

อาชญากรรมทางเทคโนโลยี ภัยคุกคามและการป้องกันในประเทศไทย

จากปัญหาแก๊งคอลเซ็นเตอร์มีอาชญากรรม และบรรดาเว็บพนันออนไลน์ ล่อลวงให้เสียทรัพย์ที่คุกคามระบอบหลัก และภาครัฐกำลังเร่งปราบปรามกันอยู่ในเวลานี้ จึงเป็นเรื่องที่เราทุกคนต้องมาตระหนักถึงภัยอาชญากรรมรูปแบบใหม่ๆ เพื่อเป็นวัคซีนป้องกันตัวในยุคสมัยนี้ไปด้วยกัน

อาชญากรรมทางเทคโนโลยี อาชญากรรมทางคอมพิวเตอร์ หรืออาชญากรรมไซเบอร์ (Cybercrime) เป็นการกระทำความผิดกฎหมายโดยใช้คอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์เป็นเครื่องมือในการก่อให้เกิดความเสียหายและ/หรือ แสวงหาผลประโยชน์ส่วนตัวโดยมิชอบด้วยกฎหมาย การทุจริตหลอกลวงให้โอนเงินจากบัญชี หรือ ชักจูงชวนเชื่อเล่นพนันออนไลน์ ที่เกิดขึ้นบนโลกอินเทอร์เน็ต

และช่องทางออนไลน์ต่างๆ อาทิ เว็บไซต์ โซเชียลมีเดีย หรือ แอปพลิเคชันบนโทรศัพท์มือถือ ไม่ว่าจะมาในรูปแบบใด ล้วนมีเป้าหมายเดียวคือมุ่งแสวงหาผลประโยชน์ โดยทำให้เราเสียทรัพย์หรือตกเป็นผู้เสียหาย จากสถิติของ thaipoliceonline.com ข้อมูลเฉพาะเดือนมกราคม 2568 พบว่ามีมูลค่าความเสียหายรวมสูงถึงราว 3 พันล้านบาท จากคดีออนไลน์มากกว่า 3 หมื่นเรื่อง

สถิติความเสียหายสะสม ตั้งแต่วันที่ 1 มกราคม 2568 ถึง วันที่ 8 กุมภาพันธ์ 2568

คดีออนไลน์

39,828

เรื่อง

มูลค่าความเสียหายรวม

3,035,458,117

บาท

ภัยคุกคามทางอาชญากรรมไซเบอร์

ปัจจุบันภัยอาชญากรรมไซเบอร์มีการพัฒนาเปลี่ยนแปลงรูปแบบและวิธีการหลอกลวงที่หลากหลาย ปรับเปลี่ยนไปตามบริบทและการรับรู้ของสังคม ตัวอย่างของภัยคุกคามที่พบเจอได้บ่อยและต้องรู้เท่าทัน ได้แก่

1. การโจมตีทางไซเบอร์ (cyber attack) หรือเจาะระบบคอมพิวเตอร์ (hacking) เพื่อมุ่งขโมยข้อมูลส่วนบุคคล ข้อมูล หรือกระทำการผิดกฎหมายอื่นๆ บนระบบคอมพิวเตอร์ของหน่วยงานรัฐ ธนาคาร บริษัท โรงพยาบาล ฯลฯ หรือแม้แต่บัญชีอีเมล บัญชีโซเชียลมีเดียรายบุคคล ก็อาจจะถูกโจมตีขโมยข้อมูลหรือยึดบัญชีไปเลยได้เช่นกัน
2. หลอกลวงซื้อขายสินค้าและบริการ แต่ไม่ได้สินค้า หรือได้แต่ไม่ตรงหรือไม่มีความคุณภาพตามที่อ้าง
3. หลอกให้โอนเงิน อ้างเพื่อสมัครทำงานหารายได้พิเศษ หรือเพื่อรับรางวัลหรือสิทธิประโยชน์
4. หลอกลวงให้กู้เงิน หรือลงทุนผ่านระบบคอมพิวเตอร์ อันมีลักษณะฉ้อโกง กรรโชก ริดเอาทรัพย์สิน หรือที่เป็นความผิดตาม พ.ร.ก.กู้ยืมเงินฯ
5. ชุมชู่ทางโทรศัพท์ให้เกิดความกลัวเพื่อหลอกโอนเงิน (call center) เช่น ปลอมเป็นตำรวจ สรรพากร ธนาคาร
6. หลอกลวงเป็นบุคคลที่รู้จักเพื่อขอยืมเงิน โอนเงิน
7. หลอกลวงให้ติดตั้งโปรแกรม แอปพลิเคชัน เพื่อเข้าควบคุมระบบโทรศัพท์มือถือแล้วโอนเงินออกไปยังบัญชีม้า
8. ชักจูงให้เข้าไปยังเว็บไซต์หลอกลวง (phishing web) หรือให้เข้าไปเล่นเว็บไซต์บ่อนการพนันออนไลน์
9. หลอกให้รัก แล้วขอให้โอนเงินให้ (romance scam)
10. หลอกให้ส่งรูปวาบหวามเซ็กซี่ส่วนตัว เพื่อแลกเงิน
11. หลอกลวงหรือว่าจ้างให้ข้อมูลส่วนบุคคลเพื่อเปิดบัญชีม้าหรือเบอร์ม้า

เจ้าของมีความผิดโทษหนักถึงจำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 3 แสนบาท หรือทั้งจำทั้งปรับได้ ยิ่งทำตนเป็นธุระจัดหา โฆษณา ให้เกิดบัญชีม้าหรือเบอร์ม้า โทษจำคุกตั้งแต่ 2-5 ปี หรือปรับตั้งแต่ 2-5 แสนบาท หรือทั้งจำทั้งปรับเลยทีเดียว

ปัจจุบันคณะรัฐมนตรีมีมติเห็นชอบร่างแก้ไขเพิ่มเติมพระราชกำหนด (พ.ร.ก.) มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ฉบับปี พ.ศ. 2566 ซึ่งคาดว่าจะประกาศบังคับใช้ พ.ร.ก. ฉบับแก้ไขเพิ่มเติมดังกล่าว ได้ในเดือนกุมภาพันธ์นี้ โดยมีการปรับปรุงเพิ่มเติมในหลายประเด็น มีสาระสำคัญหลัก อาทิ

- เพิ่มหน้าที่ให้ กสทช. หรือผู้ให้บริการโทรศัพท์มือถือ มีหน้าที่สั่งระงับการให้บริการหมายเลขโทรศัพท์มือถือเป็นการชั่วคราว เมื่อพบเหตุอันควรสงสัยหรือได้รับข้อมูลว่าอาจเกี่ยวข้องกับการกระทำความผิด
- กำหนดให้แพลตฟอร์มตลาดจนสถาบันการเงิน ต้องร่วมรับผิดชอบการทำธุรกรรมและการกระทำความผิดที่เกิดขึ้น เช่น การไม่ปฏิเสธการเปิดบัญชีม้า การห้ามซื้อขายสินทรัพย์ดิจิทัลผ่านแพลตฟอร์ม Peer-to-Peer Lending (P2P) โดยห้ามให้บริการหรือแสดงว่าพร้อมจะให้บริการซื้อขายหรือแลกเปลี่ยนสินทรัพย์ดิจิทัลประเภทคริปโตเคอร์เรนซี โทเคนดิจิทัลเพื่อการใช้ประโยชน์ที่มีวัตถุประสงค์หลักเพื่อการอุปโภคบริโภค เพื่อลดปัญหาการฟอกเงิน โดยนำมาเปลี่ยนเป็นเงินสดดิจิทัล
- เพิ่มบทกำหนดโทษสำหรับการฟอกเงินเป็นสกุลเงินดิจิทัล และการเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล
 - ผู้ประกอบการธุรกิจสินทรัพย์ดิจิทัลที่นำเงินที่ได้จากการกระทำความผิดออนไลน์มาฟอกเงินโดยนำมาเปลี่ยนเป็นเงินสดดิจิทัล ต้องระวางโทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1 แสนบาท หรือทั้งจำทั้งปรับ
 - ผู้กระทำความผิดเกี่ยวกับการพนันออนไลน์ ต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 1 แสนบาท หรือทั้งจำทั้งปรับ
 - ผู้ซื้อขายข้อมูลส่วนบุคคล ต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 5 ล้านบาท หรือทั้งจำทั้งปรับ
- ให้สถาบันการเงินหรือผู้ให้บริการเครือข่ายโทรศัพท์ ผู้ให้บริการอื่นที่เกี่ยวข้อง หรือสื่อสังคมออนไลน์ มีส่วนรับผิดชอบในความเสียหายที่เกิดขึ้นกับผู้เสียหาย

- เร่งรัดกระบวนการคืนเงินให้กับผู้เสียหาย ให้อำนาจแก่คณะกรรมการธุรกรรม ตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน เป็นผู้ตรวจสอบและพิจารณาคืนเงินให้แก่ผู้เสียหาย โดยไม่ต้องรอให้มีการยื่นฟ้องคดีต่อศาลเพื่อพิจารณามีคำสั่งถึงที่สุดก่อน ทำให้การคืนเงินแก่ผู้เสียหายเป็นไปอย่างรวดเร็วขึ้น

การปรับปรุง พ.ร.ก. ฉบับนี้ ถือเป็นหนึ่งในเครื่องมือสำคัญในการปราบปรามแก๊งคอลเซ็นเตอร์มิจฉาชีพ หรือ

อาชญากรรมไซเบอร์ในรูปแบบต่างๆ ประกอบกัน ให้อำนาจได้ทันต่อเหตุภัยคุกคามที่เปลี่ยนแปลงไปตามสมัย

รู้จักกับหน่วยงานป้องกันอาชญากรรมทางเทคโนโลยีของไทย

แน่นอนว่าการป้องกันและปราบปรามอาชญากรรมต้องเป็นบทบาทหน้าที่โดยตรงของตำรวจ ซึ่งสำนักงานตำรวจแห่งชาติ (ตร.) มีหน่วยงานส่วนสนับสนุนป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีของประเทศไทย ได้แก่

● กองบัญชาการตำรวจสอบสวนกลาง (บช.ก.) (Central Investigation Bureau; CIB)

- กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี; บก.ปอท. (Technology Crime Suppression Division; TCSD)

หรือที่รู้จักกันในชื่อ “ตำรวจ ปอท.” มีอำนาจหน้าที่และความรับผิดชอบเกี่ยวกับการรักษาความสงบเรียบร้อย ป้องกันและปราบปราม สืบสวนสอบสวนคดีอาชญากรรมทางคอมพิวเตอร์ เช่น การแฮ็กข้อมูล การละเมิดลิขสิทธิ์ออนไลน์ การหมิ่นประมาทผ่านสื่อออนไลน์ ฯลฯ ปฏิบัติงานตามประมวลกฎหมายวิธีพิจารณาความอาญา และตามกฎหมายอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ก่อตั้งขึ้นจากการประกาศใช้ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จึงต้องมีการปรับโครงสร้างหน่วยงาน บช.ก. ตามพระราชกฤษฎีกาแบ่งส่วนราชการสำนักงานตำรวจแห่งชาติ พ.ศ. 2552 โดยเกลี่ยอัตรากำลังจากกองบังคับการสืบสวนสอบสวนคดีเศรษฐกิจ ออกมาเป็น บก.ปอท. เมื่อวันที่ 7 กันยายน 2552 เป็นต้นมา

CIB
ตำรวจสอบสวนกลาง



● กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) (Cyber Crime Investigation Bureau; CCIB)

- กองบังคับการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี 1-5
- กองบังคับการตรวจสอบและวิเคราะห์อาชญากรรมทางเทคโนโลยี

หรือที่รู้จักกันในชื่อ “ตำรวจไซเบอร์” ก่อตั้งขึ้นเมื่อวันที่ 9 กันยายน 2563 ตามพระราชกฤษฎีกาแบ่งส่วนราชการสำนักงานตำรวจแห่งชาติ (ฉบับที่ 5) พ.ศ. 2563 ให้มีอำนาจหน้าที่เป็นฝ่ายอำนวยการด้านยุทธศาสตร์ให้สำนักงานตำรวจแห่งชาติ ในการวางแผน ควบคุม ตรวจสอบ ให้คำแนะนำ และเสนอแนะการปฏิบัติงานตามอำนาจหน้าที่ของ บช.สอท. และหน่วยงานในสังกัด ดำเนินการเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีทั่วราชอาณาจักร ปฏิบัติงานตามประมวลกฎหมายวิธีพิจารณาความอาญา กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และกฎหมายอื่นอันเป็นความผิดทางอาญาเกี่ยวกับอาชญากรรมทางเทคโนโลยีและความผิดอื่นที่เกี่ยวข้อง โดยมีหน้าที่สืบสวนสอบสวนโดยใช้เทคโนโลยีสารสนเทศและเครื่องมือพิเศษ ดำเนินการรวบรวมข้อมูล ตรวจสอบ และวิเคราะห์การกระทำผิดทางเทคโนโลยี พิสูจน์หลักฐานดิจิทัล ตรวจสอบสถานที่เกิดเหตุและเก็บรวบรวมพยานหลักฐานดิจิทัล ประสานความร่วมมือกับหน่วยงานที่เกี่ยวข้องทั้งในและต่างประเทศ ซึ่งจะมีความซับซ้อนหรือมีขนาดใหญ่ระดับประเทศ เช่น แก๊งคอลเซ็นเตอร์ การพนันออนไลน์ การฟอกเงินผ่านระบบดิจิทัล เป็นต้น



นอกเหนือจากหน่วยงานตำรวจ ยังมีอีกหลายหน่วยงานของรัฐที่มีบทบาทบูรณาการร่วมกันป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ที่สำคัญไม่แพ้กันอีกหลายหน่วยงาน อาทิ

● กรมสอบสวนคดีพิเศษ (กคพ.) (Department of Special Investigation; DSI) สังกัด กระทรวงยุติธรรม



• กองคดีเทคโนโลยีและสารสนเทศ

ดีเอสไอ ก่อตั้งขึ้นเมื่อวันที่ 3 ตุลาคม 2545 ตามพระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม พ.ศ. 2545 โดยปฏิบัติหน้าที่สืบสวนสอบสวน เฉพาะคดีอาชญากรรมพิเศษ ที่มีความซับซ้อนหรือส่งผลกระทบต่อสังคมในวงกว้าง กระทั่งต่อเศรษฐกิจหรือความสัมพันธ์ระหว่างประเทศ หรือเป็นองค์กรอาชญากรรม เป็นผู้มีอิทธิพลสำคัญเป็นตัวการเชื่อมโยงทั้งในและข้ามชาติ ภายใต้บทบาทหน้าที่ตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 ซึ่งจะไม่ทับซ้อนกับตำรวจ แต่จะบูรณาการการทำงานร่วมกัน

● สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) (National Cyber Security Agency; NCSA) สังกัด กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม



สกมช. ก่อตั้งขึ้นเมื่อวันที่ 28 พฤษภาคม 2562 ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยมีวัตถุประสงค์เพื่อกำหนดนโยบาย มาตรการ แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานภาครัฐและภาคเอกชนที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ

ตลอดจนประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน เฝ้าระวัง ติดตาม วิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ เป็นศูนย์กลาง ส่งเสริม สนับสนุน ศึกษาและวิจัยข้อมูลที่เป็น ความเสี่ยงและเหตุการณ์ต่างๆ มาเผยแพร่เสริมสร้างความรู้ความเข้าใจ ตลอดจนดำเนินการฝึกอบรมเพื่อยกระดับความเชี่ยวชาญในการรักษาความมั่นคงปลอดภัยไซเบอร์ และแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ ให้กับหน่วยงานของรัฐและเอกชน

● สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) (Office of the Personal Data Protection Commission; PDPC)



สคส. ก่อตั้งขึ้นตามมาตรา 43 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยมีวัตถุประสงค์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งส่งเสริมและสนับสนุนให้เกิดการพัฒนาเทคโนโลยี ด้านการคุ้มครองข้อมูลส่วนบุคคลของประเทศ สํารวจ เก็บรวบรวมข้อมูล ติดตามความเคลื่อนไหว วิเคราะห์ วิจัย ตลอดจนให้คำปรึกษา บริการทางวิชาการ ฝึกอบรม เผยแพร่ให้ความรู้ และประสานงานกับหน่วยงานของรัฐ เอกชน และประชาชนทั่วไป เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

วิธีป้องกัน คำแนะนำ สำหรับประชาชนทั่วไป

1 ตั้งสติ ตรวจสอบข้อความที่ได้รับอย่างระมัดระวัง หากอ้างว่าเป็นเจ้าหน้าที่หรือหน่วยงานติดต่อมาไม่ว่าเรื่องใด ให้โทรสอบถามจากเบอร์กลางของหน่วยงานนั้นเองทุกครั้ง อย่าโทรกลับไปทันทีตามเบอร์ที่เจ้าหน้าที่ต้องสงสัยนี้ให้ไว้

2 ห้ามกดลิงก์ หรือติดตั้งแอปพลิเคชันที่ไม่ทราบที่มา ที่ไป รวมถึงต้องไม่กรอกข้อมูลส่วนตัวใดๆ ลงไปในแอปฯ นั้น

3 หากเผลอกดลิงก์หรือติดตั้งแอปฯ แอปพลิเคชันนั้นไปแล้ว ให้รีบตัดสัญญาณอินเทอร์เน็ตทันที หากเป็นมือถือหรือ

แท็บเล็ตให้รีบเปิดโหมดเครื่องบิน หากเป็นคอมพิวเตอร์ให้ปิด Wi-Fi หรือ LAN จากนั้นทำการถอนการติดตั้งแอปฯ นั้น หรือ รีเซ็ตเครื่องใหม่ทันที

4 สำหรับผู้สูงอายุตามบ้านที่ยังสามารถพูดคุยรับ สายโทรศัพท์เองได้ ไม่ว่าจะมีการโทรมาอ้างเรื่องเร่งด่วนใด ก็ตาม ซึ่งมักลงท้ายด้วยการให้โอนเงิน ควรปรึกษาบุตรหลาน ในครอบครัวที่ไว้ใจได้ หรือให้รับเรื่องแทนไว้ก่อน อย่าเพิ่งหลง เชื่อในทันที เพราะมีฉ้อฉลมีกรับเร่งให้ดำเนินการในทันที แล้ว ปฏิบัติตามข้อ 1-3 ข้างต้น

จะตรวจสอบว่าจริงหรือปลอมได้ที่ไหน

หากไม่มั่นใจในการตรวจคัดกรองด้วยตนเอง ท่านสามารถตรวจสอบข้อมูลต้องสงสัยต่างๆ ได้ ผ่านช่องทางออนไลน์ของตำรวจไซเบอร์ ดังนี้

1. ดาวน์โหลดแอปพลิเคชัน “Cyber Check” ให้เป็นผู้ช่วยสแกนเบอร์โทรเข้าออก ตรวจสอบข้อความ SMS เพื่อแจ้งเตือนก่อนการรับสายหรือก่อนลิงก์ไปยังเว็บไซต์ที่มีความเสี่ยง ซึ่งอาจช่วยปกป้องคุณจากคอลเซ็นเตอร์มิจฉาชีพได้

2. เช็กข้อมูลด้วยตนเองผ่าน “ศูนย์บริการเช็กข้อมูล และแจ้งบัญชีต้องสงสัย” ได้ที่เว็บไซต์ “เช็กก่อน.com” (หรือ checkgon.com หรือ checkgon.go.th ก็ได้เช่นกัน) สามารถแจ้งเบาะแสภัยออนไลน์ เช็กบัญชีธนาคาร เช็กเบอร์ต้องสงสัย



เช็กเว็บปลอม ได้ และยังมีข่าวเตือนภัยออนไลน์ รู้ทันกลโกง จับคนโกง ข้อมูลสถิติประเภทคดี สถิติการแจ้งเบาะแส ให้บริการไว้เบ็ดเสร็จในเว็บไซต์เดียว



โดนเข้าให้แล้ว ต้องทำอะไร !!

ในกรณีที่โดนหลอกลวงให้โอนเงินและเข้าข่าย อาชญากรรมทางเทคโนโลยีแล้ว ต้องรีบแจ้งธนาคาร และ “แจ้งความออนไลน์” คดีอาชญากรรมทางเทคโนโลยี ผ่านทาง “ศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ” หรือรู้จัก

กันในชื่อ “ศูนย์ AOC 1441” เพื่อขออายัดบัญชี หรือขอคำปรึกษาในการแจ้งความได้ตลอด 24 ชั่วโมง โดยสามารถดำเนินการได้ที่



กองบัญชาการ
ตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี
CYBER CRIME INVESTIGATION BUREAU



แจ้งความออนไลน์
คดีอาชญากรรมทางเทคโนโลยี

📄 แจ้งความออนไลน์ 📞 สายด่วน 1441 📱 ตำรวจไซเบอร์ บข.สก.




Website : thaipoliceonline.com
LINE OA : @police1441
สายด่วน โทร. 1441

อาชญากรรมทางเทคโนโลยี เป็นภัยคุกคามสมัยใหม่ต่อหน่วยงานภาครัฐ หน่วยงานเอกชน ประชาชนทั่วไป ที่สร้างความเสียหายต่อระบบเศรษฐกิจ และงบประมาณของประเทศ ในการสืบสวน สอบสวน ป้องกัน ปราบปราม และรักษาความมั่นคงปลอดภัยทางไซเบอร์ของข้อมูลส่วนบุคคล ธุรกรรมทางการเงินต่างๆ เป็นจำนวนมาก จึงเป็นเรื่องสำคัญที่ไม่ใช่หน้าที่ของรัฐแต่เพียงลำพัง แต่ต้องรวมถึงผู้ประกอบการภาคเอกชน และประชาชนทุกคนต้องร่วมด้วยช่วยกันขับเคลื่อน สร้างสำนึกและสังคมแห่งการตระหนักรู้เท่าทันภัยคุกคามที่มากับเทคโนโลยีนี้ไปด้วยกัน

เอกสารอ้างอิง

- กรมสอบสวนคดีพิเศษ. 2568. [ออนไลน์]. เข้าถึงได้จาก: <https://www.dsi.go.th/>, [เข้าถึงเมื่อ 30 มกราคม 2568].
- กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี. 2568. [ออนไลน์]. เข้าถึงได้จาก: <https://tcsd.go.th/>, [เข้าถึงเมื่อ 30 มกราคม 2568].
- กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี. 2568. [ออนไลน์]. เข้าถึงได้จาก: <https://www.ccib.go.th/>, [เข้าถึงเมื่อ 30 มกราคม 2568].
- สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล. 2568. [ออนไลน์]. เข้าถึงได้จาก: <https://www.pdpc.or.th/>, [เข้าถึงเมื่อ 30 มกราคม 2568].
- ศูนย์บริการเช็กข้อมูลและแจ้งบัญชีต้องสงสัย. 2568. [ออนไลน์]. เข้าถึงได้จาก: <https://www.checkgon.com>, [เข้าถึงเมื่อ 9 กุมภาพันธ์ 2568].
- BBC Thai. 2568. พ.ร.ก.ไซเบอร์ ฉบับใหม่ ให้ธนาคาร-ค่ายมือถือร่วมรับผิดชอบ จะลดปัญหาแก๊งคอลเซ็นเตอร์ได้หรือไม่ ?. [ออนไลน์]. เข้าถึงได้จาก: <https://www.bbc.com/thai/articles/c20p51zdqnlo>, [เข้าถึงเมื่อ 30 มกราคม 2568].