕๑๖

[๑๗] ราชกิจจานุเบกษา, *พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐*, สืบค้นเมื่อวันที่ ๑ มีนาคม ๒๕๖๘, จาก https://www.ratchakitcha.soc.go.th/DATA/PDF/๒๕๖๐/A/๐๑๐/๒๔.PDF

สาระสำคัญที่ควรพึงระวังในพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ มีดังนี้

๑) การฝากร้านหรือโปรโมตสินค้าใน Facebook และ Instagram ถือเป็นการกระทำที่จัดอยู่ในประเภทสแปม ซึ่งมีโทษปรับไม่เกิน ๒๐๐,๐๐๐ บาท

๒) การส่งข้อความโฆษณาผ่านทาง SMS โดยไม่รับความยินยอมจากผู้รับ และไม่สามารถปฏิเสธข้อมูลดังกล่าวได้ ถือเป็นการกระทำที่จัดอยู่ในประเภทสแปม ซึ่งมีโทษปรับไม่เกิน ๒๐๐,๐๐๐ บาท

๓) การส่งอีเมล (Email) เพื่อขายสินค้าหรือบริการโดยไม่ได้รับความยินยอมจากผู้รับ ถือเป็นการกระทำที่จัดอยู่ในประเภทสแปม ซึ่งมีโทษปรับไม่เกิน ๒๐๐,๐๐๐ บาท

๔) การกดไลค์ (Like) บนสื่อออนไลน์ไม่ถือเป็นความผิดตามกฎหมายคอมพิวเตอร์ ยกเว้นในกรณีที่การกดไลค์มีความเกี่ยวข้องกับสถาบัน ซึ่งอาจเข้าข่ายความผิดตามมาตรา ๑๑๒ หรือเป็นความผิดร่วม

๕) การกดแชร์ (Share) ถือเป็นการเผยแพร่ข้อมูล หากข้อมูลที่แชร์มีผลกระทบต่อผู้อื่น อาจเข้าข่ายความผิดตามกฎหมายคอมพิวเตอร์ โดยเฉพาะในกรณีที่กระทบต่อบุคคลที่สาม

๖) หากพบข้อมูลที่ผิดกฎหมายอยู่ในระบบคอมพิวเตอร์ แต่ไม่ใช่สิ่งที่เจ้าของคอมพิวเตอร์กระทำเอง สามารถแจ้งไปยังหน่วยงานที่รับผิดชอบได้ หากมีการแจ้งและดำเนินการลบข้อมูลออกจากระบบ เจ้าของคอมพิวเตอร์จะไม่ถือว่ามีความผิดตามกฎหมาย เช่น การแสดงความคิดเห็นในเว็บไซต์ต่าง ๆ รวมถึงเฟซบุ๊ก หากพบว่าเป็นการแสดงความเห็นที่ผิดกฎหมาย สามารถแจ้งไปยังหน่วยงานที่รับผิดชอบเพื่อให้ทำการลบข้อมูลได้ทันที โดยเจ้าของระบบเว็บไซต์จะไม่ถือว่ามีความผิดทางกฎหมาย

๗) สำหรับผู้ดูแลเพจที่เปิดให้มีการแสดงความเห็น หากพบข้อความที่ผิดกฎหมายและได้ทำการลบออกจากพื้นที่ที่ดูแลแล้ว จะถือว่าเป็นผู้พ้นผิดจากการกระทำดังกล่าว

๘) ห้ามโพสต์สิ่งที่มีลักษณะลามกอนาจาร หรือเนื้อหาที่ทำให้เกิดการเผยแพร่แก่ประชาชน

๙) การโพสต์เกี่ยวกับเด็กและเยาวชนจะต้องปิดบังใบหน้า ยกเว้นในกรณีที่เป็นการเชิดชู ชื่นชม หรือให้เกียรติ

๑๐) การให้ข้อมูลเกี่ยวกับผู้เสียชีวิตจะต้องไม่ทำให้เกิดความเสื่อมเสียชื่อเสียงหรือถูกดูหมิ่นหรือเกลียดชัง โดยญาติสามารถฟ้องร้องได้ตามกฎหมาย

๑๑) การโพสต์การด่าว่าผู้อื่นโดยไม่มีข้อมูลที่เป็นจริงหรือมีการตัดต่อข้อมูลนั้นมีบทลงโทษตามกฎหมายอาญา ผู้ถูกกล่าวหาสามารถดำเนินคดีกับผู้โพสต์ได้ โดยมีโทษจำคุกไม่เกิน ๓ ปี หรือปรับไม่เกิน ๒๐๐,๐๐๐ บาท

๑๒) ห้ามกระทำการละเมิดลิขสิทธิ์ของผู้อื่น ไม่ว่าจะเป็นข้อความ เพลง รูปภาพ หรือวิดีโอ

๑๓) การส่งรูปภาพหรือข้อความที่แชร์ของผู้อื่น เช่น การส่งคำทักทายหรืออวยพรไม่ถือเป็นความผิด หากไม่ได้ใช้ภาพหรือข้อความดังกล่าวในเชิงพาณิชย์เพื่อหารายได้

๓.๑.๓ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒[๑๘]

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ย่อมาจาก PDPA (Personal Data Protection Act) เป็นกฎหมายว่าด้วยการให้สิทธิ์กับเจ้าของข้อมูลส่วนบุคคล สร้างมาตรฐานการรักษาข้อมูลส่วนบุคคลให้ปลอดภัย และนำไปใช้ให้ถูกวัตถุประสงค์ตามคำยินยอมที่เจ้าของข้อมูลส่วนบุคคลอนุญาต กฎหมาย PDPA ที่บังคับใช้ในประเทศไทยฉบับนี้ จะมีบทบาทในการคุ้มครองและให้สิทธิที่ประชาชนควรมีต่อข้อมูลส่วนบุคคลของตนเองได้ รวมไปถึงการสร้างมาตรฐานของบุคคลหรือนิติบุคคลในการเก็บ รวบรวม หรือเพื่อการเปิดเผยข้อมูลส่วนบุคคลก็ตาม ซึ่งมีความเกี่ยวข้องกับกฎหมายฉบับนี้ที่จะต้องปฏิบัติตาม หากผู้ใดหรือองค์กรใดฝ่าฝืน ย่อมมีบทลงโทษตามกฎหมายตามมา ซึ่งบทลงโทษนั้น มีทั้งโทษทางแพ่ง ทางอาญา และทางปกครองด้วย โดย PDPA (Personal Data Protection Act) ของประเทศไทย และ GDPR (General Data Protection Regulation) ซึ่งเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป เป็นกฎหมายที่มีวัตถุประสงค์ในการคุ้มครองข้อมูลส่วนบุคคล ถึงแม้ว่า PDPA และ GDPR จะมีวัตถุประสงค์ที่คล้ายคลึงกันในการคุ้มครองข้อมูลส่วนบุคคล แต่ก็มีความแตกต่างในรายละเอียดและขอบเขตการบังคับใช้ที่สำคัญ องค์กรที่ดำเนินธุรกิจในประเทศไทยและมีการประมวลผลข้อมูลส่วนบุคคลของบุคคลในสหภาพยุโรป จำเป็นต้องปฏิบัติตามทั้งสองกฎหมายเพื่อให้สอดคล้องกับข้อกำหนดที่เกี่ยวข้อง

นอกจากนี้ ยังมีข้อมูลส่วนบุคคลประเภทหนึ่งที่กฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) ให้ความสำคัญเป็นพิเศษ และกำหนดบทลงโทษที่รุนแรงในกรณีที่เกิดการรั่วไหลของข้อมูลสู่สาธารณะ ซึ่งได้แก่ ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data) เช่น ข้อมูลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสุขภาพจิต ข้อมูลเกี่ยวกับสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ ข้อมูลทางชีวมิติ (Biometric) เช่น รูปภาพใบหน้า ลายนิ้วมือ ฟิล์มเอกซเรย์ ข้อมูลสแกนม่านตา ข้อมูลอัตลักษณ์เสียง และข้อมูลพันธุกรรม รวมถึงข้อมูลอื่นใดที่อาจกระทบต่อเจ้าของข้อมูลในลักษณะเดียวกันตามที่คณะกรรมการประกาศกำหนด ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data) ได้รับบทลงโทษที่รุนแรงกว่าเมื่อเทียบกับข้อมูลส่วนบุคคลทั่วไป (Personal Data) เนื่องจากหากข้อมูลเหล่านี้ถูกเปิดเผยสู่สาธารณะ จะก่อให้เกิดผลกระทบที่ร้ายแรงต่อเจ้าของข้อมูล (Data Subject) มากกว่าข้อมูลส่วนบุคคลทั่วไป โดยอาจกระทบต่อสิทธิเสรีภาพของบุคคล เช่น สิทธิเสรีภาพในความคิด ความเชื่อทางศาสนา การแสดงออก การชุมนุม สิทธิในชีวิตร่างกาย การอยู่อาศัย และการไม่ถูกเลือกปฏิบัติ ข้อมูลที่มีลักษณะละเอียดอ่อน เช่น พฤติกรรมทางเพศ เชื้อชาติ ศาสนา หรือประวัติอาชญากรรม หากเกิดการรั่วไหล จะนำไปสู่การเกิดอคติและมีผลกระทบต่อชีวิตส่วนบุคคลอย่างรุนแรงมากกว่าข้อมูลส่วนบุคคลทั่วไป

ผู้ที่มีส่วนเกี่ยวข้องกับข้อมูลส่วนบุคคลในกฎหมาย PDPA แบ่งได้ ๓ ประเภท ประกอบด้วย (๑) เจ้าของข้อมูลส่วนบุคคล (Data Subject) คือ บุคคลซึ่งข้อมูลส่วนบุคคลนั้นสามารถระบุตัวตนได้โดยตรงหรือโดยอ้อม และเป็นผู้มีสิทธิ์ตามกฎหมายในการควบคุมข้อมูลของตนเอง

---

[๑๘] ราชกิจจานุเบกษา, *พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒*, สืบค้นเมื่อวันที่ ๑ มีนาคม ๒๕๖๘, จาก https://www.ratchakitcha.soc.go.th/DATA/PDF/๒๕๖๒/A/๐๖๙/T_๐๐๕๒.PDF

(๒) ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) คือ บุคคลหรือนิติบุคคลที่มีอำนาจและหน้าที่ในการตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ทั้งนี้ ผู้ควบคุมข้อมูลต้องดำเนินการให้เป็นไปตามข้อกำหนดทางกฎหมายและหลักการคุ้มครองข้อมูลส่วนบุคคล และ (๓) ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) คือ บุคคลหรือนิติบุคคลที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล สำหรับบทลงโทษของผู้ที่ไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) แบ่งออกเป็น ๓ ประเภท ได้แก่

๑) โทษทางแพ่ง กำหนดให้ผู้ละเมิดต้องชดใช้ค่าสินไหมทดแทนที่เกิดขึ้นจริงให้แก่เจ้าของข้อมูลส่วนบุคคลที่ได้รับความเสียหายจากการละเมิด และอาจต้องชำระค่าสินไหมทดแทนเพื่อการลงโทษเพิ่มเติมสูงสุดได้อีก ๒ เท่าของค่าเสียหายจริง เช่น หากศาลตัดสินให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องชดใช้ค่าสินไหมทดแทนแก่เจ้าของข้อมูลส่วนบุคคลเป็นจำนวน ๑๐๐,๐๐๐ บาท ศาลอาจมีคำสั่งให้เพิ่มค่าสินไหมทดแทนเพื่อการลงโทษอีก ๒ เท่าของค่าเสียหายจริง รวมเป็นเงินทั้งสิ้น ๓๐๐,๐๐๐ บาท

๒) โทษอาญา ประกอบด้วยทั้งโทษจำคุกและโทษปรับ โดยโทษจำคุกสูงสุดไม่เกิน ๑ ปี หรือปรับไม่เกิน ๑ ล้านบาท หรือทั้งจำทั้งปรับ โทษสูงสุดดังกล่าวจะเกิดขึ้นจากการไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) ในส่วนที่เกี่ยวข้องกับการใช้เปิดเผย หรือส่งโอนข้อมูลไปยังต่างประเทศ โดยเฉพาะกรณีที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data) หากผู้กระทำความผิดเป็นนิติบุคคล เช่น บริษัท (นิติบุคคล) อาจเกิดข้อสงสัยว่าใครจะเป็นผู้รับโทษจำคุก เนื่องจากบริษัทไม่สามารถถูกจำคุกได้ ในกรณีนี้ โทษจะตกอยู่กับผู้บริหาร กรรมการ หรือบุคคลที่รับผิดชอบในการดำเนินงานของบริษัทนั้น ๆ

๓) โทษทางปกครอง ในรูปแบบของการปรับ มีตั้งแต่ ๑ ล้านบาทจนถึงสูงสุดไม่เกิน ๕ ล้านบาท โดยโทษปรับสูงสุด ๕ ล้านบาท จะเกิดขึ้นในกรณีที่ไม่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) ในส่วนที่เกี่ยวข้องกับการใช้ข้อมูล เปิดเผยข้อมูล หรือส่งโอนข้อมูลไปยังต่างประเทศ โดยเฉพาะข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data) โทษทางปกครองดังกล่าวจะดำเนินการแยกต่างหากจากการชดใช้ค่าเสียหายที่เกิดจากโทษทางแพ่งและโทษทางอาญา

จะเห็นได้ว่า PDPA หรือพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลมีเจตนารมณ์หลักเพื่อคุ้มครองสิทธิในข้อมูลส่วนบุคคลของเจ้าของข้อมูล ให้มั่นใจว่าข้อมูลของตนจะได้รับการดูแลและนำไปใช้ตามวัตถุประสงค์ที่เหมาะสม โดยได้รับความยินยอมอย่างชัดเจนจากเจ้าของข้อมูล อย่างไรก็ตาม เจ้าของข้อมูลควรพิจารณาอย่างถี่ถ้วนก่อนให้ข้อมูลส่วนบุคคลกับองค์กรหรือบุคคลอื่น โดยตรวจสอบว่าข้อมูลที่ให้ไปมีความจำเป็นและเกี่ยวข้องกับวัตถุประสงค์ของการใช้งานหรือไม่ หากพบว่าการขอข้อมูลไม่สอดคล้องกับวัตถุประสงค์ เจ้าของข้อมูลมีสิทธิปฏิเสธการให้ข้อมูลดังกล่าวเพื่อป้องกันการนำข้อมูลไปใช้โดยมิชอบ ในส่วนขององค์กรและผู้ควบคุมข้อมูลส่วนบุคคล จำเป็นต้องดำเนินการตามแนวปฏิบัติที่สอดคล้องกับ PDPA อย่างเคร่งครัด โดยกำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร ให้ความรู้แก่บุคลากรเกี่ยวกับข้อจำกัดในการเก็บรวบรวม การใช้ และเปิดเผยข้อมูล

ส่วนบุคคล ตลอดจนจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล จำกัดสิทธิการเข้าถึงข้อมูล และบันทึกกิจกรรมที่เกี่ยวข้องกับการใช้ข้อมูลส่วนบุคคล ทั้งนี้ เพื่อให้มั่นใจว่าการดำเนินงานเป็นไปตามหลักเกณฑ์ของกฎหมาย PDPA อย่างครบถ้วน

๓.๑.๔ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒[๑๙]

ปัจจุบันภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างต่อเนื่องและมีความรุนแรงเพิ่มขึ้น สร้างความเสียหายให้แก่ประชาชน สังคม ตลอดจนประเทศชาติ โดยไม่เว้นแม้แต่ประเทศที่พัฒนาแล้วหรือประเทศที่กำลังพัฒนา ดังจะเห็นได้จากเหตุการณ์สำคัญที่เกิดขึ้นกับหน่วยงานโครงสร้างพื้นฐาน (Critical Infrastructures) ของประเทศ เป็นสาเหตุที่จำเป็นจะต้องมีกฎหมายด้านไซเบอร์ สำหรับประเทศไทย คือ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ โดยเหตุผลและความจำเป็นในการตราพระราชบัญญัตินี้ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์มีประสิทธิภาพและเพื่อให้มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ โดยพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ เป็นกฎหมายที่สำคัญในการปรับปรุงและควบคุมความปลอดภัยทางไซเบอร์ในประเทศไทย โดยมีเนื้อหาสำคัญ ดังนี้

๑) กำหนดหน้าที่และอำนาจของหน่วยงานที่เกี่ยวข้องเพื่อดูแลและควบคุมความปลอดภัยทางไซเบอร์ในระดับประเทศ

๒) กำหนดความรับผิดชอบของผู้ประกอบการในการรักษาความปลอดภัยทางไซเบอร์ของข้อมูลลูกค้าและลูกค้า

๓) การรักษาความลับและความเป็นส่วนตัวของข้อมูลที่เกี่ยวข้องกับการทำธุรกิจทางอิเล็กทรอนิกส์

๔) ส่งเสริมความตระหนักรู้และการศึกษาในเรื่องความปลอดภัยทางไซเบอร์ให้กับผู้ประกอบการและประชาชนทั่วไป

๕) กำหนดมาตรการความปลอดภัยที่ผู้ประกอบการต้องปฏิบัติเพื่อรักษาความปลอดภัยทางไซเบอร์ เช่น การรักษาความมั่นคงของระบบเทคโนโลยีสารสนเทศ การเข้ารหัสข้อมูล และการสร้างระบบการรายงานเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัย

๖) กำหนดการประกาศความเสียหายและการเสียชีวิตที่เกิดจากการกระทำที่ผิดกฎหมายทางไซเบอร์

๗) กำหนดมาตรการเพื่อรักษาความปลอดภัยทางไซเบอร์ในการส่งสัญญาณทางโทรคมนาคมและเนื้อหาทางอิเล็กทรอนิกส์

นอกจากนี้ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๙ (๑) บัญญัติให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) มีหน้าที่และอำนาจ เสนอนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ส่งเสริมและสนับสนุนการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๔๒ และมาตรา ๔๓

---

[๑๙] ราชกิจจานุเบกษา, *พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒*, สืบค้นเมื่อวันที่ ๑ มีนาคม ๒๕๖๘, จาก https://www.ratchakitcha.soc.go.th/DATA/PDF/๒๕๖๒/A/๐๖๙/T_๐๐๒๐.PDF

ต่อคณะรัฐมนตรีเพื่อให้ความเห็นชอบนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์และใช้เป็นแผนแม่บท ในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย การพัฒนาความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวมที่ครอบคลุมในทุกมิติ และเพื่อใช้เป็นกรอบแนวทางการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ มาตรา ๙ (๓) บัญญัติให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) มีหน้าที่และอำนาจจัดทำแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์เสนอต่อคณะรัฐมนตรี สำหรับเป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ในสถานการณ์ปกติและในสถานการณ์ที่อาจจะเกิดหรือเกิดภัยคุกคามทางไซเบอร์ โดยแผนดังกล่าวจะต้องสอดคล้องกับนโยบายยุทธศาสตร์และแผนระดับชาติ และกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ ซึ่งที่กล่าวมาทั้งหมดเป็นการเสริมสร้างความมั่นคงและความปลอดภัยทางไซเบอร์ในระบบการทำธุรกิจทางอิเล็กทรอนิกส์ในประเทศไทย

๓.๑.๕ พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๖[๒๐]

กฎหมายฉบับนี้เป็นกฎหมายสำคัญที่รัฐออกมาเพื่อให้หน่วยงานและธนาคารทุกแห่งร่วมกันกำหนดมาตรการดูแลประชาชนจากมิจฉาชีพหลอกโอนเงิน และรับมือกับการหลบเลี่ยงการตรวจสอบธุรกรรมของมิจฉาชีพผ่านสิ่งที่เรียกว่า บัญชีม้า[๒๑] เพื่อช่วยให้หน่วยงานที่เกี่ยวข้องดำเนินการระงับธุรกรรมต้องสงสัยและมีการบัญญัติความผิดเกี่ยวกับบัญชีม้าเอาไว้โดยเฉพาะ โดยมีสาระสำคัญ ดังนี้[๒๒]

๑) การแลกเปลี่ยนข้อมูล สถาบันการเงิน ผู้ให้บริการโทรคมนาคม ผู้ประกอบธุรกิจที่เกี่ยวข้อง และหน่วยงาน เช่น สำนักงานตำรวจแห่งชาติและสำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) มีอำนาจเข้าถึง และแลกเปลี่ยนข้อมูลเกี่ยวกับบัญชีและธุรกรรมของลูกค้าผ่านระบบการแลกเปลี่ยนข้อมูลได้ โดยสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ (กสทช.) เป็นหน่วยงานจัดทำระบบฐานข้อมูลกลางเท่าที่จำเป็นเกี่ยวกับข้อมูลการลงทะเบียนผู้ใช้งาน ข้อความสั้น เพื่อใช้ในการสืบสวนสอบสวนและป้องกัน

๒) เพิ่มอำนาจการดำเนินการกับแพลตฟอร์มทรัพย์สินที่เกี่ยวข้องกับการกระทำความผิด โดยกำหนดแพลตฟอร์มให้ต้องร่วมรับผิดชอบการทำธุรกรรมและการกระทำความผิดที่เกิดขึ้น เช่น การห้ามการซื้อขายสินทรัพย์ดิจิทัลผ่านแพลตฟอร์ม Peer-to-Peer Lending (P๒P) โดยห้ามให้บริการหรือแสดงว่าพร้อมจะให้บริการซื้อขายหรือแลกเปลี่ยนสินทรัพย์ดิจิทัลประเภทคริปโต

---

[๒๐] พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๖ (๑๗ มีนาคม ๒๕๖๖). *ราชกิจจานุเบกษา*, เล่ม ๑๔๐ ตอนที่ ๑๘ ก, น. ๑-๗.

[๒๑] บัญชีม้า (mule account) คือ บัญชีเงินฝากธนาคารที่เปิดขึ้นโดยบุคคลหนึ่งแต่ถูกนำไปใช้โดยบุคคลอื่นโดยเฉพาะมิจฉาชีพที่นำมาใช้เป็นช่องทางในการรับเงินและถ่ายโอนเงินที่ได้มาจากการกระทำความผิดเพื่อป้องกันไม่ให้มีพยานหลักฐานเชื่อมโยงมาถึงตัวได้

[๒๒] ปิยอร เปลี่ยนผดุง, *ทำความรู้จัก พ.ร.ก. ป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๖ และ (ร่าง) พ.ร.ก. ไซเบอร์*. สืบค้นเมื่อวันที่ ๑ มีนาคม ๒๕๖๘, จาก https://www.up.ac.th/NewsReadBlog๒.aspx?itemID=๓๓๙๙๕

เคอร์เรนซี โทเคนดิจิทัลเพื่อการใช้ประโยชน์ที่มิได้มีวัตถุประสงค์หลักเพื่อการอุปโภคบริโภค เพื่อลดปัญหาการฟอกเงินโดยนำมาเปลี่ยนเป็นเงินสกุลดิจิทัล

๓) เร่งรัดกระบวนการคืนเงินให้กับผู้เสียหาย ให้อำนาจแก่คณะกรรมการธุรกรรมตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงินเป็นผู้พิจารณาคืนเงินให้แก่ผู้เสียหาย โดยไม่ต้องรอให้มีการยื่นฟ้องคดีต่อศาลเพื่อพิจารณามีคำสั่งถึงที่สุดก่อน ทำให้ขั้นตอนกระบวนพิจารณาการคืนเงินแก่ผู้เสียหายรวดเร็วขึ้น

๔) เพิ่มความรับผิดของสถาบันการเงินหรือผู้ให้บริการเครือข่ายโทรศัพท์ โดยให้ผู้ให้บริการอื่นที่เกี่ยวข้องหรือสื่อสังคมออนไลน์มีส่วนรับผิดชอบในความเสียหายที่เกิดขึ้นกับผู้เสียหายที่ถูกหลอกลวงจากอาชญากรรมทางเทคโนโลยี หากหน่วยงานดังกล่าวไม่ได้ใช้ความระมัดระวังที่พึงปฏิบัติในวิชาชีพ

๕) เพิ่มบทกำหนดโทษสำหรับผู้ให้บริการซื้อขายหรือแลกเปลี่ยนสินทรัพย์ดิจิทัลและผู้ซื้อขายข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการกระทำความผิดออนไลน์ มีการกำหนดโทษสำหรับผู้ให้บริการซื้อขายหรือแลกเปลี่ยนสินทรัพย์ดิจิทัลประเภทคริปโทเคอร์เรนซี โทเคนดิจิทัล และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลที่นำเงินที่ได้จากการกระทำความผิดออนไลน์มาฟอกเงินโดยเปลี่ยนเป็นเงินสกุลดิจิทัล และกำหนดโทษสำหรับผู้ซื้อขายข้อมูลส่วนบุคคลด้วย

แต่อย่างไรก็ดี กฎหมายฉบับนี้ยังขาดอำนาจหน้าที่และการกำหนดโทษหลายประเด็น โดยเฉพาะอำนาจการดำเนินการกับบัญชีม้าบนแพลตฟอร์ม P๒P อำนาจการคืนเงินให้กับประชาชน และการรับผิดร่วมของผู้มีส่วนเกี่ยวข้องกับการกระทำความผิด อันนำไปสู่การปรับปรุงแก้ไขเพิ่มเติมพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๖ ซึ่งเป็นการเพิ่มมาตรการแก้ไขปัญหาอาชญากรรมออนไลน์และมิจฉาชีพ โดยเพิ่มหน้าที่ให้หน่วยงานของรัฐหรือผู้ให้บริการเลขหมายโทรศัพท์ในการสั่งระงับหรือยกเลิกการให้บริการเลขหมายโทรศัพท์สำหรับบริการโทรศัพท์เคลื่อนที่ที่ถูกใช้หรืออาจถูกใช้ทำธุรกรรมที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยีกำหนดขั้นตอนหรือกระบวนการพิจารณาโดยเฉพาะ เพื่อให้การคืนเงินแก่ผู้เสียหายเป็นไปอย่างรวดเร็วยิ่งขึ้น และเพิ่มโทษการซื้อขายข้อมูลส่วนบุคคล

๓.๑.๖ พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ ๒) พ.ศ. ๒๕๖๘[๒๓]

ปัจจุบันได้มีการประกาศใช้พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ ๒) พ.ศ. ๒๕๖๘ เพื่อเป็นกลไกในการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีที่เกิดขึ้น โดยเหตุผลและความจำเป็นในการตราพระราชกำหนดนี้มีเป้าหมายเพื่อเพิ่มประสิทธิภาพของรัฐในการจัดการกับอาชญากรรมทางไซเบอร์ ซึ่งส่งผลกระทบต่อความมั่นคงของประเทศ เศรษฐกิจ และความปลอดภัยของประชาชน พระราชกำหนดฉบับนี้ถือได้ว่าเป็นพัฒนาการที่สำคัญของระบบกฎหมายไทย ที่มุ่งเน้นการเสริมสร้างอำนาจแก่เจ้าหน้าที่รัฐและหน่วยงาน

---

[๒๓] ราชกิจจานุเบกษา, พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ ๒) พ.ศ. ๒๕๖๘, สืบค้นเมื่อวันที่ ๒๔ เมษายน ๒๕๖๘, จาก https://ratchakitcha.soc.go.th/documents/67320.pdf

ที่เกี่ยวข้องในการดำเนินการอย่างทันท่วงทีต่อผู้กระทำความผิดทางเทคโนโลยี โดยเฉพาะอย่างยิ่งการให้เจ้าหน้าที่มีอำนาจในการสั่งระงับบัญชีธนาคารหรือหมายเลขโทรศัพท์ที่ต้องสงสัย เพื่อยับยั้งความเสียหายที่อาจเกิดขึ้นแก่ประชาชนและระบบเศรษฐกิจโดยรวม อย่างไรก็ดี การใช้อำนาจดังกล่าวจำเป็นต้องอยู่ภายใต้กรอบแห่งความชอบธรรมและการตรวจสอบอย่างเข้มงวด เพื่อป้องกันมิให้เกิดการใช้อำนาจในทางที่เกินขอบเขต อันอาจเป็นการละเมิดสิทธิเสรีภาพของประชาชนโดยไม่จำเป็น ดังนั้น จึงควรกำหนดแนวปฏิบัติและขั้นตอนการใช้อำนาจอย่างชัดเจน พร้อมทั้งเปิดโอกาสให้ผู้ที่ได้รับผลกระทบสามารถอุทธรณ์หรือใช้สิทธิตามกฎหมายได้อย่างเป็นธรรม พระราชกำหนดฉบับนี้มีสาระสำคัญเป็นการแก้ไขเพิ่มเติมพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๖ โดยกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีเพิ่มเติม รวมถึงมาตรการแก้ไขปัญหาอาชญากรรมออนไลน์และกลุ่มมิจฉาชีพ สาระสำคัญสามารถสรุปได้ ดังนี้

๑) บัญญัติให้การนำข้อมูลส่วนบุคคล (เช่น เลขบัตรประชาชน บัญชีธนาคาร หมายเลขโทรศัพท์) ไปใช้เพื่อการหลอกลวงถือเป็นความผิด มีโทษจำคุกไม่เกิน ๑ ปี หรือปรับไม่เกิน ๑๐๐,๐๐๐ บาท นอกจากนี้ ผู้เปิดบัญชีหรือจำหน่ายบัญชีให้ผู้อื่น (บัญชีม้า) แม้จะอ้างว่าไม่รู้ก็เข้าข่ายมีความผิดตามกฎหมาย ทั้งนี้ กำหนดมาตรการบังคับใช้โดยสำนักงานคณะกรรมการข้อมูลส่วนบุคคลและหน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้องต้องเร่งตรวจสอบและดำเนินคดีกับผู้กระทำผิด ภายใต้นโยบายเร่งด่วนในการปกป้องประชาชนจากการฉ้อโกงออนไลน์ การลงโทษผู้เปิดเผยข้อมูลผิดวิธีจะช่วยยับยั้งการนำข้อมูลไปใช้ในทางทุจริต เสริมสร้างความเชื่อมั่นในการรักษาความปลอดภัยข้อมูลของประชาชน ในด้านการบริหารราชการ หน่วยงานที่เกี่ยวข้องจะต้องจัดทำแนวทางและเครื่องมือในการตรวจสอบดูแลข้อมูลส่วนบุคคล รวมทั้งให้ความรู้ประชาชนเกี่ยวกับการรักษาความปลอดภัยของข้อมูล เพื่อประสานกับมาตรการบังคับใช้ด้านกฎหมายอย่างเป็นระบบ

๒) กำหนดให้สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ มีอำนาจออกคำสั่งยับยั้งหรือเพิกถอนการให้บริการกับเบอร์ที่น่าสงสัย ภายใต้นโยบายเพื่อป้องกันการถูกฉ้อโกงผ่านช่องทางโทรศัพท์หรือข้อความสั้น (SMS) ซึ่งพบว่ามีปัญหาแพร่หลาย การกำหนดหน้าที่ดังกล่าวเพื่อลดโอกาสที่ข้อความหลอกลวงจะถึงมือประชาชน ในเชิงบริหารราชการ คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติจะต้องออกกฎเกณฑ์และแนวทางปฏิบัติแก่ผู้ให้บริการโทรคมนาคม ดำเนินการประสานงานกับสำนักงานตำรวจและหน่วยงานไซเบอร์ เพื่อรับข้อมูลหมายเลขต้องสงสัย และประเมินผลการกรองอย่างเป็นระบบต่อไป

๓) ให้อำนาจเจ้าหน้าที่รัฐ (เช่น สำนักงานตำรวจแห่งชาติ สำนักงานป้องกันและปราบปรามการฟอกเงิน และ กรมสอบสวนคดีพิเศษ) สามารถสั่งอายัดบัญชีหรือยับยั้งการทำธุรกรรมได้ทันทีเมื่อพบการกระทำผิดทางเทคโนโลยี ทั้งยังเปิดช่องให้แลกเปลี่ยนข้อมูลระหว่างธนาคาร ผู้ให้บริการมือถือ หน่วยงานกำกับดูแล และเจ้าหน้าที่ฝ่ายความมั่นคง เช่น รายการโอนเงินหรือพฤติกรรมทางโทรคมนาคมที่ผิดปกติ การบังคับใช้กฎหมายจึงเน้นการประสานงานข้ามหน่วยงานเพื่อสกัดกั้นอาชญากรรมอย่างรวดเร็ว ภายใต้นโยบายที่มุ่งเพิ่มประสิทธิภาพการสืบสวนและปกป้องทรัพย์สินของประชาชน ระบบการบังคับใช้นี้จะต้องสร้างขั้นตอนปฏิบัติ (เช่น คำร้องขอข้อมูล

ข้อกำหนดการอายัด) และมีกลไกประสานงานระหว่างหน่วยงานราชการต่าง ๆ ให้ชัดเจน ส่งผลให้การบริหารราชการสามารถดำเนินการอายัดทรัพย์สิน และติดตามมูลค่าความเสียหายได้รวดเร็วขึ้น

๔) กำหนดให้ธนาคารและผู้ประกอบธุรกิจบริการการชำระเงินมีหน้าที่รับผิดชอบร่วมในความเสียหายของลูกค้า หากประชาชนถูกหลอกโอนเงินแล้ว พบว่าธนาคารไม่ได้ปฏิบัติตามมาตรการป้องกันและเกณฑ์ที่กำหนดโดย หน่วยงานกำกับดูแล เช่น ไม่ตรวจสอบข้อมูลผู้ทำธุรกรรมหรือนำบัญชีบัญชีม้าเข้าระบบที่ผ่านมาธนาคารแห่งประเทศไทยได้สนับสนุนหลักการนี้และเตรียมออกประกาศกำหนดหน้าที่และความรับผิดชอบอย่างชัดเจน หากฝ่าฝืนจะมีโทษปรับสูงสุด ๕๐๐,๐๐๐ บาท หรือโทษจำคุกไม่เกินหนึ่งปีในกรณีเพิกเฉยจนเกิดความเสียหาย การบังคับใช้นี้เป็นนโยบายยึดหลักให้ภาคการเงินมีส่วนร่วมในการคุ้มครองประชาชน ยกระดับมาตรการภายในสถาบันการเงิน (เช่น ระบบยืนยันตัวตนที่เข้มงวดกว่าเดิม) และสร้างความระมัดระวังร่วมกับผู้ใช้บริการ เชิงบริหาร รัฐบาลโดยธนาคารแห่งประเทศไทยจะต้องออกประกาศและกำกับดูแลให้ธนาคารปฏิบัติตามมาตรฐาน มีการตรวจสอบการปฏิบัติจริง พร้อมทั้งกำหนดวิธีวิเคราะห์กรณีปัญหาและบทลงโทษอย่างเป็นระบบ

๕) ขยายความรับผิดชอบไปยังผู้ให้บริการโทรศัพท์มือถือ และผู้ให้บริการสื่อสังคมออนไลน์ ให้มีส่วนร่วมรับผิดชอบเช่นเดียวกับสถาบันการเงินต่อความเสียหายที่เกิดขึ้นกับผู้เสียหาย ทั้งยังให้มีหน้าที่ดำเนินมาตรการป้องกันที่สำคัญ เช่น ป้องกันการลงทะเบียนซิมโดยใช้เอกสารปลอม ติดตามข้อความหรือโพสต์หลอกลวง และต้องให้ข้อมูลตามคำสั่งของเจ้าหน้าที่ (เช่น หมายเลขผู้ใช้ ผู้ส่ง SMS ที่เกี่ยวข้อง) หากไม่ปฏิบัติตามจะมีโทษปรับและจำคุกเทียบเท่าธนาคารดังกล่าว การบังคับใช้มาตรการนี้เป็นไปตามนโยบายกระจายภาระป้องกันอาชญากรรมไซเบอร์ไปยังภาคส่วนดิจิทัลทั้งหมด ดึงดูดให้เอกชนลงทุนในระบบตรวจสอบภายใน และเสริมสร้างมาตรฐานอุตสาหกรรมการคุ้มครองผู้บริโภคทางไซเบอร์ ด้านการบริหาร หน่วยงาน กสทช. และกระทรวงดิจิทัลฯ ต้องกำหนดแนวทางและติดตามการปฏิบัติของผู้ให้บริการฯ และส่งเสริมการประสานงานกับหน่วยงานบังคับใช้กฎหมายในการตรวจสอบและแลกเปลี่ยนข้อมูลอย่างต่อเนื่อง

๖) บัญญัติให้หน่วยงานรัฐสำคัญจัดตั้งศูนย์ปฏิบัติการเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ศปอท.) ประกอบด้วย สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ ธนาคารแห่งประเทศไทย สำนักงานป้องกันและปราบปรามการฟอกเงิน คณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ หรือหน่วยงานอื่นของรัฐหรือหน่วยงานของเอกชนที่รัฐมนตรีประกาศกำหนดแต่งตั้งผู้แทนเข้าร่วมให้ปฏิบัติงานในศูนย์ปฏิบัติการเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี เพื่อรับคำร้องเรียน ตรวจสอบและระงับธุรกรรมที่เกี่ยวข้องกับอาชญากรรมเทคโนโลยี และประสานงานคืนเงินให้ผู้เสียหาย การบังคับใช้มาตรการนี้เป็นการย้ำประเด็นเชิงนโยบายในการบูรณาการการทำงานระดับชาติให้เป็นเครือข่ายเดียวกัน ช่วยให้การสืบสวนและตอบโต้คดีไซเบอร์มีประสิทธิภาพขึ้น ในแง่การบริหารราชการต้องมีการจัดตั้งหน่วยงานเฉพาะกิจหรือศูนย์ประสานงานในแต่ละองค์กร เพิ่มบุคลากรเชี่ยวชาญ ฝึกอบรมบุคลากร และพัฒนา

กรอบการทำงานร่วมกัน เช่น การแบ่งปันข้อมูลระหว่างศูนย์และกำหนดกระบวนการส่งต่อผู้เสียหายอย่างรวดเร็ว

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ ๒) พ.ศ. ๒๕๖๘ มีผลใช้บังคับตั้งแต่วันที่ ๑๓ เมษายน ๒๕๖๘ โดยมีวัตถุประสงค์เพื่อปรับปรุงกฎหมายเดิมให้สามารถใช้เป็นเครื่องมือสำคัญในการปราบปรามแก๊งคอลเซ็นเตอร์และอาชญากรรมไซเบอร์ รวมถึงการเพิ่มอำนาจให้แก่เจ้าหน้าที่รัฐและผู้ให้บริการโทรคมนาคมในการระงับหมายเลขต้องสงสัย ตลอดจนเร่งรัดกระบวนการคืนเงินแก่ผู้เสียหาย นอกจากนี้ ยังมีการกำหนดให้แพลตฟอร์มสื่อสังคมออนไลน์ สถาบันการเงิน และผู้ให้บริการโทรคมนาคมต้องมีส่วนร่วมรับผิดชอบต่อความเสียหายที่เกิดขึ้น

๓.๒ กฎหมายลำดับรองที่เกี่ยวข้องกับการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยี[๒๔]

๓.๒.๑ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การจัดตั้ง หน้าที่และอำนาจของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ พ.ศ. ๒๕๖๔

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ อาศัยอำนาจตามความในมาตรา ๒๒ วรรคสอง แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ออกประกาศฉบับนี้ เพื่อกำหนดให้มีการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติขึ้นเป็นหน่วยงานภายในสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตาม วิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

๓.๒.๒ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและภารกิจหรือการให้บริการที่เกี่ยวข้อง พ.ศ. ๒๕๖๔

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ อาศัยอำนาจตามความในมาตรา ๕๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ออกประกาศฉบับนี้ เพื่อกำหนดลักษณะ หน้าที่ และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (Sectoral CERT) สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญ

---

[๒๔] สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (NCSA), *กฎหมายลำดับรอง*, สืบค้นเมื่อวันที่ ๒๘ กุมภาพันธ์ ๒๕๖๘. จาก https://drive.ncsa.or.th/s/m๗m๘๙wj๓ywgSXfJ?fbclid=IwY๒xjawJNB๓hleHRuA๒FlbQIxMAABHYihfLKS๘HxX๙aQRPlY_๒i๙BvsZc๑sY๐th๕btfvv๘F๑LbhNg๖RudZ๕gfnQ_aem_๘๒yEjCilQcRAwmktwLIrQg

ทางสารสนเทศ เพื่อประสานงาน เฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์ ปัจจุบันมีหน่วยงาน Sectoral CERT ในประเทศไทย[๒๕]ดังนี้

(๑) ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์กระทรวงกลาโหม (Ministry of Defence Computer Security Incident Response Team: MODCSIRT)

(๒) ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านความมั่นคงของรัฐฝ่ายพลเรือน (Thailand Civilian Sector CERT: TCS-CERT)

(๓) ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์กระทรวงการคลัง (Ministry of Finance Computer Security Incident Response Team: MOF-CSIRT)

(๔) ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์กรมศุลกากร

(๕) ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ ในด้านบริการภาครัฐสำคัญ ที่มีการให้บริการโดยตรงแก่ประชาชน

(๖) ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร (Thailand Banking Sector CERT: TB-CERT)

(๗) ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (Thai Capital Market CERT: TCM-CERT)

(๘) ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม (Thailand Telecommunication CERT: TTC-CERT)

(๙) ศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข (Health CIRT)

(๑๐) ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านพลังงาน (Energy CERT)

๓.๒.๓ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง กำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ อาศัยอำนาจตามความในมาตรา ๔๙ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ออกประกาศฉบับนี้ เพื่อเป็นการประกาศกำหนดภารกิจหรือบริการของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้งสิ้น ๘ ด้าน ปัจจุบันประกาศฯ ดังกล่าวมีหน่วยงานควบคุม ๑๙ หน่วยงาน ประกอบด้วย

(๑) ด้านความมั่นคงของรัฐ ได้แก่ สำนักงานปลัดกระทรวงกลาโหม สำนักงานตำรวจแห่งชาติ และสำนักงานสภาความมั่นคงแห่งชาติ

---

[๒๕] ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT), *รายชื่อ CERT ในประเทศไทย*, สืบค้นเมื่อวันที่ ๒๘ กุมภาพันธ์ ๒๕๖๘. จาก https://www.thaicert.or.th/%E0%B8%AB%E0%B8%99%E0%B9%88%E0%B8%A7%E0%B8%A2%E0%B8%87%E0%B8%B2%E0%B8%99-cert/

(๒) ด้านบริการภาครัฐที่สำคัญ ได้แก่ กระทรวงการคลัง กรมศุลกากร กรมการปกครอง สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) และกรมชลประทาน

(๓) ด้านการเงินการธนาคาร ได้แก่ ธนาคารแห่งประเทศไทย และสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

(๔) ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ได้แก่ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

(๕) ด้านการขนส่งและโลจิสติกส์ ได้แก่ สำนักงานตำรวจแห่งชาติ กรมการขนส่งทางราง สำนักงานปลัดกระทรวงคมนาคม และสำนักงานการบินพลเรือนแห่งประเทศไทย

(๖) ด้านพลังงานและสาธารณูปโภค ได้แก่ กระทรวงพลังงาน และการประปาส่วนภูมิภาค (เฉพาะบริการส่วนภูมิภาค)

(๗) ด้านสาธารณสุข ได้แก่ สำนักงานปลัดกระทรวงสาธารณสุข สำนักงานคณะกรรมการอาหารและยา และสำนักงานปรมาณูเพื่อสันติ

(๘) ด้านอื่นตามที่คณะกรรมการประกาศกำหนดเพิ่มเติม

โดยสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (NCSA) กำหนดให้หน่วยงานควบคุมหรือกำกับดูแลดำเนินการ ๕ ขั้นตอน ดังนี้

(๑) การระบุกระบวนการที่สำคัญ

(๒) การพิจารณาผลกระทบจากการหยุดชะงักของกระบวนการที่สำคัญ

(๓) การประเมินเวลาการหยุดชะงักที่ยอมรับได้

(๔) เลือกกระบวนการที่สำคัญและการระบุทรัพย์สินสารสนเทศ

(๕) การระบุหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ[๒๖]

๓.๒.๔ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ อาศัยอำนาจตามความในมาตรา ๑๓ วรรคหนึ่ง (๔) และวรรคสอง และมาตรา ๕๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ออกประกาศฉบับนี้ เพื่อกำหนดให้หน่วยของรัฐ หน่วยงานควบคุม หรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีหน้าที่ในการจัดทำประมวลแนวทางปฏิบัติ และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อันเป็นข้อกำหนดขั้นต่ำ โดยมีแนวทางปฏิบัติ คือ (๑) แผนการตรวจสอบ (๒) การประเมินความเสี่ยง และ (๓) แผนการรับมือภัยคุกคามทางไซเบอร์ ซึ่งมีกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ดังนี้

---

[๒๖] หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) หมายถึง หน่วยงานของรัฐหรือเอกชนใช้ในการดำเนินงาน เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ สาธารณะ และเศรษฐกิจของประเทศ รวมถึงโครงสร้างพื้นฐานที่เกิดประโยชน์แก่สาธารณะ หากระบบถูกรบกวนจะทำให้ไม่สามารถดำเนินงานหรือให้บริการได้

(๑) การระบุความเสี่ยงที่อาจจะเกิดขึ้น (Identify)
(๒) มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)
(๓) มาตรการตรวจสอบและเฝ้าระวัง (Detect)
(๔) มาตรการเผชิญเหตุ (Respond)
(๕) มาตรการรักษาและฟื้นฟูความเสียหาย (Recover)

๓.๒.๕ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดระดับความรู้ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อแต่งตั้งเป็นพนักงานเจ้าหน้าที่ พ.ศ. ๒๕๖๔

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ อาศัยอำนาจตามความในมาตรา ๑๙ วรรคสอง แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ออกประกาศฉบับนี้ เพื่อกำหนดคุณสมบัติและความรู้ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคคลที่จะได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่

๓.๒.๖ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ อาศัยอำนาจตามความในมาตรา ๖๐ วรรคสอง แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ออกประกาศฉบับนี้ เพื่อประโยชน์ในการจำแนกลักษณะของภัยคุกคามทางไซเบอร์แต่ละระดับ รวมทั้งประเมินจากระดับผลกระทบที่อาจเกิดขึ้นหากระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือระบบงานที่มีความสำคัญอื่น ๆ ถูกโจมตีจากภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง ระดับร้ายแรง และระดับวิกฤติ

๓.๒.๗ ระเบียบคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ว่าด้วยการมอบอำนาจให้ปฏิบัติการแทนคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๕

คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) อาศัยอำนาจตามความในมาตรา ๑๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ออกประกาศฉบับนี้ เพื่อให้การดูแลและดำเนินการในการรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรงได้ทันท่วงที ให้ กกม. จึงมีการมอบอำนาจให้คณะกรรมการรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรง (ครร.) พิจารณาสั่งการกรณีเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรงหรือระดับวิกฤติ

๓.๒.๘ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐)

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ อาศัยอำนาจตามความในมาตรา ๙ (๑) (๒) และ (๓) และมาตรา ๔๓ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ออกประกาศฉบับนี้ เพื่อเป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย การพัฒนาความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวมที่ครอบคลุมในทุกมิติ และเพื่อใช้เป็นกรอบแนวทางการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ

๓.๒.๙ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ อาศัยอำนาจตามความในมาตรา ๑๓ (๕) และมาตรา ๕๗ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ออกประกาศฉบับนี้ เพื่อกำหนดแนวทางในการแจ้งและรายงานกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๓.๒.๑๐ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง หลักเกณฑ์และอัตราค่าธรรมเนียม ค่าบำรุง ค่าตอบแทน และค่าบริการในการดำเนินงาน พ.ศ. ๒๕๖๖

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ อาศัยอำนาจตามความในมาตรา ๒๓ (๔) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ออกประกาศฉบับนี้ เพื่อให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (NCSA) มีแนวทางในการเรียกเก็บค่าธรรมเนียมและ/หรือค่าบริการจากผู้รับบริการ สำหรับกรณีดังต่อไปนี้

(๑) การใช้ระบบหรือบริการสารสนเทศ เครื่องมือ หรืออุปกรณ์ หรือสิ่งอำนวยความสะดวก และพื้นที่หรือสถานที่

(๒) การใช้บริการสำรวจ การวางแผน การจัดการ หรือการวิจัย ในลักษณะการว่าจ้าง

(๓) การใช้บริการจัดฝึกอบรม สัมมนา หรือประชุมเชิงปฏิบัติการ

(๔) การรับรองมาตรฐานผู้ให้บริการเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(๕) การใช้บริการดำเนินโครงการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์หรือบริการอื่นที่เกี่ยวกับ หรือเกี่ยวเนื่องกับการรักษาความมั่นปลอดภัยไซเบอร์

๓.๒.๑๑ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูล หรือระบบสารสนเทศ พ.ศ. ๒๕๖๖

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ อาศัยอำนาจตามความในมาตรา ๙ (๔) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ออกประกาศฉบับนี้ เพื่อให้หน่วยงานของรัฐ หน่วยงานควบคุม หรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีการกำหนดคุณลักษณะและการจัดระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ โดยการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์พิจารณาจากวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objectives) ดังต่อไปนี้

(๑) การรักษาความลับ (Confidentiality)

(๒) การรักษาความถูกต้องครบถ้วน (Integrity)

(๓) การรักษาสภาพพร้อมใช้งาน (Availability)

ทั้งนี้ การประเมินและจัดระดับผลกระทบ แบ่งเป็น ๓ ระดับ คือ ระดับต่ำ ระดับกลาง และระดับสูง

๓.๒.๑๒ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ อาศัยอำนาจตามความในมาตรา ๙ (๔) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ออกประกาศฉบับนี้ เพื่อให้หน่วยงานของรัฐ หน่วยงานควบคุม หรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ได้กำหนดคุณลักษณะและการจัดระดับผลกระทบของข้อมูลหรือระบบสารสนเทศของตนว่ามีลักษณะ สูง กลาง หรือต่ำ โดยต้องกำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศนั้นในแต่ละระดับ

๓.๒.๑๓ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๖

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ อาศัยอำนาจตามความในมาตรา ๙ (๔) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ออกประกาศฉบับนี้ เพื่อให้มีกระบวนการตรวจสอบและรับรองการดำเนินงานของผู้ให้บริการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ไม่ว่าจะเป็นกระบวนการดำเนินงานระบบหรือเครื่องมือที่ใช้ในการดำเนินงาน หรือบุคลากรที่เกี่ยวข้องในการดำเนินงาน ว่ามีคุณภาพเป็นไปตามมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ โดยการรับรองคุณภาพของผู้ให้บริการ แบ่งเป็น ๓ ระดับ คือ ขั้นต้น ขั้นก้าวหน้า และขั้นสูง

๓.๒.๑๔ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๗

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ อาศัยอำนาจตามความในมาตรา ๙ (๕) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ออกประกาศฉบับนี้ เพื่อกำหนดมาตรการและแนวทางในการยกระดับทักษะ ความรู้ และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของพนักงานเจ้าหน้าที่ หรือเจ้าหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุม หรือกำกับดูแล และหน่วยงานเอกชนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และให้ระดับความรู้ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของพนักงานเจ้าหน้าที่

๓.๒.๑๕ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง หน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานควบคุมหรือกำกับดูแล พ.ศ. ๒๕๖๗

คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) อาศัยอำนาจตามความในมาตรา ๑๓ วรรคหนึ่ง (๕) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ออกประกาศฉบับนี้ เพื่อกำหนดหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ดังนี้

(๑) ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคาม

(๒) จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(๓) จัดให้มีการทบทวนเพื่อปรับปรุงหรือแก้ไขเพิ่มเติมนโยบาย มาตรฐาน และประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(๔) ให้ความร่วมมือและมีส่วนร่วมในการฝึกซ้อมรับมือภัยคุกคามทางไซเบอร์

(๕) แจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการเพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(๖) แจ้งรายชื่อหน่วยงานภายในหรือบุคคลที่เป็นเจ้าของกรรมสิทธิ์ ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์

(๗) จัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์

(๘) กำหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(๙) จัดให้มีการทบทวนระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(๑๐) จัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(๑๑) กำหนดกลไก ขั้นตอนหรือกระบวนการตรวจสอบหรือเฝ้าระวังภัยคุกคามทางไซเบอร์

(๑๒) จัดทำให้มีการทบทวนกลไก ขั้นตอนหรือกระบวนการตรวจสอบหรือเฝ้าระวังภัยคุกคามทางไซเบอร์

(๑๓) เข้าร่วมการทดสอบสถานะความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์

(๑๔) ตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ รวมถึงพฤติกรรมแวดล้อมของตน ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศ

(๑๕) ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามหลักเกณฑ์ที่กำหนดในประกาศประมวลแนวทางปฏิบัติ และในกรณีที่มีภัยคุกคามทางไซเบอร์เกิดขึ้นให้ดำเนินการต่อไปนี้ด้วย

ก. เก็บรักษาข้อมูลและพยานหลักฐาน

ข. แจ้งเหตุและส่งรายงานภัยคุกคามทางไซเบอร์

(๑๖) จัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity)

(๑๗) จัดให้มีการฝึกซ้อมตามแผนความต่อเนื่องทางธุรกิจ

(๑๘) จัดทำรายงานประจำปี

(๑๙) ดำเนินการตามที่ กมช. หรือ กมม. มอบหมาย หรือให้ความร่วมมือกับ สกมช. หรือหน่วยงานควบคุมหรือกำกับดูแล

๓.๒.๑๖ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยอาศัยอำนาจตามมาตรา ๙ (๔) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้ออกประกาศฉบับนี้เพื่อบังคับใช้กับหน่วยงานภาครัฐ (GOV) หน่วยงานที่อยู่ภายใต้การกำกับดูแลของรัฐบาล (REG) และโครงสร้างพื้นฐานข้อมูลที่สำคัญ (CII) รวมถึงกำหนดมาตรการสำหรับผู้ให้บริการคลาวด์และผู้ใช้บริการคลาวด์สาธารณะ (Public Cloud Service Provider) ที่ต้องให้บริการแก่หน่วยงานภาครัฐหรือหน่วยงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ตามพระราชบัญญัติฯ โดยใช้ฐานสัญญาระหว่างผู้ใช้บริการคลาวด์และผู้ให้บริการคลาวด์ เพื่อสนับสนุนการดำเนินการตามนโยบาย Cloud First Policy เพื่อให้หน่วยงานภาครัฐรวมถึงภาคเอกชนที่เกี่ยวข้องได้รับประโยชน์สูงสุดจากการดำเนินการตามนโยบายดังกล่าว

๓.๓ ความร่วมมือระหว่างประเทศที่เกี่ยวข้องกับการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยี

๓.๓.๑ ปฏิญญาอาเซียนว่าด้วยการป้องกันและต่อต้านอาชญากรรมไซเบอร์[๒๗]

การประชุมสุดยอดผู้นำอาเซียน ครั้งที่ ๓๑ ระหว่างวันที่ ๑๓-๑๔ พฤศจิกายน ๒๕๖๐ ณ กรุงมะนิลา สาธารณรัฐฟิลิปปินส์ ผู้นำอาเซียนได้ตระหนักถึงความจำเป็นในการเสริมสร้างความร่วมมือ

---

[๒๗] จันทพร ศรีโพน, *ปฏิญญาอาเซียนว่าด้วยการป้องกันและต่อต้านอาชญากรรมไซเบอร์ และบทวิเคราะห์กฎหมายไทยที่เกี่ยวข้อง*, สืบค้นเมื่อวันที่ ๒๘ กุมภาพันธ์ ๒๕๖๘. จาก https://lawforasean.krisdika.go.th/Content/View?Id=๓๔๙&Type=๑

ในการต่อต้านอาชญากรรมทางไซเบอร์ โดยมุ่งเน้นการป้องกันสังคมของภูมิภาคอาเซียน รวมถึงการริเริ่มวิธีการในระดับภูมิภาคที่มั่นคงและมีประสิทธิภาพ โดยการประชุมสุดยอดอาเซียนในครั้งดังกล่าว ผู้นำอาเซียนทั้ง ๑๐ ประเทศได้รับรองปฏิญญาอาเซียนว่าด้วยการป้องกันและต่อต้านอาชญากรรมไซเบอร์ (ASEAN Declaration to Prevent and Combat Cybercrime) ให้ความสำคัญกับการปรับปรุงกฎหมายที่เกี่ยวข้องกับอาชญากรรมทางไซเบอร์และหลักฐานทางอิเล็กทรอนิกส์ รวมทั้งสนับสนุนการร่างกรอบการทำงานระดับภูมิภาคเพื่อสร้างความร่วมมือระหว่างประเทศสมาชิก และการกำหนดแผนปฏิบัติการระดับชาติในการป้องกันและต่อต้านอาชญากรรมทางไซเบอร์ ตลอดจนการให้ความช่วยเหลือด้านผู้เชี่ยวชาญทางเทคนิคในการป้องกันและต่อต้านอาชญากรรมไซเบอร์ อันเป็นการยกระดับความร่วมมือระหว่างประเทศสมาชิกอาเซียนและประเทศคู่เจรจา รวมทั้งหน่วยงานและองค์กรต่าง ๆ ที่เกี่ยวข้องทั้งในระดับภูมิภาคและนานาชาติ เช่น หัวหน้าตำรวจอาเซียน หัวหน้าตำรวจภาคพื้นยุโรป องค์การตำรวจสากล นอกจากนี้ ปฏิญญาฯ ยังมีวัตถุประสงค์ในการเสริมสร้างความมั่นคงทางเทคโนโลยี การป้องกัน และความสามารถในการแก้ไขปัญหาเกี่ยวกับอาชญากรรมทางไซเบอร์ เพื่อพัฒนาขีดความสามารถของอาเซียนในการสร้างและพัฒนาศักยภาพในการต่อสู้กับอาชญากรรมทางไซเบอร์อีกด้วย

๓.๓.๒ ร่างอนุสัญญาว่าด้วยการต่อต้านอาชญากรรมไซเบอร์[๒๘]

เมื่อวันที่ ๙ สิงหาคม ๒๕๖๗ คณะผู้แทนไทย นำโดยกระทรวงการต่างประเทศ ร่วมรับรองร่างอนุสัญญาว่าด้วยการต่อต้านอาชญากรรมทางไซเบอร์ ในการประชุมเจรจาร่างอนุสัญญาฯ ระหว่างวันที่ ๒๙ กรกฎาคม - ๙ สิงหาคม ๒๕๖๗ ณ สำนักงานใหญ่สหประชาชาติ นครนิวยอร์ก โดยร่างอนุสัญญาฉบับนี้จะเป็นตราสารระหว่างประเทศฉบับแรกในกรอบสหประชาชาติที่ครอบคลุมเรื่องอาชญากรรมไซเบอร์ ซึ่งเป็นประเด็นที่มีลักษณะข้ามพรมแดนและต้องอาศัยความร่วมมือระหว่างประเทศด้านการดำเนินคดีและการบังคับใช้กฎหมายที่มีประสิทธิภาพ การเจรจาร่างอนุสัญญาฉบับนี้อยู่ภายใต้กรอบคณะกรรมการระหว่างรัฐเฉพาะกิจเพื่อจัดทำอนุสัญญาระหว่างประเทศอย่างครอบคลุมว่าด้วยการต่อต้านการใช้เทคโนโลยีและการสื่อสาร เพื่อวัตถุประสงค์ทางอาชญากรรมในกรอบสหประชาชาติ (United Nations Ad Hoc Committee (AHC) to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes) ซึ่งได้เจรจาร่างอนุสัญญาฯ มาแล้วรวม ๘ สมัย จนสามารถบรรลุฉันทามติได้ในการประชุมสมัยสรุปครั้งล่าสุด โดยจะมีการเสนอร่างอนุสัญญาฯ ให้ที่ประชุมสมัชชาสหประชาชาติครั้งที่ ๗๘ พิจารณาให้การรับรองอย่างเป็นทางการต่อไป

ทั้งนี้ ประเทศไทยให้ความสำคัญกับความร่วมมือด้านการต่อต้านอาชญากรรมไซเบอร์ และได้ส่งผู้แทนเข้าร่วมการเจรจาร่างอนุสัญญาฯ โดยในการประชุมสมัยสรุปครั้งล่าสุด คณะผู้แทนไทยได้กล่าวถ้อยแถลงแสดงความยินดีที่คณะกรรมการระหว่างรัฐเฉพาะกิจฯ สามารถรับรองร่างอนุสัญญาฯ และหวังให้อนุสัญญาฯ มีผลใช้บังคับโดยเร็ว ซึ่งจะเป็นประโยชน์ต่อประเทศไทยและนานาประเทศในการป้องกันและปราบปรามอาชญากรรมไซเบอร์ โดยเฉพาะปัญหาการหลอกลวง

---

[๒๘] กระทรวงการต่างประเทศ, ไทยร่วมรับรองร่างอนุสัญญาว่าด้วยการต่อต้านอาชญากรรมไซเบอร์, สืบค้นเมื่อวันที่ ๒๘ กุมภาพันธ์ ๒๕๖๘. จาก https://www.mfa.go.th/th/content/thai-adopt-cybercrime-th

ทางอินเตอร์เน็ต การค้ามนุษย์ และการค้ายาเสพติด เมื่อพิจารณาถึงปัญหาอาชญากรรมข้ามชาติที่มีแนวโน้มเพิ่มสูงขึ้นอย่างมากในไทยผ่านการใช้เทคโนโลยีสารสนเทศ และรัฐบาลไทยให้ความสำคัญในการแก้ไขปัญหานี้เป็นลำดับต้น

๓.๓.๓ บันทึกความเข้าใจ (MOU) ระหว่าง ไทย-กัมพูชา และไทย-ฟิลิปปินส์ เพื่อส่งเสริมความร่วมมือด้านดิจิทัลในระดับภูมิภาค[๒๙]

การประชุมรัฐมนตรีอาเซียนด้านดิจิทัล (The ๕th ASEAN Digital Ministers' Meeting: The ๕th ADGMIN) ครั้งที่ ๕ จัดขึ้นระหว่างวันที่ ๑๖ - ๑๗ มกราคม ๒๕๖๘ ณ กรุงเทพมหานคร ประเทศไทย โดยในที่ประชุมได้มีการลงนามในบันทึกความเข้าใจ (MOU) ระหว่างประเทศไทยและกัมพูชา รวมทั้งประเทศไทยและฟิลิปปินส์ เพื่อส่งเสริมความร่วมมือด้านดิจิทัลในระดับภูมิภาค โดยมุ่งเน้นประเด็นสำคัญ ได้แก่ การพัฒนากำลังคนด้านดิจิทัล ธรรมาภิบาลภาครัฐอิเล็กทรอนิกส์ และการป้องกันและการต่อสู้กับปัญหาการหลอกลวงออนไลน์ ดังนี้

MOU ไทย-กัมพูชา เป็นความร่วมมือด้านเทคโนโลยีดิจิทัลระหว่างกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งราชอาณาจักรไทย และกระทรวงการไปรษณีย์และโทรคมนาคมแห่งราชอาณาจักรกัมพูชา เพื่อเสริมสร้างความสัมพันธ์ระหว่าง ๒ ประเทศ พร้อมทั้งพัฒนาความร่วมมือในสาขาต่าง ๆ เช่น บริการแพลตฟอร์มดิจิทัล สินค้าและบริการของรัฐบาลดิจิทัล การเปลี่ยนแปลงทางดิจิทัล การสร้างโอกาสในการเข้าถึงเทคโนโลยีดิจิทัล การพัฒนากำลังคนด้านดิจิทัล และความปลอดภัยออนไลน์ รวมถึงป้องกันการหลอกลวงทางดิจิทัล

MOU ไทย-ฟิลิปปินส์ เป็นความร่วมมือระหว่างกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งราชอาณาจักรไทย และกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารแห่งสาธารณรัฐฟิลิปปินส์ เพื่อส่งเสริมความสัมพันธ์ที่มีพื้นฐานบนผลประโยชน์ร่วมกันและความเข้าใจซึ่งกันและกัน การส่งเสริมการลงทุนในโครงสร้างพื้นฐานดิจิทัล ธรรมาภิบาลภาครัฐอิเล็กทรอนิกส์ เช่น ยุทธศาสตร์รัฐบาลดิจิทัลและการใช้ปัญญาประดิษฐ์ รวมถึงระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล รวมทั้งการพัฒนาเทคโนโลยีอุบัติใหม่ เช่น คลาวด์คอมพิวติ้ง (บริการ การจัดเก็บและประมวลผลข้อมูลบนระบบออนไลน์) IoT (Internet of Things: อุปกรณ์ต่าง ๆ ที่เชื่อมต่อผ่านระบบอินเทอร์เน็ต) และข้อมูลขนาดใหญ่ นอกจากนี้ ยังให้ความสำคัญกับการส่งเสริมความมั่นคงปลอดภัยทางไซเบอร์ผ่านการแลกเปลี่ยนความรู้ ความเชี่ยวชาญ และการฝึกอบรมร่วมกัน

---

[๒๙] รัฐบาลไทย, *ไทย นำ อาเซียน ขับเคลื่อนอนาคตดิจิทัล มุ่งแก้ปัญหาหลอกลวงออนไลน์-สร้างความมั่นคงทางไซเบอร์ ในการประชุมรัฐมนตรีอาเซียนด้านดิจิทัล ครั้งที่ ๕ สู่อนาคตดิจิทัลที่ปลอดภัยและยั่งยืน*, สืบค้นเมื่อวันที่ ๒๘ กุมภาพันธ์ ๒๕๖๘. จาก https://www.thaigov.go.th/news/contents/ministry_details/๙๒๕๓๑

๓.๔ กลไกการบังคับใช้กฎหมาย

อำนาจในการตัดสินคดีการก่ออาชญากรรมที่เกิดขึ้นในโลกออนไลน์จะขึ้นอยู่กับเขตอำนาจศาล ซึ่งประกอบด้วย ๓ หลักเกณฑ์[๓๐] ดังนี้

๑) หลักเกณฑ์เชิงเขตแดน (Territorial Principle) เป็นสิทธิของรัฐในการปกครองบุคคลและทรัพย์สินที่อยู่ในเขตแดนของตน หากความผิดเกิดขึ้นในประเทศใดและผู้กระทำผิดได้กระทำการที่เป็นความผิดตามกฎหมายในประเทศ ผู้กระทำผิดย่อมต้องถูกบังคับตามกฎหมายของประเทศนั้น และศาลอาญาของประเทศนั้น ๆ ย่อมมีสิทธิในการพิจารณาคดี เช่น หากผู้กระทำผิดโพสต์เนื้อหาที่เป็นความผิดตามกฎหมายไทยในประเทศไทย แม้ว่าเนื้อหาดังกล่าวจะสามารถเข้าถึงได้จากผู้ใช้งานในประเทศอื่น ศาลไทยยังคงมีเขตอำนาจในการพิจารณาคดีและใช้กฎหมายไทยได้ หรือในกรณีที่บุคคลในประเทศไทยทำการเจาะระบบคอมพิวเตอร์ของประเทศอื่นจากประเทศไทย ซึ่งการเจาะระบบดังกล่าวเป็นความผิดตามกฎหมายไทย หากผู้เสียหายยื่นฟ้องต่อศาลไทย ศาลไทยก็มีเขตอำนาจในการพิจารณาคดีนี้ได้เช่นกัน

๒) หลักเกณฑ์เชิงบุคคล (Personality Principle) เป็นสิทธิของรัฐในการปกครองพลเมืองของตนไม่ว่าจะอยู่ที่ใดในโลก ซึ่งหลักการนี้อิงกับสัญชาติของบุคคลนั้น ๆ หากผู้กระทำความผิดเป็นพลเมืองของรัฐใด รัฐมีสิทธิในการบังคับใช้กฎหมายของตนกับผู้กระทำผิดแม้ว่าการกระทำผิดจะเกิดขึ้นนอกเขตแดนของรัฐนั้น เช่น ตามกฎหมายของประเทศไทย แม้ความผิดจะเกิดขึ้นนอกประเทศ หากผู้กระทำผิดเป็นคนไทยและรัฐบาลประเทศที่เกิดเหตุการณ์หรือผู้เสียหายร้องขอประเทศไทยสามารถบังคับใช้กฎหมายไทยกับผู้กระทำผิดนั้นได้

๓) หลักการเชิงผลลัพธ์ (Effects Principle) เป็นสิทธิของรัฐในการปกครองผลลัพธ์ทางเศรษฐกิจและกฎหมายที่เกิดขึ้นในเขตแดนของตนจากการกระทำที่เกิดขึ้นในต่างประเทศ หากผู้กระทำผิดกระทำความผิดในประเทศหนึ่งแต่เกิดผลกระทบในประเทศอื่น โดยทั่วไปแล้ว หลายประเทศจะมีกฎหมายที่ขยายหลักเขตแดนให้สามารถเอาผิดกับบุคคลดังกล่าวตามกฎหมายของประเทศที่ผลกระทบเกิดขึ้น เช่น กฎหมายอาญาของประเทศไทย หากผู้กระทำผิดกระทำการโพสต์เนื้อหาที่เป็นความผิดตามกฎหมายไทยบนอินเทอร์เน็ตจากต่างประเทศ หรือทำการเจาะระบบคอมพิวเตอร์ที่ตั้งอยู่ในประเทศไทยจากต่างประเทศ ศาลไทยยังมีเขตอำนาจในการพิจารณาคดีและใช้กฎหมายไทยได้ หากผู้กระทำผิดเดินทางเข้าสู่ประเทศไทย ในกรณีที่ผู้กระทำผิดไม่เดินทางเข้ามายังประเทศไทย การดำเนินการพิจารณาคดีอาจต้องขึ้นอยู่กับความร่วมมือระหว่างประเทศ หรือการร้องขอให้ประเทศที่ผู้กระทำความผิดอาศัยอยู่ส่งผู้ร้ายข้ามแดนมาพิจารณาคดีในประเทศไทย หรืออาจเป็นการร้องขอให้ศาลในประเทศที่ผู้กระทำผิดอาศัยอยู่ดำเนินคดีให้หากการกระทำดังกล่าวเป็นความผิดตามกฎหมายของประเทศนั้นเช่นกัน ซึ่งเป็นการปฏิบัติตามหลักเขตแดนของประเทศนั้น

---

[๓๐] คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, *ความรู้ทางกฎหมายหลากหลายและเข้าใจง่าย ชุดที่ ๒๐ : CYBER CRIME เมื่อโลกออนไลน์ เต็มไปด้วยอาชญากรรม : อาชญาวิทยาและบทบาทของกฎหมาย*, สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘. จาก https://www.law.tu.ac.th/tulawinfographic๒๐/

การกระทำความผิดในโลกออนไลน์หรือในโลกเสมือนอย่าง Metaverse อาจไม่สามารถถือเป็นความผิดตามกฎหมายอาญาของประเทศไทยได้ เนื่องจากการกระทำที่จะถือเป็นความผิดตามกฎหมายอาญาจะต้องมีวัตถุของการกระทำเป็นมนุษย์หรือบุคคลจริงเท่านั้น ตัวอย่างเช่น ความผิดในกรณีของการฆ่าหรือทำร้ายร่างกาย และการกระทำชำเรา ซึ่งไม่สามารถเกิดขึ้นได้ในโลกออนไลน์หรือโลกเสมือน แต่การกระทำที่เกี่ยวข้องกับข้อมูลที่มีมูลค่า เช่น การหลอกลวงเพื่อเข้าถึงข้อมูลหรือการทำลายข้อมูลจนเกิดความเสียหาย อาจถือเป็นความผิดตามกฎหมายคอมพิวเตอร์ได้ ดังนั้น จำเป็นต้องมีการทบทวนว่า กฎหมายที่มีอยู่ในปัจจุบันเพียงพอที่จะรับมือกับอาชญากรรมทางเทคโนโลยีที่เกิดขึ้นในโลกออนไลน์ ซึ่งคาดว่าจะมีการใช้งานเพิ่มมากขึ้นในอนาคตหรือไม่ หรือจะต้องมีการบัญญัติกฎหมายใหม่ที่เฉพาะเจาะจงเพื่อควบคุมการกระทำเหล่านี้โดยตรง

๓.๕ บทบาทและหน้าที่ของหน่วยงานที่เกี่ยวข้อง[๓๑]

การดำเนินการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีในปัจจุบันยังคงดำเนินการแยกตามบทบาท หน้าที่ และอำนาจของแต่ละหน่วยงานที่กำหนดโดยกฎหมาย ซึ่งยังไม่มีการบูรณาการอย่างเต็มที่ ทำให้ประชาชนที่ประสบปัญหาต้องติดต่อหน่วยงานหลายแห่ง จึงเกิดความไม่สะดวกและใช้เวลาในการแก้ไขปัญหาที่ซับซ้อนที่เกี่ยวข้องกับหลายหน่วยงานเป็นระยะเวลานาน ปัจจุบันหน่วยงานที่เกี่ยวข้องกับการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยี มีดังนี้

๑) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ดศ.) มีอำนาจในการปิดกั้นเว็บไซต์ และเรียกพยานหลักฐานเกี่ยวกับข้อมูลจราจรทางคอมพิวเตอร์ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม รวมถึงการบูรณาการและขับเคลื่อนการแก้ไขปัญหาการฉ้อโกงออนไลน์ในรูปแบบของคณะกรรมการระดับชาติร่วมกับภาคีหน่วยงานที่เกี่ยวข้อง

๒) สำนักงานตำรวจแห่งชาติ (สตช.) ป้องกันและปราบปรามการกระทำความผิดอาญาตามประมวลกฎหมายวิธีพิจารณาความอาญา และเป็นพนักงานเจ้าหน้าที่ตามกฎหมายที่ได้รับแต่งตั้งดำเนินคดีต่อผู้กระทำความผิดตามกระบวนการยุติธรรม โดยได้จัดตั้งกองบัญชาการสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (CCIB) หรือกองบัญชาการตำรวจไซเบอร์ตามพระราชกฤษฎีกาแบ่งส่วนราชการสำนักงานตำรวจแห่งชาติ (ฉบับที่ ๕) พ.ศ. ๒๕๖๓ เพื่อวางแผนและควบคุมการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีทั่วประเทศ พร้อมทั้งพิสูจน์หลักฐานและเก็บรวบรวมพยานหลักฐานทางดิจิทัล

๓) ธนาคารแห่งประเทศไทย (ธปท.) กำกับและตรวจสอบสถาบันการเงินตามพระราชบัญญัติธนาคารแห่งประเทศไทย พ.ศ. ๒๔๘๕ ที่แก้ไขเพิ่มเติม กำหนดมาตรการการจัดการภัยทุจริตทางการเงินเพื่อให้สถาบันการเงินดำเนินการตามมาตรฐานเดียวกันในการบริหารจัดการความเสี่ยงจากการทำธุรกรรมทางการเงิน

---

[๓๑] สัจจะ โชคบุญส่งสวัสดิ์, “แนวทางการเพิ่มประสิทธิภาพในการตัดวงจรอาชญากรรมออนไลน์,” หลักสูตรนักบริหารระดับสูง : ผู้นำที่มีวิสัยทัศน์และคุณธรรม รุ่นที่ ๙๘ วิทยาลัยนักบริหาร สถาบันพัฒนาข้าราชการพลเรือน สำนักงาน ก.พ., ๒๕๖๖.

๔) สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) กำกับดูแลกิจการโทรคมนาคมให้เป็นไปตามกฎหมาย และดำเนินคดีผู้กระทำผิดเกี่ยวกับกิจการโทรคมนาคม โดยการปิดเบอร์โทรศัพท์ที่ผิดกฎหมายที่ไม่สามารถแสดงตัวตนได้

๕) สำนักงานคณะกรรมการป้องกันและปราบปรามการฟอกเงิน (ปปง.) ตรวจสอบและวิเคราะห์ข้อมูลทางการเงินที่เกี่ยวข้องกับการฟอกเงินตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. ๒๕๕๒ เพื่อเฝ้าระวังบุคคลที่มีความเสี่ยงสูง

๖) สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (กลต.) กำกับดูแลตลาดทุนตามพระราชบัญญัติหลักทรัพย์และตลาดหลักทรัพย์ พ.ศ. ๒๕๓๕ และที่แก้ไขเพิ่มเติม โดยการออกใบอนุญาตและจดทะเบียนผู้ให้บริการในตลาดทุน

๗) กรมสอบสวนคดีพิเศษ (ดีเอสไอ) ป้องกัน ปราบปราม และควบคุมอาชญากรรมที่มีผลกระทบต่อเศรษฐกิจ สังคม ความมั่นคง และความสัมพันธ์ระหว่างประเทศ ตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. ๒๕๔๗

๘) สำนักงานคณะกรรมการคุ้มครองผู้บริโภค (สคบ.) กำกับดูแลการซื้อสินค้าออนไลน์ตามพระราชบัญญัติขายตรงและตลาดแบบตรง พ.ศ. ๒๕๔๕ ซึ่งผู้บริโภคมีสิทธิในการเลิกสัญญาหรือขอคืนสินค้าได้ภายใน ๗ วัน นับแต่วันที่ได้รับสินค้า โดยผู้บริโภคต้องทำหนังสือแจ้งการขอคืนสินค้าและส่งทางไปรษณีย์ลงทะเบียนตอบรับไปยังผู้ประกอบธุรกิจ พร้อมทั้งเก็บเอกสารการซื้อ-ขายและสินค้าที่ต้องการขอคืนไว้ในระยะเวลาไม่เกิน ๒๑ วัน นับแต่วันที่ใช้สิทธิขอคืนสินค้า

อย่างไรก็ตาม ที่ผ่านมาพบว่ากฎหมายที่เกี่ยวข้องกับการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีที่เกิดขึ้นยังมีมาตรการบังคับทางกฎหมายที่ไม่เพียงพอที่จะรับมือกับรูปแบบอาชญากรรมทางเทคโนโลยีที่พัฒนาขึ้นโดยกลุ่มมิจฉาชีพ จึงควรเร่งพัฒนาและปรับปรุงกฎหมายปัจจุบันให้ทันสมัย เหมาะสม และครอบคลุมกับสถานการณ์ในยุคดิจิทัลที่อาชญากรรมทางเทคโนโลยีสามารถเกิดขึ้นในหลากหลายรูปแบบ เช่น การเร่งคืนเงินให้แก่ผู้เสียหาย การอายัดบัญชีม้า การกำหนดหน้าที่และความรับผิดชอบของสถาบันการเงินและผู้ให้บริการเครือข่ายโทรศัพท์ รวมถึงมาตรการการโอนเงินผิดกฎหมายผ่านสินทรัพย์ดิจิทัล ซึ่งจะเป็นเครื่องมือทางกฎหมายที่สามารถบังคับใช้เพื่อให้หน่วยงานที่เกี่ยวข้องเร่งรัดการกวาดล้างอาชญากรรมทางเทคโนโลยี และช่วยติดตามควบคุมการบรรเทาความเดือดร้อนของประชาชน เพื่อลดปัญหาสังคมและผลกระทบต่อระบบเศรษฐกิจของประเทศ การดำเนินการดังกล่าวไม่สามารถรอดำเนินการได้ตามวิธีการแก้ไขปรับปรุงกฎหมายในลักษณะปกติ เนื่องจากกระบวนการและขั้นตอนอาจทำให้ประชาชนไม่ได้รับการเยียวยาความเสียหายในเวลาอันสมควร ดังนั้น รัฐจึงต้องเร่งดำเนินการให้มีมาตรการป้องกันอาชญากรรมทางเทคโนโลยีอย่างเร่งด่วน เพื่อแก้ปัญหาช่องว่างทางกฎหมายที่ทำให้เกิดความเสียหายแก่ประชาชนและระบบเศรษฐกิจของประเทศ โดยจะช่วยลดความเสียหายที่เกิดขึ้นจากการหลอกลวงของมิจฉาชีพทางออนไลน์ได้อย่างเป็นรูปธรรมต่อไป

บทที่ ๔
ถอดบทเรียนความสำเร็จการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยี

การแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีเป็นเรื่องที่ทุกองค์กรควรให้ความสำคัญ เพราะการก่ออาชญากรรมทางเทคโนโลยีหรืออาชญากรรมไซเบอร์ในปัจจุบันนั้นมีการพัฒนารูปแบบการกระทำผิดมากขึ้นเรื่อย ๆ ตามความก้าวหน้าของเทคโนโลยี มีวิวัฒนาการหลากหลายรูปแบบ ซึ่งส่งผลกระทบได้อย่างรวดเร็วและเป็นวงกว้าง หลายประเทศทั่วโลกมีการยกระดับและพัฒนาระบบกฎหมายในการควบคุมอาชญากรรมทางเทคโนโลยีให้ทันสมัยและทันต่อภัยคุกคามทางเทคโนโลยี โดยภาครัฐและภาคเอกชนต้องมีการเตรียมพร้อมและบริหารจัดการความเสี่ยงที่อาจเกิดขึ้น การวางแผนสำรองข้อมูลเมื่อถูกจู่โจม และความเข้มงวดของกฎหมาย การศึกษาและถอดบทเรียนการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีของต่างประเทศจะช่วยสร้างกลไกในการพัฒนาและควบคุมระบบกฎหมายและเจ้าหน้าที่ให้ดำเนินการได้อย่างเหมาะสม เพื่อเป็นแนวทางในการพัฒนามาตรการทางกฎหมายและนโยบายในการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีของประเทศไทยต่อไป ซึ่งการเติบโตของเทคโนโลยีทำให้ระบบสารสนเทศและโครงสร้างพื้นฐานต่าง ๆ เชื่อมต่อกันมากขึ้น ซึ่งสร้างโอกาสให้กับอาชญากรทางเทคโนโลยี หรืออาชญากรไซเบอร์ จะโจมตีได้ในรูปแบบต่าง ๆ เช่น การโจมตีแบบ Ransomware การโจมตีแบบ Phishing และการโจมตีแบบ DDoS เป็นต้น โดยการโจมตีทางไซเบอร์สามารถส่งผลกระทบต่อทั้งภาครัฐ ภาคเอกชน และประชาชนทั่วไป ที่จะสามารถก่อให้เกิดความเสียหายต่อระบบทางเศรษฐกิจ สังคม หรือความมั่นคงของประเทศได้

หลายประเทศทั่วโลกตระหนักถึงความสำคัญในการกำกับดูแล ตลอดจนออกนโยบายแนวทางในการรับมือกับการโจมตีทางไซเบอร์ เช่นเดียวกับทางสหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union หรือ ITU) องค์กรระหว่างประเทศที่มีหน้าที่ส่งเสริมการพัฒนาเทคโนโลยีโทรคมนาคมและสารสนเทศ ITU ได้ให้ความสำคัญของความมั่นคงปลอดภัยไซเบอร์ จึงมีบทบาทในการส่งเสริมความมั่นคงปลอดภัยไซเบอร์ให้กับประเทศต่าง ๆ ทั่วโลก ผ่านการจัดประเมิน Global Cybersecurity Index หรือ GCI ที่จะช่วยให้ประเทศต่าง ๆ สามารถพัฒนากลยุทธ์และนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพ[๓๒] โดยดัชนีด้านความมั่นคงปลอดภัยไซเบอร์มีรูปแบบการประเมินเป็นกรอบคำถามตามสหภาพโทรคมนาคมระหว่างประเทศ (ITU) โดยมีคะแนน ๑๐๐ คะแนนเต็ม ซึ่งพิจารณาจากปัจจัยหลัก ๕ ด้าน[๓๓] ประกอบด้วย

---

[๓๒] สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน), *รายงานความมั่นคงปลอดภัยทางไซเบอร์ของโลก (Global Cybersecurity Index)*, สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘. จาก https://www.dga.or.th/wp-content/uploads/๒๐๒๑/๐๒/๗.pdf

[๓๓] International Telecommunication Union (ITU), *GCI scope and framework*, สืบค้นเมื่อวันที่ ๑๙ กุมพันธ์ ๒๕๖๘. จาก https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv๔/New_Reference_Model_GCIv๔_V๒_.pdf

๑) ด้านกฎหมาย (Legal Measure) เป็นมาตรการการประเมินความครอบคลุมและประสิทธิภาพของกฎหมายและกฎระเบียบด้านความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ โดยพิจารณาจากหน่วยงานและกรอบกฎหมายที่มีอยู่ เช่น การมีกฎหมายด้านความมั่นคงปลอดภัยทางไซเบอร์ที่ครอบคลุม เป็นต้น

๒) ด้านมาตรการทางเทคนิค (Technical Measure) เป็นการประเมินความพร้อมด้านโครงสร้างพื้นฐานและเทคโนโลยีด้านความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ โดยพิจารณาจากหน่วยงานและกรอบทางเทคโนโลยีที่มีอยู่ เช่น การมีเทคโนโลยีด้านความมั่นคงปลอดภัยทางไซเบอร์ที่ทันสมัย เป็นต้น

๓) ด้านหน่วยงาน/นโยบาย (Organizational Measure) เป็นการประเมินความพร้อมของหน่วยงานและนโยบายด้านความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ โดยพิจารณาจากหน่วยงานประสานงานนโยบายและกลยุทธ์การพัฒนาความมั่นคงปลอดภัยไซเบอร์ระดับชาติที่มีอยู่ เช่น การมีหน่วยงานรับผิดชอบด้านความมั่นคงปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพ มีนโยบายและแผนงานด้านความมั่นคงปลอดภัยทางไซเบอร์ที่ชัดเจน เป็นต้น

๔) ด้านการพัฒนาศักยภาพ (Capacity Development Measure) เป็นการประเมินความพร้อมของบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ โดยพิจารณาจากการวิจัยและพัฒนา รวมถึงโปรแกรมการศึกษาและการฝึกอบรม และผู้เชี่ยวชาญที่ผ่านการรับรองที่มีอยู่ เช่น การมีระบบการศึกษาและการฝึกอบรมด้านความมั่นคงปลอดภัยทางไซเบอร์ที่มีคุณภาพ การมีบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ที่มีทักษะและความรู้ที่เพียงพอ เป็นต้น

๕) ด้านความร่วมมือ (Cooperative Measure) เป็นการประเมินความร่วมมือระหว่างประเทศด้านความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ โดยพิจารณาจากความร่วมมือต่างๆ เช่น การมีความร่วมมือระหว่างประเทศด้านความมั่นคงปลอดภัยทางไซเบอร์ที่ครอบคลุม มีกลไกในการแลกเปลี่ยนข้อมูลและความร่วมมือระหว่างประเทศด้านความมั่นคงปลอดภัยทางไซเบอร์ เป็นต้น

ทั้งนี้ การประเมินความมั่นคงปลอดภัยไซเบอร์จะต้องอาศัยความร่วมมือจากภาครัฐ ภาคเอกชน และประชาชน โดยเริ่มพัฒนาจากปัจจัยที่มีความสำคัญในการเร่งพัฒนามากที่สุด คือ ด้านมาตรการทางเทคนิค (Technical Measures) และด้านอื่น ๆ ตามมา เพื่อพัฒนาการรับมือกับภัยคุกคามทางไซเบอร์ และเพื่อยกระดับภาพลักษณ์ของประเทศ โดยดัชนีความมั่นคงปลอดภัยไซเบอร์ หรือ GCI ถือเป็นเครื่องมือสำคัญที่ช่วยให้ประเทศไทยและประเทศอื่น ๆ สามารถประเมินความสามารถในการแข่งขันของตนเอง และนำไปสู่การปรับแผนนโยบายและกลยุทธ์เพื่อเพิ่มขีดความสามารถในการแข่งขันของประเทศ รวมถึงการประเมินความมั่นคงปลอดภัยไซเบอร์นี้จะช่วยชี้แนะว่าประเทศเรานั้นควรเร่งพัฒนาที่ด้านไหนเป็นพิเศษ นำมาซึ่งการเป็นประเทศชั้นนำด้านความมั่นคงปลอดภัยไซเบอร์สู่การขับเคลื่อนเศรษฐกิจระดับระหว่างประเทศได้ในอนาคต

๔.๑ การแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีของประเทศสิงคโปร์

จากการศึกษารายงาน Global Cybersecurity Index ปี ๒๐๒๔ พบว่าอันดับประเทศที่มีการดำเนินนโยบายด้านความมั่นคงปลอดภัยทางไซเบอร์ได้ผลสำเร็จสูงสุดในอาเซียน อันดับหนึ่ง คือ

ประเทศอินโดนีเซีย โดยได้คะแนนจากตัวชี้วัดทั้ง ๕ ด้าน รวมเป็น ๑๐๐ (จากจำนวนเต็ม ๑๐๐) อันดับสอง คือ สาธารณรัฐสิงคโปร์ ได้คะแนนรวม ๙๙.๘๖ และอันดับที่สาม คือ ประเทศเวียดนาม ได้คะแนนรวม ๙๙.๗๔ รายละเอียดปรากฏตามตารางที่ ๒

ตารางที่ ๒ ลำดับประเทศในอาเซียนในการดำเนินการทั้ง ๕ ด้านของ GCI ปี ๒๐๒๔

ประเทศ	ตัวชี้วัดผลสัมฤทธิ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์					รวม (คะแนนเต็ม ๑๐๐)	อันดับอาเซียน
	ด้านกฎหมาย	ด้านเทคนิค	ด้านหน่วยงาน/นโยบาย	ด้านการพัฒนาศักยภาพ	ด้านความร่วมมือ		
อินโดนีเซีย	๒๐.๐๐	๒๐.๐๐	๒๐.๐๐	๒๐.๐๐	๒๐.๐๐	๑๐๐.๐๐	๑
สิงคโปร์	๒๐.๐๐	๒๐.๐๐	๒๐.๐๐	๑๙.๘๖	๒๐.๐๐	๙๙.๘๖	๒
เวียดนาม	๒๐.๐๐	๒๐.๐๐	๒๐.๐๐	๑๙.๗๔	๒๐.๐๐	๙๙.๗๔	๓
ไทย	๒๐.๐๐	๒๐.๐๐	๑๙.๒๒	๒๐.๐๐	๒๐.๐๐	๙๙.๒๒	๔
มาเลเซีย	๒๐.๐๐	๒๐.๐๐	๑๘.๘๒	๒๐.๐๐	๒๐.๐๐	๙๘.๘๒	๕
ฟิลิปปินส์	๒๐.๐๐	๑๙.๑๑	๑๙.๕๑	๑๗.๑๗	๑๗.๗๐	๙๓.๔๙	๖
บรูไนดารุสซาลาม	๑๗.๒๐	๑๗.๘๙	๑๑.๓๕	๑๐.๗๖	๑๖.๑๘	๗๓.๓๘	๗
เมียนมา	๑๕.๓๔	๑๐.๙๐	๑๓.๐๖	๑๔.๔๒	๒๐.๐๐	๗๓.๗๓	๘
กัมพูชา	๑๑.๘๒	๔.๕๖	๘.๓๐	๖.๑๒	๖.๒๒	๓๗.๐๒	๙
สปป.ลาว	๑๐.๓๘	๖.๑๘	๕.๕๒	๒.๐๕	๙.๖๑	๓๓.๗๔	๑๐

ที่มา : สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน), รายงานความมั่นคงปลอดภัยทางไซเบอร์ของโลก (Global Cybersecurity Index), สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘. จาก https://www.dga.or.th/wp-content/uploads/๒๐๒๑/๐๒/๗.pdf

๔.๑.๑ ถอดบทเรียนผลการวิเคราะห์ปัจจัยความสำเร็จของสิงคโปร์ ตามตัวชี้วัดหลักทั้ง ๕ ด้าน มีดังนี้

๑) ด้านกฎหมาย (Legal Measures)

จากการศึกษา พบว่ารัฐบาลสิงคโปร์ให้ความสำคัญกับการออกกฎหมาย กฎระเบียบที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างครอบคลุม เนื่องจากเป็นเครื่องมือสำคัญในการดำเนินการและเป็นกรอบกฎหมายที่กำหนดนโยบาย ขั้นตอนดำเนินการและแนวทางปฏิบัติ เพื่อให้หน่วยงานที่เกี่ยวข้องดำเนินการ โดยมีแผนแม่บทและกฎหมายอื่น

ที่เกี่ยวข้องไม่ว่าจะเป็นกฎหมายเกี่ยวกับการแทรกแซงระบบคอมพิวเตอร์ กฎหมายเกี่ยวกับข้อมูล รวมทั้งการกำหนดกฎระเบียบหรือแนวทางปฏิบัติเกี่ยวกับการป้องกันข้อมูล การแจ้งเมื่อมีการละเมิดข้อมูล การให้ประกาศนียบัตรหรือใบรับรองด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ มาตรฐานการตรวจสอบรับรองด้านความมั่นคงปลอดภัยไซเบอร์ การคุ้มครองข้อมูลส่วนบุคคล การโอนเงินและการทำธุรกรรมอิเล็กทรอนิกส์ โดยรัฐบาลสิงคโปร์ได้มีการแก้ไขและออกกฎหมายและกฎระเบียบอย่างต่อเนื่อง และให้ความสำคัญกับขั้นตอนก่อนการตรากฎหมายหรือกฎระเบียบต่าง ๆ โดยมีการหารือและทำการศึกษากับทุกภาคส่วนที่เกี่ยวข้อง รวมทั้งนักวิชาการ นักเทคนิค สถาบันการศึกษา และสถาบันวิจัย

แผนแม่บทและกฎหมายที่สำคัญของสิงคโปร์ ได้แก่ แผนแม่บทด้านความมั่นคงปลอดภัยไซเบอร์ฉบับแรก คือ Infocom Security Masterplan ๒๐๐๕–๒๐๐๗ ซึ่งมีสาระสำคัญในการประสานงานระหว่างหน่วยงานของรัฐเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ โดยให้ความสำคัญในลำดับแรก คือ การเสริมสร้างความสามารถของหน่วยงานภาครัฐในการบรรเทาและรับมือกับภัยคุกคามทางไซเบอร์ ต่อมาในปี ๒๐๐๘ ได้ประกาศแผนแม่บทการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติฉบับที่ ๒ สำหรับช่วงปี ๒๐๐๘–๒๐๑๒ ซึ่งมุ่งเน้นการรักษาความมั่นคงปลอดภัยของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Infrastructure Information หรือ CII) ของสิงคโปร์ ในปี ๒๐๑๓ สิงคโปร์ได้ประกาศใช้แผนแม่บทการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติฉบับที่ ๓ ซึ่งครอบคลุมระบบนิเวศสารสนเทศและการสื่อสารในวงกว้างมากขึ้น รวมถึงภาคเอกชนและบุคคลทั่วไป ไม่จำกัดเฉพาะ CII เพื่อให้สิงคโปร์กลายเป็นศูนย์กลางสารสนเทศและการสื่อสารที่มีความมั่นคงและแข็งแกร่ง นอกจากนี้ สิงคโปร์ยังได้ประกาศใช้แผนปฏิบัติการต่อต้านอาชญากรรมไซเบอร์แห่งชาติ (National Cybercrimes Action Plan) ในเดือนกรกฎาคม ๒๐๑๖ โดยกระทรวงกิจการภายใน ในปี ๒๐๑๗ สิงคโปร์ได้ทำการแก้ไขกฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์และการใช้คอมพิวเตอร์ในทางที่ผิด (Computer Misuse and Cybersecurity Act) และเมื่อวันที่ ๒ มีนาคม ๒๐๑๘ กฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Act) ได้มีผลบังคับใช้ ซึ่งเป็นกรอบกฎหมายสำคัญในการรักษาความมั่นคงปลอดภัยไซเบอร์ ในปี ๒๐๒๔ สิงคโปร์ได้ปรับปรุงกฎหมายความมั่นคงทางไซเบอร์ (Cybersecurity Act) ให้มีความเข้มแข็งมากยิ่งขึ้น เพื่อปกป้องและรักษาความมั่นคงปลอดภัยของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยขยายขอบเขตหน้าที่ของหน่วยงานรักษาความปลอดภัยทางไซเบอร์ของสิงคโปร์ (Cyber Security Agency of Singapore – CSA) ให้สามารถตรวจสอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของกิจการในบางสาขาเศรษฐกิจ รวมทั้งควบคุมหรือยับยั้งการโจมตีทางไซเบอร์ ซึ่งทำให้คะแนนของสิงคโปร์ในส่วนของตัวชี้วัดด้านกฎหมายในปี ๒๐๒๔ ได้คะแนนเต็ม ๒๐ คะแนน นอกจากนี้ สิงคโปร์ยังอยู่ระหว่างการร่างกฎหมาย Digital Infrastructure Act[๓๔] ซึ่งมุ่งเน้นการบริหารจัดการความเสี่ยง

[๓๔] ไทยพับลิก้า, *สิงคโปร์แก้ไขกฎหมายความปลอดภัยไซเบอร์ยกระดับการกำกับดูแลผลประโยชน์ประเทศ*, สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘. จาก https://thaipublica.org/๒๐๒๔/๐๕/asean-weekly-roundup-๒๔๙/

ที่อาจเกิดขึ้นต่อโครงสร้างพื้นฐานด้านดิจิทัลและผู้ให้บริการทางดิจิทัลที่อาจส่งผลให้การใช้งานระบบหยุดชะงัก โดยครอบคลุมตั้งแต่ข้อผิดพลาดทางเทคนิคไปจนถึงอันตรายทางกายภาพ เช่น ไฟไหม้ เป็นต้น[๓๕]

๒) ด้านเทคนิค (Technical Measures)

จากการศึกษา พบว่าปัจจัยความสำเร็จของสิงคโปร์ในด้านเทคนิค ประกอบด้วย (๑) รัฐบาลให้การสนับสนุนงบประมาณในการส่งเสริมโครงการต่าง ๆ ที่จะพัฒนาด้านเทคนิค ส่งเสริมการศึกษาและวิจัย รวมทั้งการนำเทคโนโลยีที่ทันสมัยมาใช้ (๒) มีศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (Computer Emergency Response Team: CERT) เพื่อเตรียมรับมือกับสถานการณ์จริง และเหตุเกี่ยวกับความปลอดภัยทางไซเบอร์[๓๖] (๓) มีกรอบมาตรฐานการดำเนินการด้านความปลอดภัยทางไซเบอร์สำหรับหน่วยงานต่าง ๆ และการมีองค์กรที่จัดทำด้านมาตรฐาน (๔) ภาครัฐและภาคเอกชนร่วมมือและทำงานร่วมกันอย่างใกล้ชิดและต่อเนื่อง รวมทั้งการจัดหาพันธมิตรใหม่ ๆ เพื่อพัฒนามาตรฐานความมั่นคงปลอดภัยไซเบอร์ และ (๕) พัฒนาการจัดทำ Best Practice Guideline สำหรับการให้บริการรักษาความปลอดภัย เพื่อให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ทุกสาขา ได้ใช้เป็นแนวทางปฏิบัติ

รัฐบาลสิงคโปร์ตระหนักและให้ความสำคัญกับการพัฒนาเทคโนโลยีการสื่อสารโทรคมนาคมและเทคโนโลยีใหม่ ๆ เพื่อให้เท่าทันและสามารถป้องกันและรับมือกับภัยคุกคามไซเบอร์ โดยการจัดสรรงบประมาณในการส่งเสริมโครงการต่าง ๆ ที่จะพัฒนาด้านเทคนิค ส่งเสริมการศึกษาและวิจัย รวมทั้งการนำเทคโนโลยีที่ทันสมัยมาใช้ เพื่อป้องกันระบบข้อมูลของหน่วยงานภาครัฐ นอกจากนี้ สิงคโปร์ยังกระตุ้นให้หน่วยงานภาครัฐและเอกชนจัดสรรเงินจำนวนร้อยละ ๘ ของงบประมาณในส่วนเทคโนโลยีสารสนเทศ (IT) เพื่อใช้สำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งถือว่าเป็นการลงทุนในการจัดการความเสี่ยง ปัจจัยสำคัญอีกประการหนึ่งที่สิงคโปร์ประสบความสำเร็จในตัวชี้วัดเทคนิค คือ การมีศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศสิงคโปร์ (SingCERT) ซึ่งมีหน้าที่ประกาศเตือนและแนะนำการปฏิบัติงานเชิงเทคนิคเมื่อเกิดเหตุ ส่งเสริมการสร้างความตระหนักรู้ผ่านการสัมมนา ประชุมปฏิบัติการ และการซ้อมรับมือกับสถานการณ์จริง (Cyber Drills) และร่วมมือกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์อื่น ๆ เพื่อรับมือกับเหตุเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ อีกทั้งยังพบว่าภาครัฐและภาคเอกชนของสิงคโปร์ได้ร่วมมือและทำงานร่วมกันอย่างใกล้ชิดและต่อเนื่อง รวมทั้งมีพันธมิตรใหม่เพิ่มขึ้นในการพัฒนาและนำมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์มาลดช่องว่างมาตรฐานความมั่นคงปลอดภัยไซเบอร์

---

[๓๕] สถานเอกอัครราชทูต ณ สิงคโปร์, *ศูนย์ข้อมูลเพื่อธุรกิจไทย (BIC), สิงคโปร์ยกระดับระบบดิจิทัลเพื่อความมั่นคงทางไซเบอร์*, สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘. จาก https://thaibizsingapore.com/news/main/strategies/reinforce-cybersecurity/

[๓๖] Cyber Security Agency of Singapore (CSA), *About Singapore Cyber Emergency Response Team (SingCERT)*, สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘. จาก https://www.csa.gov.sg/resources/singcert

๓) ด้านองค์กร (Organizational Measure)

สิงคโปร์มีพัฒนาการในการจัดตั้งองค์กรหรือหน่วยงานที่กำหนดนโยบาย มีการกำหนดยุทธศาสตร์การพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศ รวมทั้งมีหน่วยงานที่รับผิดชอบการรับมือกับภัยคุกคามไซเบอร์ได้อย่างครอบคลุมและมีการประสานงานข้ามองค์กรระหว่างหน่วยงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ทำให้การดำเนินนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ของสิงคโปร์ประสบความสำเร็จบรรลุตามเป้าหมายและแผนยุทธศาสตร์ระดับชาติ นอกจากนี้ สิงคโปร์ยังมีหน่วยงานอื่น ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ทั้งภาครัฐและเอกชน โดยเฉพาะอย่างยิ่งหน่วยงานที่เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ซึ่งตามกฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์ของสิงคโปร์ได้กำหนดไว้ ได้แก่ พลังงาน น้ำ การเงินและการธนาคาร ระบบดูแลสุขภาพ การขนส่ง (บก น้ำ อากาศ) สารสนเทศและการสื่อสาร สื่อ ความมั่นคงปลอดภัยและการให้บริการฉุกเฉิน และรัฐบาลโดยหน่วยงานที่เกี่ยวข้องต่าง ๆ ของสิงคโปร์ได้ปฏิบัติตามกฎระเบียบที่เกี่ยวข้องอย่างเคร่งครัด ทำให้ระบบการรักษาความมั่นคงปลอดภัยไซเบอร์ของสิงคโปร์เป็นไปอย่างมีประสิทธิภาพ แม้จะมีช่องโหว่อยู่บ้างแต่ก็สามารถรับมือได้อย่างทันท่วงที ทำให้ลดความเสียหายที่จะเกิดขึ้น

๔) ด้านการเสริมสร้างศักยภาพ (Capacity Building)

ตัวชี้วัดด้านการเสริมสร้างศักยภาพจะพิจารณาจากการรณรงค์สร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่สาธารณะชน การส่งเสริมเรื่องมาตรฐานความมั่นคงปลอดภัยไซเบอร์ และการให้ใบรับรองแก่ผู้เชี่ยวชาญ/ผู้ชำนาญการในเรื่องดังกล่าว การฝึกอบรมให้แก่ผู้เชี่ยวชาญ/ผู้ชำนาญการด้านความมั่นคงปลอดภัยไซเบอร์ การมีหลักสูตรในสถาบันการศึกษาและในโปรแกรมการศึกษาของประเทศ การมีโครงการศึกษาวิจัยและการพัฒนา (R&D) การมีมาตรการส่งเสริมแรงจูงใจ และการส่งเสริมภาคอุตสาหกรรมเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ให้เติบโตในประเทศ ซึ่งสิงคโปร์ได้มีการดำเนินนโยบายในเรื่องนี้อย่างจริงจังและต่อเนื่อง[๓๗] รัฐบาลสิงคโปร์ทำงานใกล้ชิดกับภาคอุตสาหกรรมและสถาบันการศึกษาในการริเริ่มโครงการต่าง ๆ ที่ส่งเสริมการเติบโตและพัฒนาสายงานอาชีพด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับการวิจัยและพัฒนาสิงคโปร์ได้ดำเนินการ ดังนี้

๑) พัฒนาความสามารถในเรื่องความปลอดภัย Cyber–Physical Systems และเทคโนโลยี Blockchain สำหรับอุตสาหกรรมโลจิสติกส์

๒) จัดทำกฎเกณฑ์การประเมินผลที่ทำให้ง่ายขึ้นในการรับรองมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ IoT และผลิตภัณฑ์อื่น ๆ ที่เกี่ยวข้อง

๓) สนับสนุนการเติบโตและการพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์ในกลุ่มผู้ประกอบการตั้งต้น (Startup) ซึ่งเป็นตัวขับเคลื่อนสำคัญในเศรษฐกิจดิจิทัล

---

[๓๗] นงลักษณ์ อัจนปัญญา, *มหาวิทยาลัยสิงคโปร์จับมือหน่วยงานรัฐตั้งศูนย์ความปลอดภัยไซเบอร์*, สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘. จาก https://www.eef.or.th/news-ntu-singapore-and-csa-singapore-launch-joint-centre-for-cybersecurity-evaluation/

ปัจจัยสำคัญในการเสริมสร้างศักยภาพอีกประการหนึ่งคือ การสร้างความตระหนักรู้แก่ประชาชนเกี่ยวกับภัยคุกคามทางไซเบอร์และการจัดการกับภัยคุกคามดังกล่าว สิงคโปร์ได้ให้ความสำคัญเป็นอันดับแรกในการให้ความรู้เกี่ยวกับการปฏิบัติที่สามารถป้องกันข้อมูลและทำให้เครื่องมืออุปกรณ์ดิจิทัลสะอาดปลอดภัยจากไวรัสไซเบอร์ เช่น การตั้งรหัสผ่านที่มีความซับซ้อนยากต่อการเข้าถึง การสำรองข้อมูลอย่างสม่ำเสมอ การอัพเดตและอัพเกรดซอฟต์แวร์และฮาร์ดแวร์อย่างต่อเนื่อง และการจำกัดการเข้าถึงระบบที่มีความสำคัญ นอกจากนี้ สิงคโปร์ยังให้ความสำคัญกับการเตรียมกำลังคนด้านไซเบอร์ โดยได้จัดทำแผนระดับชาติว่าด้วยการส่งเสริมการเพิ่มศักยภาพบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ (National Cyber Security Capacity and Capacity Building Plan) รวมทั้งการกำหนดให้มีหลักสูตรเกี่ยวกับความปลอดภัยทางไซเบอร์ (Cybersecurity) ทั้งในระดับโรงเรียนและสถาบันการศึกษาขั้นสูง ตลอดจนการจัดให้มีการเรียนรู้ ฝึกอบรม และพัฒนาทักษะสำหรับผู้เชี่ยวชาญและบุคคลทั่วไป ทั้งในส่วนของภาครัฐและเอกชน

๕) ด้านความร่วมมือ (Cooperation)

สหภาพโทรคมนาคมระหว่างประเทศ (ITU) ได้ทำการวิเคราะห์และให้คะแนนตัวชี้วัดจากหุ้นส่วนพันธมิตร กรอบความร่วมมือ และเครือข่ายในการแบ่งปันข้อมูลที่มีอยู่จริง โดยได้แบ่งตัวชี้วัดย่อยออกเป็น ๕ ด้าน ได้แก่ (๑) การจัดทำความตกลงทวิภาคีว่าด้วยความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ (๒) การจัดทำข้อตกลงและ/หรือการเข้าร่วมความตกลงพหุภาคี (๓) การเข้าร่วมในเวทีระหว่างประเทศ (๔) ความร่วมมือระหว่างภาครัฐและเอกชน และ (๕) ความร่วมมือกับหน่วยงานระหว่างประเทศ และการมีแบบปฏิบัติที่ดีด้านความมั่นคงปลอดภัยไซเบอร์ จากการศึกษาพบว่า สิงคโปร์มีการจัดทำความตกลงทวิภาคีว่าด้วยความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์กับประเทศต่าง ๆ รวมถึงการจัดทำข้อตกลงและ/หรือการเข้าร่วมความตกลงพหุภาคีที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ นอกจากนี้ สิงคโปร์ยังได้เข้าร่วมและมีบทบาทสำคัญในเวทีระหว่างประเทศ เช่น การมีความร่วมมือกับ UN Open–Ended Working Group (OEWG) on ICT Security ซึ่งสิงคโปร์เป็นประธาน เพื่อพัฒนาและดำเนินการตามกฎระเบียบในด้าน Cyberspace สิงคโปร์ยังเป็นสมาชิกของ Counter–Ransomware Initiative (CRI) เพื่อร่วมกันต่อสู้กับ Ransomware และในปี ๒๐๒๔ สิงคโปร์ได้ลงนามบันทึกความเข้าใจว่าด้วยการยอมรับร่วมต่อระดับความปลอดภัยของอุปกรณ์ IT ระหว่างกัน (MOU on Cybersecurity Labelling) กับเกาหลีใต้และเยอรมนี เพื่อช่วยลดค่าใช้จ่ายในการตรวจสอบอุปกรณ์ IT อำนวยความสะดวกในการเข้าถึงตลาดระหว่างกัน และสร้างความมั่นใจต่อผู้ใช้และผู้ผลิต[๓๘]

[๓๘] ศูนย์ข้อมูลเพื่อธุรกิจไทยในสิงคโปร์, *ยุทธศาสตร์เพื่อสร้างความเชื่อมั่นทางไซเบอร์ของสิงคโปร์*, สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘. จาก https://thaibizsingapore.com/news/main/opportunities/cyber-security-trust/

๔.๒ การแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีของประเทศไทย[๓๙]

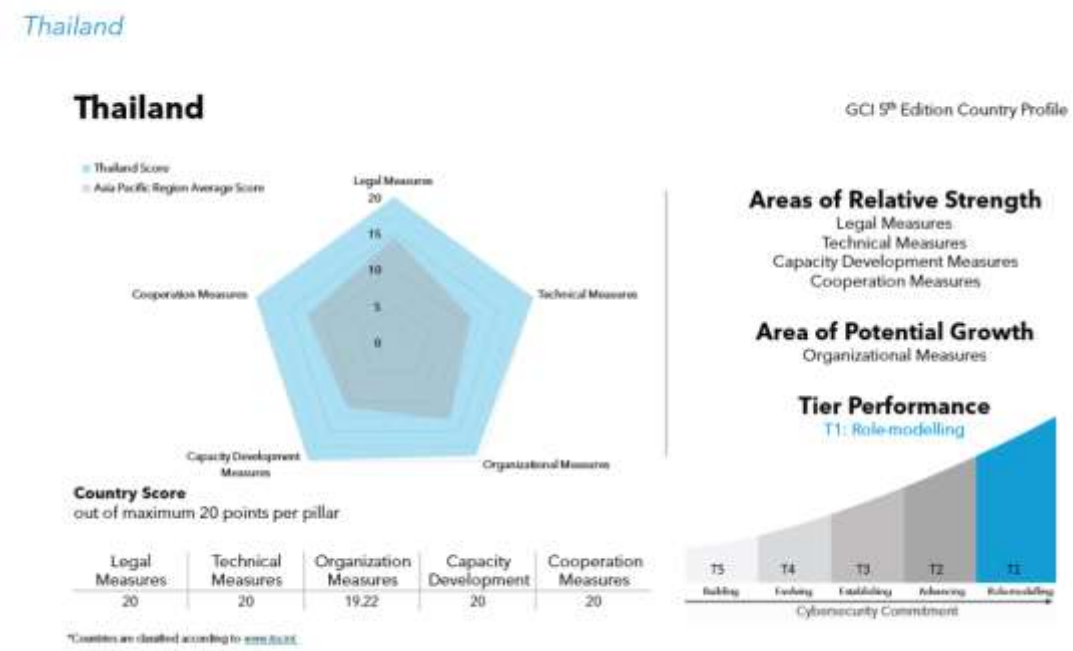
ลักษณะของสังคมดิจิทัลนำมาซึ่งผลประโยชน์ทางเศรษฐกิจ จึงทำให้อาเซียนเป็นตลาดสังคมออนไลน์อันดับหนึ่งของโลก ซึ่งการเปลี่ยนแปลงไปสู่สังคมดิจิทัล (Digitalization) จะนำมาซึ่งภัยคุกคามความมั่นคงในลักษณะของการใช้อินเทอร์เน็ตและคอมพิวเตอร์เป็นช่องทางในการโจมตี หรือที่เรียกว่า อาชญากรรมทางเทคโนโลยี หรืออาชญากรรมไซเบอร์[๔๐] จากการจัดอันดับ Global Cybersecurity Index ๒๐๒๔ (GCI) โดย International Telecommunication Union (ITU) ในปี ๒๐๒๔ ประเทศไทยก้าวขึ้นสู่อันดับที่ ๗ ของโลก[๔๑] จากผลการประเมินของ ๑๙๔ ประเทศทั่วโลก จากนโยบายการดำเนินงานของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ภายใต้แผนงาน The Growth Engine of Thailand หรือเครื่องยนต์หลักในการขับเคลื่อนเศรษฐกิจและสังคมดิจิทัลของประเทศ โดยให้ความสำคัญใน ๓ ด้าน ประกอบด้วย (๑) การเพิ่มขีดความสามารถด้านดิจิทัลในการสร้างข้อได้เปรียบทางการแข่งขันของประเทศ (Thailand Competitiveness) (๒) การสร้างความมั่นคงและปลอดภัยของเศรษฐกิจและสังคมดิจิทัล (Safety & Security) และ (๓) การเพิ่มศักยภาพทุนมนุษย์ด้านดิจิทัลของประเทศ (Human Capital) และความมุ่งมั่นของรัฐบาลที่จะพัฒนารัฐบาลให้เป็นรัฐบาลดิจิทัล และนโยบายรัฐบาลประการที่ห้าที่รัฐบาลจะเร่งกระตุ้นเศรษฐกิจ สร้างความเชื่อมั่นควบคู่กับการเพิ่มโอกาสในการประกอบอาชีพ โดยการวางรากฐานเศรษฐกิจดิจิทัล ซึ่งประเทศไทยได้รับการจัดอันดับด้านความมั่นคงปลอดภัยไซเบอร์ หรือ GCI ในปี ๒๐๒๔ ประเทศไทยได้คะแนนอยู่ที่ ๙๙.๒๒ คะแนน เป็นอันดับที่ ๗ ของโลกจากจำนวน ๑๙๔ ประเทศ ซึ่งก้าวกระโดดจากลำดับที่ ๔๔ ในการจัดลำดับในครั้งที่ผ่านมา ทำให้ประเทศไทยก้าวขึ้นสู่ประเทศชั้นนำใน Tier ๑ ซึ่งหมายถึงการเป็นหนึ่งในประเทศที่เป็น role models ด้านไซเบอร์ของโลก จากรายงาน Global Cybersecurity Index (GCI) ๒๐๒๔ ของ ITU ที่วัดผลสัมฤทธิ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศต่าง ๆ ผ่าน ๕ ด้าน ได้แก่ ด้านกฎหมาย (Legal) ด้านเทคนิค (Technical) ด้านหน่วยงาน/นโยบาย (Organizational) ด้านการพัฒนาศักยภาพ (Capacity Development) และด้านความร่วมมือ Cooperation)

---

[๓๙] International Telecommunication Union (ITU), *Global Cybersecurity Index ๒๐๒๔*, ๕th Edition, Geneva: ITU.

[๔๐] ลัฐกา เนตรทัศน์, *อาเซียนกับการจัดการปัญหาอาชญากรรมไซเบอร์*, สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘. จาก https://lawforasean.krisdika.go.th/File/files/cybersecurity_dec๒.pdf

[๔๑] จะเด็ด คุณคงกฤต, *Global Cybersecurity Index ๒๐๒๔*, สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘. จาก https://www.facebook.com/photo?fbid=๑๐๒๓๒๑๕๕๑๓๕๒๙๑๓๒๕&set=a.๑๒๓๐๔๖๔๔๑๑๙๕๓



ภาพที่ ๓ Thailand Score in Global Cybersecurity Index ๒๐๒๔

ที่มา : International Telecommunication Union (ITU), *Global Cybersecurity Index ๒๐๒๔*, ๕th Edition, Geneva: ITU, ๒๐๒๕, p. ๙๗.

ผลคะแนนในดัชนีนี้สะท้อนถึงความมุ่งมั่นของประเทศไทยในการพัฒนาและเสริมสร้างมาตรการความมั่นคงปลอดภัยไซเบอร์ในหลายด้าน โดยผลคะแนนที่ได้เกิดจากความร่วมมือร่วมใจของหน่วยงานต่าง ๆ ทุกภาคส่วน ซึ่งได้ร่วมผลักดันงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งในระดับบุคคล องค์กร ภาคส่วน และระดับประเทศ รวมถึงพันธมิตรทั้งในและต่างประเทศที่มีส่วนร่วมในการขับเคลื่อนการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศอย่างต่อเนื่องในด้านต่าง ๆ ดังนี้

๑) การยกระดับด้านกฎหมาย (Legal) ประเทศไทยได้ออกกฎหมายที่เกี่ยวข้องกับด้านดิจิทัลหลายฉบับ เช่น กฎหมายการกระทำผิดเกี่ยวกับข้อมูลคอมพิวเตอร์ที่ห้ามการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรือการเผยแพร่ข้อมูลเท็จ กฎหมายข้อมูลส่วนบุคคลเพื่อคุ้มครองข้อมูลส่วนบุคคลของประชาชนและกำหนดหลักเกณฑ์ในการเก็บใช้และเผยแพร่ข้อมูลส่วนบุคคล รวมถึงกฎหมายการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มุ่งเน้นการสร้างความมั่นคงปลอดภัยทางไซเบอร์

๒) การยกระดับด้านเทคนิค (Technical) ประเทศไทยได้จัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT) รวมถึงการดำเนินการด้านเทคนิคอื่น ๆ อาทิ การขึ้นทะเบียน ThaiCERT กับองค์กร CERT ระดับสากล เช่น First.org และ The Asia Pacific Computer Emergency Response Team (APCERT) การฝึกทดสอบขีดความสามารถทางไซเบอร์ในระดับประเทศ (Thailand's National

Cyber Exercise) และระดับภาคส่วน รวมทั้งการจัดตั้งระบบแพลตฟอร์มสำหรับการแบ่งปันข้อมูลภัยคุกคามทางไซเบอร์ (Malware Information Sharing Platform: MISP)

๓) การยกระดับด้านหน่วยงาน/นโยบาย (Organizational) ประเทศไทยได้จัดทำนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๕-๒๕๗๐ โดยมุ่งหวังให้เป็นยุทธศาสตร์ในการพัฒนาด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ โดยมีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เป็นหน่วยงานหลักที่รับผิดชอบในการขับเคลื่อนยุทธศาสตร์ร่วมกับหน่วยงานที่เกี่ยวข้อง นอกจากนี้ ยังได้จัดตั้งประชาคมไซเบอร์แห่งชาติ เพื่อให้เกิดการแลกเปลี่ยนองค์ความรู้และแนวคิดในการปฏิบัติตามนโยบายและแผนปฏิบัติการดังกล่าว

๔) การยกระดับด้านการพัฒนาศักยภาพ (Capacity Development) สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้ดำเนินโครงการเร่งรัดการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ (Intensive Cybersecurity Capacity Building Program) ระยะที่ ๑ โดยมีเป้าหมายเพื่อพัฒนาขีดความสามารถของบุคลากรที่ทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยสามารถพัฒนาบุคลากรได้มากกว่า ๕,๐๐๐ คน การจัดกิจกรรม Thailand Cyber Top Talent และ Thailand National Cyber Week ตั้งแต่ปี ๒๐๒๑-๒๐๒๓ ซึ่งมีการเข้าร่วมจากนักเรียน นิสิต นักศึกษา และประชาชนทั่วไปมากกว่า ๖,๐๐๐ คน นอกจากนี้ ยังมีการจัดตั้งสถาบันวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อพัฒนาศักยภาพบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์

๕) การยกระดับด้านความร่วมมือ (Cooperation) สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้ทำบันทึกข้อตกลง (MOU) ร่วมกับหน่วยงานทั้งภายในและต่างประเทศแล้วกว่า ๓๔ ฉบับ เช่น สาธารณรัฐประชาชนจีน อิสราเอล Microsoft Fortinet Huawei และหน่วยงานต่าง ๆ ในประเทศ รวมถึงการขับเคลื่อน ASEAN-Japan Cybersecurity Capacity Building Centre ร่วมกับประเทศญี่ปุ่นมาตั้งแต่ปี ๒๕๖๑ เพื่อพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ในอาเซียน และยังได้ริเริ่มแคมเปญเพื่อสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ในกลุ่มเยาวชน รวมถึงการปกป้องเด็กบนโลกออนไลน์ (Child Online Protection)

อย่างไรก็ตาม รายงานฉบับนี้ยังชี้ให้เห็นประเด็นที่ประเทศไทยจำเป็นต้องพัฒนาเพิ่มเติม เช่น การปรับปรุงกฎหมายที่เกี่ยวข้องกับการปกป้องเด็กในโลกออนไลน์ หรือการเพิ่มขีดความสามารถด้านเทคนิคในการรับมือกับภัยคุกคามที่ทันสมัยขึ้น การเข้าร่วมเป็นส่วนหนึ่งของประชาคมอาเซียนได้เสริมสร้างความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ในระดับนานาชาติอย่างสม่ำเสมอ โดยเฉพาะความร่วมมือในกรอบ ASEAN Cyber Coordinating Committee (ASEAN Cyber-CC) และ ASEAN-EU Statement on Cybersecurity Cooperation เป็นต้น

บทที่ ๕
บทสรุปและข้อเสนอแนะ

บทนี้เป็นการสรุปผลการศึกษาและข้อเสนอแนะเกี่ยวกับสภาพปัญหาของรูปแบบการกระทำความผิดที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี ตลอดจนการบังคับใช้กฎหมายและนโยบายที่เกี่ยวข้องกับการแก้ไขปัญหาดังกล่าว ทั้งนี้ เพื่อใช้เป็นแนวทางประกอบการพิจารณากำหนดมาตรการทางกฎหมายและนโยบายที่มีประสิทธิภาพในการป้องกันและแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีของประเทศไทย โดยมีรายละเอียดดังต่อไปนี้

๕.๑ สรุปผลการศึกษา

การขับเคลื่อนนโยบายเศรษฐกิจและสังคมดิจิทัลของรัฐบาลส่งผลให้ประชาชนส่วนใหญ่สามารถเข้าถึงและใช้ประโยชน์จากเทคโนโลยีดิจิทัลได้อย่างแพร่หลาย ซึ่งช่วยเพิ่มประสิทธิภาพในการทำงานและอำนวยความสะดวกในชีวิตประจำวัน อย่างไรก็ตาม การเข้าถึงและการใช้งานเทคโนโลยีดิจิทัลที่สะดวกรวดเร็วย่อมส่งผลให้ปัญหาภัยออนไลน์และอาชญากรรมทางเทคโนโลยีในรูปแบบต่าง ๆ ทวีความรุนแรงมากขึ้น โดยเฉพาะปัญหาการฉ้อโกงและการหลอกลวงประชาชนผ่านสื่อสังคมออนไลน์ ซึ่งเกิดขึ้นอย่างต่อเนื่องและมีแนวโน้มเพิ่มขึ้นอย่างมีนัยสำคัญ ตัวอย่างของการฉ้อโกงและการหลอกลวงออนไลน์ที่พบได้บ่อย ได้แก่ การหลอกลวงผ่านแก๊งคอลเซ็นเตอร์ (Call Center) การหลอกลวงให้ลงทุนโดยการระดมทุนออนไลน์ การฉ้อโกงการซื้อขายสินค้าและบริการผ่านแพลตฟอร์มออนไลน์ เป็นต้น กรณีดังกล่าวก่อให้เกิดความเสียหายแก่ประชาชน ทั้งในแง่ของการสูญเสียทรัพย์สินเป็นจำนวนมาก รวมถึงส่งผลกระทบต่อเศรษฐกิจ ความเชื่อมั่นของประชาชนและความมั่นคงทางเทคโนโลยีของประเทศ ทั้งนี้ ปัญหาการฉ้อโกงและการหลอกลวงออนไลน์เกิดจากหลายปัจจัย เช่น การขาดความตระหนักรู้ของประชาชนเกี่ยวกับภัยออนไลน์ ทำให้ตกเป็นเหยื่อของมิจฉาชีพ การรับจ้างเปิดบัญชีธนาคาร และการซื้อขายบัญชีธนาคาร (บัญชีม้า) ซึ่งถูกนำไปใช้เป็นเครื่องมือในการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี การใช้ซิมโทรศัพท์ที่ไม่ได้ลงทะเบียนในชื่อของตน ทำให้ยากต่อการตรวจสอบและติดตามตัวผู้กระทำความผิด ข้อจำกัดของกฎหมาย กฎระเบียบ และอำนาจหน้าที่ของธนาคารในการส่งต่อหรือแลกเปลี่ยนข้อมูลบัญชีต้องสงสัยหรือข้อมูลของผู้กระทำความผิดระหว่างธนาคาร ทำให้การระบุตัวผู้กระทำความผิดและการยับยั้งธุรกรรมทางการเงินไม่สามารถดำเนินการได้อย่างมีประสิทธิภาพและทันท่วงที ความสามารถของผู้ให้บริการโทรศัพท์เคลื่อนที่ในการตรวจสอบข้อความสั้น (SMS) หรือการส่งลิงก์และเว็บไซต์ที่เป็นการหลอกลวงประชาชน รวมถึงการระงับหรือยับยั้งข้อความที่ต้องสงสัยก่อนที่ประชาชนจะได้รับความเสียหาย ดังนั้น การแก้ไขปัญหาภัยออนไลน์และอาชญากรรมทางเทคโนโลยีจำเป็นต้องอาศัยความร่วมมือจากทุกภาคส่วน รวมถึงการปรับปรุงกฎหมาย กฎระเบียบ และมาตรการต่าง ๆ ให้มีประสิทธิภาพมากยิ่งขึ้น เพื่อป้องกันและลดความเสียหายที่อาจเกิดขึ้นแก่ประชาชนและประเทศโดยรวม

การกำหนดรูปแบบการกระทำผิดอาชญากรรมทางเทคโนโลยีที่กระทำผิดเกี่ยวกับการฉ้อโกง กรรโชก หรือรีดเอาทรัพย์ ซึ่งทำให้บุคคลอื่นเสียหายตามพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๖ และคำสั่งสำนักงานตำรวจแห่งชาติ ที่ ๑๘๒/๒๕๖๖ ลงวันที่ ๑๗ มีนาคม ๒๕๖๖ มีดังต่อไปนี้

๑) หลอกลวงซื้อขายสินค้าหรือบริการ ที่ไม่มีลักษณะเป็นขบวนการ

๒) หลอกลวงเป็นบุคคลอื่นเพื่อยืมเงิน

๓) หลอกลวงให้รักแล้วโอนเงิน (Romance Scam)

๔) หลอกลวงให้โอนเงินเพื่อรับรางวัล หรือวัตถุประสงค์อื่น ๆ

๕) หลอกลวงให้กู้เงิน

๖) หลอกลวงให้โอนเงินเพื่อทำงานหารายได้พิเศษ

๗) ข่มขู่ทางโทรศัพท์ให้เกิดความกลัวแล้วหลอกให้โอนเงิน (Call Center)

๘) การกระทำต่อระบบหรือข้อมูลคอมพิวเตอร์โดยผิดกฎหมาย (Hacking) เพื่อให้ได้ไปซึ่งทรัพย์

๙) การเข้ารหัสข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบเพื่อกรรโชก หรือรีดเอาทรัพย์ (Ransomware)

๑๐) หลอกลวงให้ติดตั้งโปรแกรมควบคุมระบบในเครื่องโทรศัพท์ เพื่อให้ได้ไปซึ่งทรัพย์

๑๑) หลอกลวงเกี่ยวกับสินทรัพย์ดิจิทัล

๑๒) หลอกลวงให้ลงทุนผ่านระบบคอมพิวเตอร์

๑๓) หลอกลวงซื้อขายสินค้าหรือบริการ ที่มีลักษณะเป็นขบวนการ

๑๔) หลอกลวงให้ลงทุนที่เป็นความผิดตามพระราชกำหนดการกู้ยืมเงินที่เป็นการฉ้อโกงประชาชน พ.ศ. ๒๕๒๗

ประเภทอาชญากรรมทางเทคโนโลยีและกฎหมายที่เกี่ยวข้อง สามารถสรุปได้ ดังนี้

กลุ่มที่ ๑ อาชญากรรมที่เกิดขึ้นกับข้อมูลและระบบคอมพิวเตอร์ หรือ Cyber Dependent Crime ซึ่งหมายถึงการกระทำที่ต้องอาศัยเทคโนโลยีสารสนเทศและระบบคอมพิวเตอร์เป็นเครื่องมือหลักในการก่ออาชญากรรม โดยสามารถแบ่งประเภทของการกระทำความผิดได้ ดังนี้ ประการแรก การเข้าถึงระบบหรือข้อมูลของบุคคลอื่นโดยมิชอบ หรือการเปิดเผยมาตรการที่เกี่ยวข้องกับความลับในการเข้าถึงระบบ ซึ่งเป็นการละเมิดหลักการด้าน Confidentiality หรือการรักษาความลับของข้อมูล ประการที่สอง การแก้ไข ดัดแปลง หรือทำให้ข้อมูลของบุคคลอื่นเสียหาย หรือมีการเปลี่ยนแปลงข้อมูลโดยมิชอบ ซึ่งกระทบต่อความสมบูรณ์ของข้อมูลคอมพิวเตอร์ หรือ Integrity อาชญากรรมในลักษณะนี้อาจส่งผลให้ข้อมูลสำคัญถูกเปลี่ยนแปลงโดยไม่ได้รับอนุญาต อันอาจก่อให้เกิดความเสียหายต่อบุคคล องค์กร หรือภาครัฐ ประการที่สาม การกระทำที่ทำให้ระบบคอมพิวเตอร์ไม่สามารถทำงานได้ตามปกติ อันเป็นการรบกวนหรือขัดขวางการทำงานของระบบ ซึ่งส่งผลต่อ Availability หรือความสามารถในการเข้าถึงและใช้งานข้อมูลและระบบคอมพิวเตอร์ได้อย่างต่อเนื่อง ซึ่งรวมถึงการโจมตีระบบให้เกิดการล่ม (Denial-of-Service หรือ DoS) และการกระจายการโจมตีจากหลายแหล่ง (Distributed Denial-of-Service หรือ DDoS) ประการที่สี่ การส่ง

ข้อมูลหรืออีเมลโดยปกปิดหรือปลอมแปลงแหล่งที่มา อันเป็นการรบกวนบุคคลอื่น รวมถึงการส่งอีเมลสแปมที่เป็นอันตรายหรือสร้างความรำคาญแก่ผู้รับ ประการที่ห้า การกระทำความผิดที่ร้ายแรง ซึ่งส่งผลกระทบต่อความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจ หรือโครงสร้างพื้นฐานที่มีความสำคัญต่อสังคม โดยเกี่ยวข้องกับ Availability Integrity และ Confidentiality ของข้อมูลและระบบคอมพิวเตอร์ ประการที่หก การจำหน่ายหรือเผยแพร่ชุดคำสั่งคอมพิวเตอร์ (Malicious Software หรือ Malware) ที่สามารถนำไปใช้เพื่อกระทำความผิดทางเทคโนโลยี อาทิ ไวรัสคอมพิวเตอร์ โทรจัน หรือโปรแกรมที่มุ่งร้ายต่อระบบ ประการที่เจ็ด การเผยแพร่ข้อมูลเท็จ ข่าวปลอม หรือการนำเข้าข้อมูลปลอม บิดเบือน ผิดเพี้ยน และสื่อที่อาจกระทบต่อความมั่นคงของรัฐ รวมถึงการเผยแพร่เนื้อหาที่เป็นสื่อลามกอนาจารผ่านระบบคอมพิวเตอร์ ประการที่แปด การให้ความร่วมมือ สนับสนุน หรือยินยอมให้มีการกระทำความผิดทางเทคโนโลยี ซึ่งอาจรวมถึงการร่วมมือกับผู้กระทำผิดหรือการละเลยไม่ป้องกันการกระทำความผิดดังกล่าว ประการที่เก้า การตัดต่อ เติม หรือดัดแปลงภาพ โดยเฉพาะการใช้เทคโนโลยีดิจิทัลในการปลอมแปลงภาพเพื่อวัตถุประสงค์ที่ไม่ชอบธรรม และประการที่สิบ ผู้ให้บริการที่มีหน้าที่เกี่ยวข้องกับการจัดเก็บข้อมูลทางคอมพิวเตอร์ต้องปฏิบัติตามข้อกำหนดในการเก็บรักษาข้อมูล มิฉะนั้นอาจถือว่าเป็นการกระทำผิด ทั้งนี้ การกระทำความผิดในลักษณะดังกล่าวถือเป็นความผิดตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ซึ่งกำหนดบทลงโทษแก่ผู้ที่ฝ่าฝืนและมีส่วนเกี่ยวข้องกับการกระทำความผิดด้านอาชญากรรมทางเทคโนโลยี โดยมีวัตถุประสงค์เพื่อป้องกันและปราบปรามการใช้เทคโนโลยีสารสนเทศในทางที่ผิด และเสริมสร้างความมั่นคงปลอดภัยให้กับระบบข้อมูลและโครงสร้างพื้นฐานทางดิจิทัลของประเทศ

กลุ่มที่ ๒ อาชญากรรมในลักษณะของการฉ้อโกงหรือการหลอกลวงโดยใช้ข้อมูลหรือระบบคอมพิวเตอร์ เป็นเครื่องมือในการกระทำผิด การฉ้อโกงประเภทนี้มักอาศัยปัจจัยด้านความเชื่อใจ ความโลภ ความหลง หรือความกลัวของเหยื่อ เพื่อทำให้ตกเป็นเหยื่อของการหลอกลวง โดยรูปแบบของการกระทำความผิดในกลุ่มนี้ประกอบด้วย การหลอกลวงเกี่ยวกับการซื้อขายสินค้าและบริการ ซึ่งรวมถึงการฉ้อโกงการซื้อขายสินค้าในลักษณะทั่วไปและการฉ้อโกงที่เป็นขบวนการ การหลอกลวงที่เกี่ยวข้องกับเงินดิจิทัล เช่น การโอนเงินเพื่อรับรางวัลที่ไม่มีอยู่จริง การฉ้อโกงทางโทรศัพท์แบบเป็นขบวนการ (Call Center Scam) ซึ่งมิจฉาชีพมักแอบอ้างเป็นเจ้าหน้าที่รัฐหรือองค์กรที่มีความน่าเชื่อถือเพื่อหลอกให้เหยื่อโอนเงิน การแอบอ้างเป็นบุคคลอื่นเพื่อขอยืมเงิน และการหลอกลวงให้เกิดความรักแล้วให้โอนเงิน (Romance Scam) การกระทำความผิดในลักษณะนี้ถือเป็นความผิดฐาน ฉ้อโกง ตามประมวลกฎหมายอาญา มาตรา ๓๕๑ ซึ่งบัญญัติว่า การทุจริตหลอกลวงผู้อื่นโดยการให้ข้อมูลอันเป็นเท็จ หรือปกปิดข้อเท็จจริงที่ควรต้องแจ้งให้ทราบ ถือเป็นการกระทำที่มีโทษทางกฎหมาย

กลุ่มที่ ๓ อาชญากรรมในลักษณะของการฉ้อโกงประชาชน เป็นการหลอกลวงบุคคลจำนวนมากให้ลงทุนหรือทำธุรกิจโดยใช้เทคโนโลยีสารสนเทศเป็นเครื่องมือ การกระทำผิดในลักษณะนี้ รวมถึง การหลอกให้โอนเงินโดยอ้างว่าทำกิจกรรมแล้วจะได้รับผลตอบแทน การหลอกให้ลงทุนในธุรกิจที่ไม่มีอยู่จริง หรือ การชักชวนให้ลงทุนในลักษณะที่เข้าข่ายเป็นการฉ้อโกงประชาชน ซึ่งอาจ

รวมถึงแชร์ลูกโซ่ (Ponzi Scheme) และ การหลอกให้เกิดความรักเพื่อชักชวนให้ลงทุน หรือ Hybrid Scam ซึ่งเป็นการผสมผสานระหว่างการหลอกลวงในเชิงอารมณ์และการชักชวนให้ลงทุนโดยอาศัยความไว้วางใจของเหยื่อ การกระทำดังกล่าวถือเป็นความผิดฐานฉ้อโกงประชาชน ตามประมวลกฎหมายอาญา มาตรา ๓๔๓ ซึ่งกำหนดโทษที่รุนแรงกว่าการฉ้อโกงในกรณีทั่วไป เนื่องจากเป็นการกระทำที่ส่งผลกระทบเป็นวงกว้างต่อประชาชนจำนวนมาก

กลุ่มที่ ๔ อาชญากรรมที่เกี่ยวข้องกับเสรีภาพ ชื่อเสียง ความผิดทางเพศ และการกระทำต่อผู้เยาว์ ซึ่งอาศัยเทคโนโลยีเป็นเครื่องมือในการกระทำความผิด โดยสามารถจำแนกได้เป็นหลายประเภท ได้แก่ การหมิ่นประมาทหรือดูหมิ่นบุคคลอื่น ซึ่งเป็นการใส่ความบุคคลอื่นต่อบุคคลที่สามโดยวิธีการที่อาจทำให้ผู้นั้นได้รับความเสียหายทางชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง ถือเป็นความผิดตามประมวลกฎหมายอาญา มาตรา ๓๒๖ และหากเป็นการกระทำผ่านช่องทางที่เผยแพร่ต่อสาธารณะ เช่น การโพสต์ข้อความในสื่อสังคมออนไลน์เพื่อประจานบุคคลอื่น หรือ การระบุชื่อนามสกุล และเผยแพร่รูปภาพของบุคคลอื่นเพื่อทำให้เสื่อมเสียชื่อเสียง ถือเป็นความผิดตามมาตรา ๓๒๘ ฐานหมิ่นประมาทโดยการโฆษณา การข่มขู่หรือคุกคามทางเพศ ซึ่งเป็นการกระทำที่มุ่งรังแก ข่มเหง คุกคาม หรือทำให้ผู้อื่นได้รับความอับอาย หรือเกิดความเดือดร้อนรำคาญ ถือเป็นความผิดตามประมวลกฎหมายอาญา มาตรา ๓๙๗ และในบางกรณีอาจเข้าข่ายเป็นความผิดเกี่ยวกับการล่วงละเมิดทางเพศที่ร้ายแรงขึ้นอยู่กับพฤติการณ์ของการกระทำความผิด นอกจากนี้ การหลอกลวงบุคคลให้เดินทางไปทำงานต่างประเทศโดยอ้างว่าจะได้รับค่าตอบแทนสูงหรือเงื่อนไขที่ดีเกินจริง ถือเป็นการฉ้อโกงแรงงาน ซึ่งเป็นความผิดตามประมวลกฎหมายอาญา มาตรา ๓๔๔ อาชญากรรมในกลุ่มต่าง ๆ ดังกล่าวล้วนเป็นปัญหาที่ส่งผลกระทบต่อสังคมเป็นวงกว้าง จำเป็นต้องได้รับการบังคับใช้กฎหมายอย่างเข้มงวด รวมถึงการพัฒนามาตรการป้องกันและแก้ไขปัญหาอย่างเป็นระบบเพื่อให้สามารถรับมือกับภัยคุกคามทางเทคโนโลยีที่ทวีความซับซ้อนมากขึ้น

จากบทเรียนความสำเร็จการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีของประเทศสิงคโปร์พบว่า ประเทศสิงคโปร์ถือเป็นหนึ่งในประเทศที่ประสบความสำเร็จในการรับมือกับปัญหาอาชญากรรมทางเทคโนโลยี โดยรัฐบาลให้ความสำคัญอย่างยิ่งกับการสร้างความตระหนักรู้ของประชาชน เพื่อให้สามารถรับมือกับภัยคุกคามทางเทคโนโลยีได้อย่างมีประสิทธิภาพ ทั้งนี้ สิงคโปร์มุ่งเน้นการเพิ่มขีดความสามารถของประเทศในการรักษาความปลอดภัยบนโลกออนไลน์ ผ่านการดำเนินมาตรการและนโยบายที่สำคัญในหลายด้าน

๑) การสร้างความร่วมมือระหว่างภาครัฐและภาคเอกชน (Public-Private Partnership) โดยมีการลงนามในบันทึกความเข้าใจระหว่าง Cyber Security Agency of Singapore (CSA) และบริษัทเทคโนโลยีระดับโลก เช่น Google และ Microsoft ความร่วมมือดังกล่าวช่วยส่งเสริมการแบ่งปันข้อมูลภัยคุกคามทางไซเบอร์อย่างอัจฉริยะระหว่างภาครัฐและเอกชน ส่งผลให้สามารถต่อสู้กับกิจกรรมที่มุ่งร้ายและอาชญากรรมออนไลน์ได้อย่างมีประสิทธิภาพ รวมถึงการแลกเปลี่ยนองค์ความรู้ด้าน ปัญญาประดิษฐ์ (Artificial Intelligence – AI) ซึ่งเป็นเครื่องมือสำคัญในการยกระดับศักยภาพของทุกภาคส่วนในการเผชิญกับอาชญากรรมทางเทคโนโลยี

๒) การจัดตั้งศูนย์ต่อต้านขบวนการหลอกลวงเงินทางออนไลน์ (Singapore Anti-Scam Command) ซึ่งอยู่ภายใต้การกำกับดูแลของกองกำลังตำรวจสิงคโปร์ (Singapore Police Force: SPF) โดยศูนย์ดังกล่าวเป็นหน่วยงานที่ทำงานร่วมกันระหว่างสถาบันการเงินและหน่วยงานบังคับใช้กฎหมายของสิงคโปร์ มีบทบาทสำคัญในการแลกเปลี่ยนข้อมูลที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี และสามารถดำเนินการอายัดบัญชีที่เกี่ยวข้องกับขบวนการหลอกลวงทางออนไลน์ได้อย่างทันท่วงที

๓) การพัฒนาศักยภาพด้านความมั่นคงทางไซเบอร์ผ่านโครงการ SG Cyber Leadership and Alumni Program ซึ่งเป็นโครงการฝึกอบรมที่ครอบคลุมตั้งแต่ระดับพื้นฐานไปจนถึงระดับผู้บริหาร อีกทั้งยังเปิดโอกาสให้ผู้เข้าร่วมจากหลายประเทศสามารถเข้ามาแลกเปลี่ยนมุมมองเกี่ยวกับปัญหาทางไซเบอร์ในปัจจุบัน โดยรัฐบาลสิงคโปร์ให้การสนับสนุนทางการเงินแก่โครงการดังกล่าวเป็นมูลค่ากว่า ๓๐ ล้านดอลลาร์สิงคโปร์ และได้ขยายกรอบเวลาของโครงการต่อไปอีกสามปี (พ.ศ. ๒๕๖๗ – ๒๕๖๙) เพื่อส่งเสริมการพัฒนาองค์ความรู้ด้านความมั่นคงทางไซเบอร์อย่างต่อเนื่อง

๔) การเสริมสร้างความร่วมมือระหว่างประเทศและกลุ่มอุตสาหกรรม ปัจจุบันสิงคโปร์เป็นสมาชิกของ United Nations Open-Ended Working Group ซึ่งมีบทบาทสำคัญในด้านความมั่นคงและการใช้งานข้อมูลเทคโนโลยีสารสนเทศ นอกจากนี้ สิงคโปร์ยังได้ลงนามในความตกลงทางเศรษฐกิจดิจิทัล (Digital Economy Agreements: DEAs) กับประเทศพันธมิตร เช่น ออสเตรเลีย สหราชอาณาจักร และเกาหลีใต้ เพื่อเสริมสร้างความมั่นคงทางเศรษฐกิจดิจิทัลและส่งเสริมการดำเนินธุรกิจในสภาพแวดล้อมที่ปลอดภัยยิ่งขึ้น

๕) การกำหนดแนวทางความร่วมมือระหว่างประเทศบนพื้นฐานของกฎระเบียบที่เป็นมาตรฐานสากล โดยยึดถือแนวปฏิบัติที่เกี่ยวข้องกับข้อบังคับด้านเทคนิค ตลอดจนการกำหนดแนวทางการใช้พื้นที่ออนไลน์อย่างสันติ ซึ่งนโยบายดังกล่าวไม่เพียงช่วยให้เกิดความเข้าใจที่ตรงกันในด้านการกำกับดูแลระบบเทคโนโลยีสารสนเทศ แต่ยังช่วยลดโอกาสของความขัดแย้งในโลกไซเบอร์ที่อาจเกิดขึ้นจากจำนวนผู้ใช้งานที่เพิ่มขึ้นอย่างรวดเร็ว

๖) การเสริมสร้างขีดความสามารถของประเทศต่าง ๆ ในการรับมือกับภัยคุกคามทางไซเบอร์ โดยสิงคโปร์ได้จัดตั้งศูนย์ความเป็นเลิศด้านความมั่นคงปลอดภัยไซเบอร์อาเซียน-สิงคโปร์ (ASEAN – Singapore Cybersecurity Centre of Excellence: ASCCE) เมื่อปี พ.ศ. ๒๕๖๒ ซึ่งเป็นส่วนขยายของโครงการ ASEAN Cyber Capacity Programme (ACCP) ศูนย์ดังกล่าวมีบทบาทสำคัญในการสนับสนุนประเทศสมาชิกอาเซียนผ่านการดำเนินโครงการวิจัยและการฝึกอบรมด้านความมั่นคงทางไซเบอร์ ปัจจุบัน ศูนย์แห่งนี้ได้จัดอบรมหลักสูตรด้านความมั่นคงปลอดภัยทางไซเบอร์แล้วกว่า ๕๐ หลักสูตร และให้การฝึกอบรมแก่เจ้าหน้าที่อาวุโสของประเทศสมาชิกอาเซียนแล้วกว่า ๑,๕๐๐ ราย

นอกจากนี้ รัฐบาลสิงคโปร์ยังได้ตราพระราชบัญญัติป้องกันการฉ้อโกง พ.ศ. ๒๕๖๗ ซึ่งให้อำนาจแก่เจ้าหน้าที่ตำรวจในการออกคำสั่งไปยังสถาบันการเงินเพื่อระงับการโอนเงินหรือการถอนเงินของเหยื่อที่ตกเป็นเป้าหมายของมิจฉาชีพออนไลน์ได้โดยทันที มาตรการดังกล่าวมีเป้าหมายเพื่อคุ้มครองประชาชนที่อาจหลงเชื่อหรือไม่ตระหนักว่าตนกำลังถูกหลอกลวงทางออนไลน์ โดยธนาคารกลางสิงคโปร์ (Monetary Authority of Singapore – MAS) ได้ร่วมมือกับสำนักงานพัฒนาสื่อสารและสารสนเทศ

(Infocomm Media Development Authority – IMDA) ในการบังคับใช้ กรอบความรับผิดชอบร่วม (Shared Responsibility Framework – SRF) เพื่อป้องกันการฉ้อโกงทางการเงินในทุกรูปแบบ โดยมุ่งเน้นให้ทุกภาคส่วนที่เกี่ยวข้องร่วมกันรับผิดชอบอย่างเป็นธรรม มิใช่ให้ผู้บริโภคเป็นผู้รับภาระเพียงฝ่ายเดียว ภายใต้กรอบนโยบายดังกล่าว ได้มีการกำหนดหน้าที่ความรับผิดชอบของ สถาบันการเงินและผู้ให้บริการโทรคมนาคมอย่างชัดเจน ดังนี้ สถาบันการเงินต้องดำเนินมาตรการรักษาความปลอดภัย อาทิ การส่งการแจ้งเตือนธุรกรรม (Transaction Alerts) ให้แก่ลูกค้าเมื่อมีการทำธุรกรรมทางการเงิน การตรวจสอบธุรกรรมที่มีลักษณะน่าสงสัย และการให้ความรู้แก่ลูกค้าเกี่ยวกับรูปแบบของการฉ้อโกงทางการเงิน ผู้ให้บริการโทรคมนาคมต้องดำเนินมาตรการป้องกัน เช่น การใช้ ระบบคัดกรองและบล็อกข้อความสั้นที่น่าสงสัย (Suspicious SMS Filtering and Blocking System) ตลอดจนให้ความร่วมมือกับหน่วยงานบังคับใช้กฎหมายในการสอบสวนและดำเนินคดีต่อผู้กระทำความผิด จากแนวทางดังกล่าว สิงคโปร์ถือเป็นประเทศต้นแบบที่มีความโดดเด่นในด้านการป้องกันภัยคุกคามทางเทคโนโลยี โดยเฉพาะในกรอบความรับผิดชอบร่วม (SRF) ซึ่งกำหนดให้ทั้งสถาบันการเงินและผู้บริโภคต้องรับผิดชอบร่วมกันในกรณีที่เกิดความเสียหายจากการถูกฉ้อโกงทางการเงิน นอกจากนี้ สิงคโปร์ยังได้พัฒนาระบบปิดสวิตช์ (Kill-Switch System) ซึ่งช่วยให้ผู้บริโภคสามารถระงับบัญชีของตนได้โดยทันทีหากพบความผิดปกติ รวมถึงมาตรการล็อกเงิน (Money Lock) ที่ช่วยให้ลูกค้าสามารถกำหนดวงเงินบางส่วนเพื่อป้องกันไม่ให้ถูกใช้ทำธุรกรรมออนไลน์โดยไม่ได้รับอนุญาต มาตรการเชิงรุกเหล่านี้สะท้อนให้เห็นถึง ความมุ่งมั่นของรัฐบาลสิงคโปร์ในการป้องกันและแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีอย่างจริงจัง เนื่องจากมูลค่าความเสียหายที่เกิดขึ้นอาจส่งผลกระทบในระยะยาวต่อความเชื่อมั่นของสิงคโปร์ในฐานะศูนย์กลางทางการเงินของภูมิภาคและของโลก ทั้งนี้ การจัดการกับอาชญากรรมทางเทคโนโลยีจำเป็นต้องอาศัยความร่วมมือระหว่างประเทศ รวมถึงการเสริมสร้างความตระหนักรู้ให้แก่ภาคธุรกิจและประชาชน เพื่อให้สามารถรับมือกับภัยคุกคามที่เปลี่ยนแปลงไปอย่างรวดเร็ว

๕.๒ ข้อเสนอแนะ

๑) เพื่อยกระดับประสิทธิภาพของพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ ๒) พ.ศ. ๒๕๖๘ ภาครัฐควรปรับปรุงเพิ่มเติมทั้งในเชิงโครงสร้างกลไก และการบังคับใช้กฎหมายอย่างบูรณาการ โดยกำหนดหน้าที่และความรับผิดชอบของผู้ให้บริการและหน่วยงานที่เกี่ยวข้องให้ชัดเจนยิ่งขึ้น สอดรับกับพัฒนาการทางเทคโนโลยีและรูปแบบอาชญากรรมรูปแบบใหม่ ๆ อาทิ กำหนดให้แพลตฟอร์มการให้สินเชื่อแบบ P๒P เพื่อปฏิเสธการเปิดบัญชีหรือระงับบริการเมื่อพบการฉ้อโกง และให้องค์กรกำกับดูแล เช่น คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) มีอำนาจระงับซิมโทรศัพท์ที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ได้ทันที รวมทั้งขยายขอบเขตการคุ้มครองให้ครอบคลุมการทำธุรกรรมผ่านสกุลเงินอิเล็กทรอนิกส์หรือสินทรัพย์ดิจิทัลทุกประเภท (ซึ่งเป็นช่องว่างในกฎหมายเดิม) พร้อมเพิ่มบทบัญญัติเยียวยาผู้เสียหาย เช่น การคืนเงินแก่เหยื่ออย่างรวดเร็ว นอกจากนี้ ควรเสริมกลไกเชิงเทคนิคและมาตรการป้องปรามโดยกำหนดระบบกรองข้อความ SMS ทุจริตและการพิสูจน์ตัวตน (Know Your Customer: KYC) เพื่อเพิ่มความปลอดภัยทางการเงินสำหรับซิมการ์ดหรือบัญชีผู้ใช้งานให้เข้มงวด โดยให้อำนาจเจ้าหน้าที่รัฐสามารถสั่งอายัดบัญชี ระงับซิม หรือระงับธุรกรรม

ที่น่าสงสัยได้ทันที รวมถึงเปิดช่องทางแลกเปลี่ยนข้อมูลสำคัญ (เช่น เลขบัญชี หมายเลขโทรศัพท์ รายการโอนเงิน ฯลฯ) ระหว่าง ธนาคารแห่งประเทศไทย ตำรวจ สำนักงานป้องกันและปราบปรามการฟอกเงิน และ คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ เพื่อเร่งสืบสวนและยับยั้งกระบวนการทุจริตทันท่วงที ในเชิงกลไกองค์กร ควรจัดตั้งศูนย์เฉพาะกิจประสานงานป้องกันอาชญากรรมไซเบอร์ระหว่างหน่วยงานหลัก (ตามแนวทางศูนย์ต่อต้านอาชญากรรมไซเบอร์ที่กฎหมายบัญญัติไว้) เพื่อรับคำร้องของผู้เสียหาย ระงับธุรกรรมผิดกฎหมาย และประสานการคืนความเสียหายแก่ประชาชนอย่างมีประสิทธิภาพ พร้อมทั้งทบทวนและตราบัญญัติมาตรการสำคัญเหล่านี้เข้าสู่กฎหมายถาวร โดยจัดตั้งกลไกกำกับติดตามเพื่อปรับปรุงบทบัญญัติให้ทันสมัยสอดคล้องกับภัยไซเบอร์ที่เปลี่ยนแปลงอย่างต่อเนื่อง

๒) ควรมีการนำระบบความรับผิดชอบร่วม (Shared Responsibility Framework – SRF) มาใช้เป็นแนวทางในการจัดการปัญหาอาชญากรรมทางเทคโนโลยี รวมถึงการบังคับใช้มาตรการหน่วงเงิน (Money Lock) เพื่อเพิ่มระดับความปลอดภัยให้แก่ประชาชน ซึ่งมาตรการดังกล่าวจะไม่เพียงช่วยลดความเสียหายที่อาจเกิดขึ้นจากการฉ้อโกงทางการเงิน แต่ยังช่วยเสริมสร้างความมั่นใจให้แก่ประชาชนในการทำธุรกรรมทางการเงินผ่านระบบดิจิทัล

๓) ควรส่งเสริมวัฒนธรรมแห่งการป้องกันภัยทางเทคโนโลยี โดยใช้เทคโนโลยีเป็นสื่อในการรณรงค์เพื่อสร้างความตระหนักรู้ให้แก่ประชาชน ทั้งนี้ ประชาชนควรได้รับข้อมูลที่ถูกต้องและครบถ้วนเกี่ยวกับภัยคุกคามทางเทคโนโลยี และแนวทางในการป้องกันตนเองจากอาชญากรรมออนไลน์ ผ่านช่องทางออนไลน์ที่ได้รับความนิยมในประเทศไทย อาทิ Facebook Line TikTok X และ Instagram ซึ่งเป็นแพลตฟอร์มที่สามารถเข้าถึงกลุ่มเป้าหมายได้อย่างมีประสิทธิภาพ

บรรณานุกรม

หนังสือ

International Telecommunication Union (ITU). *Global Cybersecurity Index ๒๐๒๔*. ๕th Edition. Geneva: ITU, ๒๐๒๕.

Shelly, G. & Vermaat, M. *Discovering Computers ๒๐๑๑*. Complete: Cengage Learning, ๒๐๑๐.

รายงานการวิจัยและรายงานทางวิชาการ

สัจจะ โชคบุญส่งสวัสดิ์. “แนวทางการเพิ่มประสิทธิภาพในการตัดวงจรอาชญากรรมออนไลน์.” หลักสูตรนักบริหารระดับสูง : ผู้นำที่มีวิสัยทัศน์และคุณธรรม รุ่นที่ ๙๘ วิทยาลัยนักบริหาร สถาบันพัฒนาข้าราชการพลเรือน สำนักงาน ก.พ., ๒๕๖๖.

บทความวิชาการ

อภิชาต บวบขม. อาชญากรรมทางเทคโนโลยี: กฎหมายและแนวทางการป้องกันแบบบูรณาการ, *Journal of Roi Kaensarn Academi*, ๘(๑๒) ธันวาคม ๒๕๖๖: ๗๒๖-๗๔๓.

สื่ออิเล็กทรอนิกส์

กรมประชาสัมพันธ์. *Romance Scam คืออะไร รู้จักไว้ก่อนตกเป็นเหยื่อ*. สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘, จากhttps://www.prd.go.th/th/content/category/detail/id/๓๑/iid/๒๖๖๒๘๙

กระทรวงการต่างประเทศ. *ไทยร่วมรับรองร่างอนุสัญญาว่าด้วยการต่อต้านอาชญากรรมไซเบอร์*. สืบค้นเมื่อวันที่ ๒๘ กุมภาพันธ์ ๒๕๖๘, จาก https://www.mfa.go.th/th/content/thai-adopt-cybercrime-th

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (MDES). *พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐*. สืบค้นเมื่อวันที่ ๑ มีนาคม ๒๕๖๘, จาก https://www.mdes.go.th/law/detail/๓๕๑๖

กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี. *สถิติความเสียหายสะสมตั้งแต่วันที่ ๑ มกราคม ๒๕๖๘ ถึงวันที่ ๒๑ มีนาคม ๒๕๖๘*. สืบค้นเมื่อวันที่ ๒๒ มีนาคม ๒๕๖๘, จาก https://www.thaipoliceonline.com/

เขมชาติ ประกายหงส์มณี. *อาชญากรรมออนไลน์*. สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘, จาก https://www.oscc.consulting/media/๒๗๒

คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์. *ความรู้ทางกฎหมายหลากหลายและเข้าใจง่าย ชุดที่ ๒๐ : CYBER CRIME เมื่อโลกออนไลน์ เต็มไปด้วยอาชญากรรม : อาชญาวิทยาและบทบาทของกฎหมาย*. สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘, จาก https://www.law.tu.ac.th/tulawinfographic๒๐/

คำอธิบายลักษณะคดี ออกตามความใน ข้อ ๕ ของคำสั่งสำนักงานตำรวจแห่งชาติ ที่ ๑๘๒/๒๕๖๖ ลงวันที่ ๑๗ มีนาคม ๒๕๖๖. สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘. จาก https://www.gcc.go.th/wp-content/uploads/๒๐๒๔/๐๓/๖๗_cybercrime_๑๔type.pdf

จะเด็ด คุณคงกฤต. *Global Cybersecurity Index ๒๐๒๔*. สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘, จาก https://www.facebook.com/photo?fbid=๑๐๒๓๒๑๕๕๑๓๕๒๙๑๓๒๕&set=a.๑๒๓๐๔๖๔๔๑๑๙๕๓

จันทพร ศรีโพน. *ปฏิญญาอาเซียนว่าด้วยการป้องกันและต่อต้านอาชญากรรมไซเบอร์และบทวิเคราะห์กฎหมายไทยที่เกี่ยวข้อง*. สืบค้นเมื่อวันที่ ๒๘ กุมภาพันธ์ ๒๕๖๘. จาก https://lawforasean.krisdika.go.th/Content/View?Id=๓๔๙&Type=๑

ไทยพีบีเอส. *พิษอาชญากรรมออนไลน์ปี ๖๘ เกือบ ๒ เดือนสูญ ๓.๔ พันล้าน*. สืบค้นเมื่อวันที่ ๑ มีนาคม ๒๕๖๘, จาก https://www.thaipbs.or.th/news/content/๓๔๙๒๔๘

ไทยพับลิก้า. *สิงคโปร์แก้ไขกฎหมายความปลอดภัยไซเบอร์ยกระดับการกำกับดูแลผลประโยชน์ประเทศ*. สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘, จาก https://thaipublica.org/๒๐๒๔/๐๕/asean-weekly-roundup-๒๔๙/

นงลักษณ์ อัจนปัญญา. *มหาวิทยาลัยสิงคโปร์จับมือหน่วยงานรัฐตั้งศูนย์ความปลอดภัยไซเบอร์*. สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘, จาก https://www.eef.or.th/news-ntu-singapore-and-csa-singapore-launch-joint-centre-for-cybersecurity-evaluation/

ปิยอร เปลี่ยนผดุง. *ทำความรู้จัก พ.ร.ก. ป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๖ และ (ร่าง) พ.ร.ก. ไซเบอร์*. สืบค้นเมื่อวันที่ ๑ มีนาคม ๒๕๖๘, จาก https://www.up.ac.th/NewsReadBlog๒.aspx?itemID=๓๓๙๙๕

ราชกิจจานุเบกษา. *พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๖*. (๑๗ มีนาคม ๒๕๖๖). เล่ม ๑๔๐ ตอนที่ ๑๘ ก, น. ๑-๗.

_____. พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ ๒) พ.ศ. ๒๕๖๘, สืบค้นเมื่อวันที่ ๒๔ เมษายน ๒๕๖๘, จาก https://ratchakitcha.soc.go.th/documents/67320.pdf

_____. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒, สืบค้นเมื่อวันที่ ๑ มีนาคม ๒๕๖๘, จาก https://www.ratchakitcha.soc.go.th/DATA/PDF/๒๕๖๒/A/๐๖๙/T_๐๐๒๐.PDF

_____. *พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒*. สืบค้นเมื่อวันที่ ๑ มีนาคม ๒๕๖๘, จาก https://www.ratchakitcha.soc.go.th/DATA/PDF/๒๕๖๒/A/๐๖๙/T_๐๐๕๒.PDF

_____. *พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐*. สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘, จาก https://ratchakitcha.soc.go.th/documents/๒๑๗๕๕๓.pdf

_____. *พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐*. สืบค้นเมื่อวันที่ ๑ มีนาคม ๒๕๖๘, จาก https://www.ratchakitcha.soc.go.th/DATA/PDF/๒๕๖๐/A/๐๑๐/๒๔.PDF

รัฐบาลไทย. *ไทย นำ อาเซียน ขับเคลื่อนอนาคตดิจิทัล มุ่งแก้ปัญหาหลอกลวงออนไลน์-สร้างความมั่นคงทางไซเบอร์ ในการประชุมรัฐมนตรีอาเซียนด้านดิจิทัล ครั้งที่ ๕ สู่อนาคตดิจิทัลที่ปลอดภัยและยั่งยืน*. สืบค้นเมื่อวันที่ ๒๘ กุมภาพันธ์ ๒๕๖๘, จาก https://www.thaigov.go.th/news/contents/ministry_details/๙๒๕๓๑

รุ่งโรจน์ กิตติถาวรกุล. *รู้ เข้าใจและตระหนัก “อาชญากรรมทางไซเบอร์” (Cybercrime) ป้องกันภัยคุกคามใกล้ตัว*. สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘, จาก https://www.chula.ac.th/news/๑๓๘๒๙๑/

ลัฐกา เนตรทัศน์. *อาเซียนกับการจัดการปัญหาอาชญกรรมไซเบอร์*. สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘, จาก https://lawforasean.krisdika.go.th/File/files/cybersecurity_dec๒.pdf

ศูนย์ข้อมูลเพื่อธุรกิจไทยในสิงคโปร์. *ยุทธศาสตร์เพื่อสร้างความเชื่อมั่นทางไซเบอร์ของสิงคโปร์*. สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘, จาก https://thaibizsingapore.com/news/main/opportunities/cyber-security-trust/

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC). *ปัญหาคอมพิวเตอร์*. สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘, จาก https://www.nectec.or.th/schoolnet/library/create-web/๑๐๐๐๐/technology/๑๐๐๐๐-๑๒๓๗๙.html

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT). *รายงาน MITRE ATT&CK Matrix ประจำเดือนธันวาคม ปี ๒๕๖๗*. สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ มกราคม ๒๕๖๘, จาก https://drive.ncsa.or.th/s/eQx๒Y๓yP๓๒oaQpN

_____. *รายชื่อ CERT ในประเทศไทย*. สืบค้นเมื่อวันที่ ๒๘ กุมภาพันธ์ ๒๕๖๘. จาก https://www.thaicert.or.th/%E๐%B๘%AB%E๐%B๘%๙๙%E๐%B๙%๘๘%E๐%B๘%A๗%E๐%B๘%A๒%E๐%B๘%๘๗%E๐%B๘%B๒%E๐%B๘%๙๙-cert/

สถานเอกอัครราชทูต ณ สิงคโปร์, ศูนย์ข้อมูลเพื่อธุรกิจไทย (BIC). *สิงคโปร์ยกระดับระบบดิจิทัลเพื่อความมั่นคงทางไซเบอร์*. สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘, จาก https://thaibizsingapore.com/news/main/strategies/reinforce-cybersecurity/

สภาผู้แทนราษฎร. (๒๕๖๗). *รายงานผลการพิจารณาศึกษาของคณะอนุกรรมาธิการบังคับใช้และแก้ไขกฎหมายว่าด้วยการป้องกันปราบปรามอาชญากรรมทางเทคโนโลยี*. กรุงเทพฯ : สำนักงานเลขาธิการสภาผู้แทนราษฎร.

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (NCSA). *กฎหมายลำดับรอง*. สืบค้นเมื่อวันที่ ๒๘ กุมภาพันธ์ ๒๕๖๘. จาก https://drive.ncsa.or.th/s/m๗m๘๙wj๓ywgSXfJ?fbclid=IwY๒xjawJNB๓hleHRuA๒FlbQIxMAABHYihfLKS๘HxX๙aQRPlY_๒i๙BvsZc๑sY๐th๕btfvv๘F๑LbhNg๖RudZ๕gfnQ_aem_๘๒yEjCilQcRAwmktwLIrQg

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA). *พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ (ฉบับอัพเดท)*. สืบค้นเมื่อวันที่ ๑ มีนาคม ๒๕๖๘. จาก https://www.etda.or.th/th/Useful-Resource/กฎหาย-HTML/

สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน). *รายงานความมั่นคงปลอดภัยทางไซเบอร์ของโลก (Global Cybersecurity Index)*. สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘, จาก https://www.dga.or.th/wp-content/uploads/๒๐๒๑/๐๒/๗.pdf

Cyber Security Agency of Singapore (CSA). *About Singapore Cyber Emergency Response Team (SingCERT)*. สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘, จาก https://www.csa.gov.sg/resources/singcert

International Telecommunication Union (ITU). *GCI scope and framework*. สืบค้นเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘, จาก https://www.itu.int/en/ITU-/Cybersecurity/Documents/GCIv๔/New_Reference_Model_GCIv๔_V๒_.pdf