ความมั่นคงปลอดภัยทางไซเบอร์ในการทำงานและการป้องกันการหลอกลวง

โดย ศูนย์เทคโนโลยีดิจิทัล มหาวิทยาลัยวลัยลักษณ์

ในยุคดิจิทัลที่เทคโนโลยีเข้ามามีบทบาทในทุกมิติของการทำงาน ความมั่นคงปลอดภัยทางไซเบอร์จึงกลายเป็นสิ่งสำคัญที่ทุกคนไม่ควรมองข้าม ไม่ว่าจะเป็นการใช้ระบบออนไลน์ การจัดเก็บข้อมูล หรือการสื่อสารผ่านเครือข่าย ล้วนมีความเสี่ยงต่อการถูกโจมตีหรือหลอกลวงทางไซเบอร์ เช่น การขโมยข้อมูล การแพร่กระจายมัลแวร์ หรือการฟิชชิงเพื่อหลอกเอารหัสผ่านและข้อมูลสำคัญ

การมีความรู้ ความเข้าใจ และการปฏิบัติตามแนวทางด้านความมั่นคงปลอดภัยทางไซเบอร์อย่างถูกต้อง ไม่เพียงแต่ช่วยป้องกันความเสียหายต่อตนเอง แต่ยังช่วยเสริมสร้างความปลอดภัยโดยรวมให้กับมหาวิทยาลัยด้วย เนื้อหานี้จะช่วยให้ผู้อ่านตระหนักถึงภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นในที่ทำงาน และเรียนรู้วิธีการป้องกันตนเองจากการถูกหลอกลวงหรือโจมตีทางเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพ เนื้อหาในเอกสารนี้ประกอบด้วย 8 หัวข้อดังต่อไปนี้

1. ความสำคัญของการรักษาความมั่นคงปลอดภัยทางไซเบอร์
2. แนวคิดในการรักษาความมั่นคงปลอดภัยของข้อมูล
3. ประเภทของภัยคุกคามทางไซเบอร์
4. ผลกระทบจากภัยคุกคามทางไซเบอร์ต่อมหาวิทยาลัย
5. กฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล
6. กรณีศึกษาการหลอกลวงทางออนไลน์
7. Security Checklist
8. Digital Footprint และการปกป้องข้อมูลส่วนบุคคล

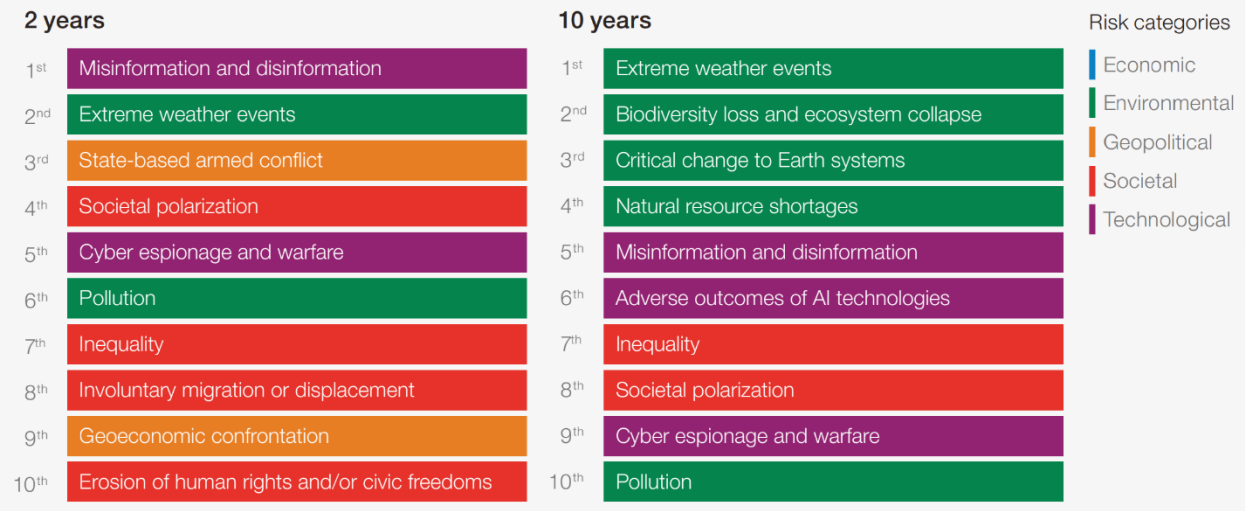
1. ความสำคัญของการรักษาความมั่นคงปลอดภัยทางไซเบอร์

การดำเนินชีวิตในยุคปัจจุบันมีความเสี่ยงหลากหลายรูปแบบเพิ่มขึ้น ข้อมูลจากรายงาน Global Risks Report 2025 ของ World Economic Forum ที่ได้ทำแบบสำรวจและเก็บข้อมูลที่เกิดขึ้นระหว่างวันที่ 2 กันยายน – 18 ตุลาคม 2024 สรุปผลได้ดังรูปที่ 1 จะเห็นได้ว่ามีความเสี่ยงทางด้านเทคโนโลยี (แถบสีม่วง) ติดอันดับ Top 10 ความเสี่ยงของโลกทั้งแบบ Short term และ Long term ซึ่งสามารถกล่าวโดยสรุปเกี่ยวกับความเสี่ยงด้านเทคโนโลยีได้ 3 กลุ่มดังต่อไปนี้

1) **ข้อมูลเท็จและบิดเบือน (Misinformation and disinformation):** การแพร่กระจายข้อมูลที่เป็นเท็จหรือจงใจบิดเบือนเพื่อเปลี่ยนแปลงความคิดเห็นของสาธารณะและลดความเชื่อมั่นในข้อเท็จจริง

2) **การจารกรรมและสงครามไซเบอร์ (Cyber espionage and warfare)**: การใช้เทคโนโลยีดิจิทัลหรือระบบคอมพิวเตอร์ในการล้วงข้อมูลหรือโจมตีทางไซเบอร์ โดยมีวัตถุประสงค์ด้านความมั่นคงของชาติ การเมือง หรือเศรษฐกิจ โดยลักลอบเข้าถึงข้อมูลลับ ก่อกวนการปฏิบัติงาน หรือทำลายเครือข่ายเทคโนโลยีและข้อมูลของทั้งภาครัฐและเอกชน

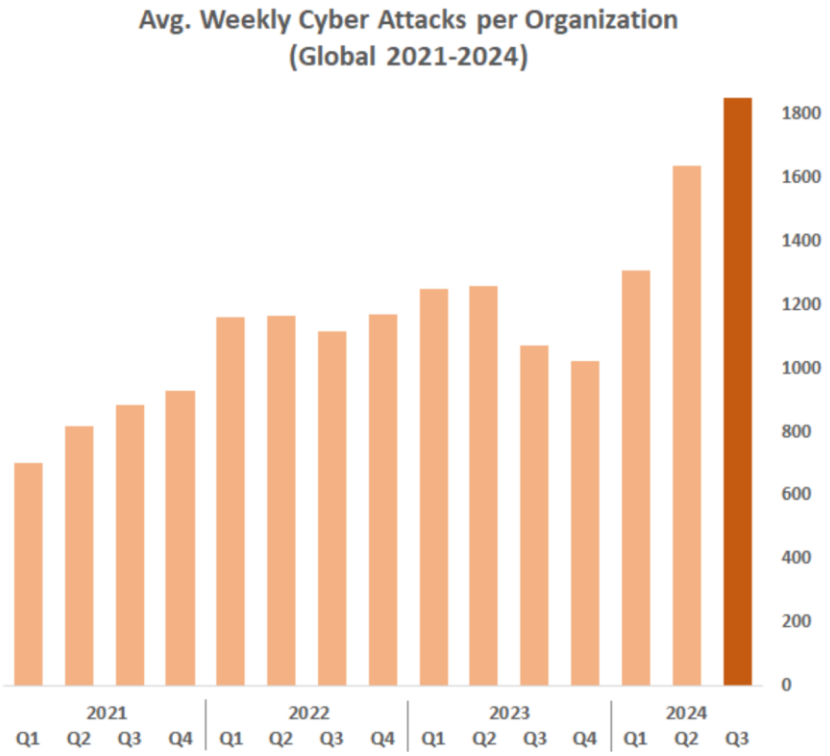
3) **ความเสี่ยงจาก AI (Adverse outcomes of AI technologies)**: ผลกระทบเชิงลบที่เกิดจากการใช้งาน AI รวมถึง Generative AI ทั้งโดยเจตนาและไม่เจตนา เช่น ความลำเอียงในการตัดสินใจ (เนื่องจากข้อมูลที่ใช้สอน AI ไม่เป็นกลาง) การละเมิดความเป็นส่วนตัว การตัดสินใจที่ผิดพลาด เช่น อุบัติเหตุจากรถยนต์ไร้คนขับ รวมถึงการนำ AI ไปใช้ในทางที่ผิด เช่น การสร้างข่าวปลอม หรือควบคุมอาวุธอัตโนมัติ เป็นต้น



รูปที่ 1 Global Risks จัดลำดับตามความรุนแรง ทั้งในช่วง Short term (2 ปี) และ Long term (10 ปี)

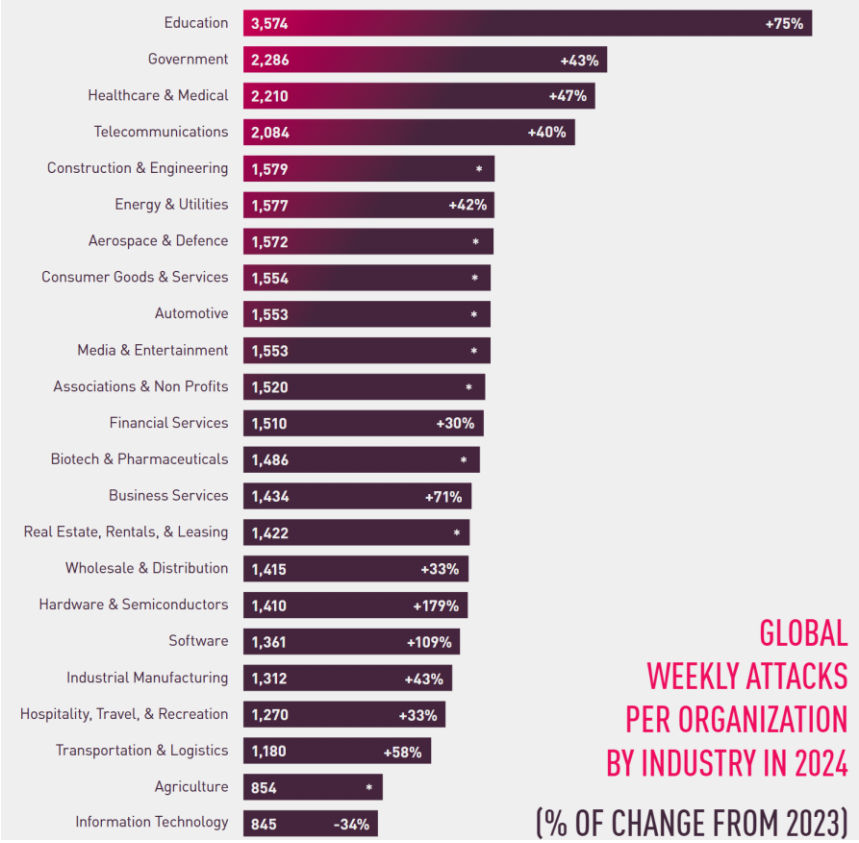
ในทำนองเดียวกัน ข้อมูล Cyber Security Report จากเว็บไซต์ Check Point ระบุว่าการโจมตีทางไซเบอร์ทั่วโลกพุ่งสูงขึ้นกว่า 75% ดังรูปที่ 2 และมีสถิติการโจมตีที่น่าสนใจดังนี้

- **จำนวนการโจมตีที่พุ่งสูงเป็นประวัติการณ์**: ในไตรมาสที่ 3 ปี 2024 มีการบันทึกการโจมตีทางไซเบอร์เฉลี่ย 1,876 ครั้งต่อองค์กร ซึ่งเพิ่มขึ้น 75% เมื่อเทียบกับช่วงเวลาเดียวกันในปี 2023 และเพิ่มขึ้น 15% เมื่อเทียบกับไตรมาสก่อนหน้า
- **การแยกย่อยตามอุตสาหกรรม**: ภาคการศึกษา/การวิจัยเป็นเป้าหมายมากที่สุด โดยมีการโจมตี 3,828 ครั้งต่อสัปดาห์ รองลงมาคือภาครัฐบาล/ทหาร และภาคการดูแลสุขภาพ โดยมีการโจมตี 2,553 และ 2,434 ครั้ง ตามลำดับ
- **ระดับภูมิภาค**: แอฟริกาเผชิญกับการโจมตีเฉลี่ยสูงสุดที่ 3,370 ครั้งต่อสัปดาห์ (เพิ่มขึ้น 90% เมื่อเทียบกับปีก่อนหน้า) ในขณะที่ยุโรปและลาตินอเมริกาก็พบว่าเพิ่มขึ้นอย่างมีนัยสำคัญเช่นกัน
- **Ransomware**: เป็นภัยคุกคามที่ยังคงมีอยู่อย่างต่อเนื่อง มีรายงานเหตุการณ์ Ransomware มากกว่า 1,230 ครั้ง โดยอเมริกาเหนือได้รับผลกระทบมากที่สุด (57% ของเหตุการณ์) รองลงมาคือยุโรป (24% ของเหตุการณ์)

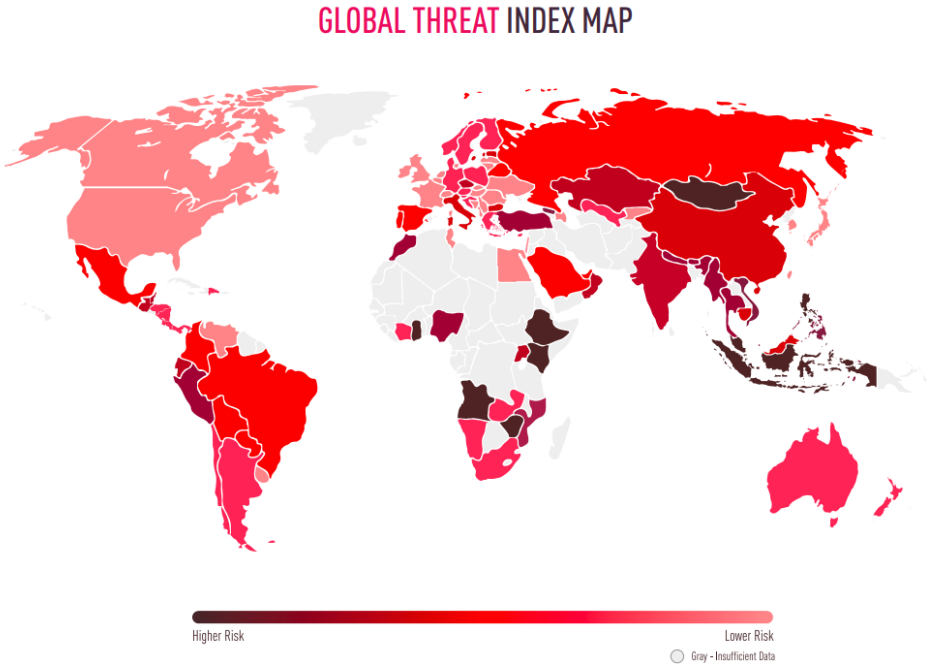


รูปที่ 2 แสดงจำนวนการโจมตีทางไซเบอร์ระหว่างปี 2021 ถึง 2024

เมื่อพิจารณาเป้าหมายการโจมตีทางไซเบอร์ตามกลุ่มอุตสาหกรรม จะเห็นได้ว่ากลุ่มเป้าหมายอันดับ 1 ในปี 2024 คือ องค์กรด้านการศึกษา ตามด้วยหน่วยงานรัฐบาล รายละเอียดดังรูปที่ 3 โดยองค์กรด้านการศึกษามีจำนวนครั้งการโจมตีต่อสัปดาห์เพิ่มสูงขึ้นถึง 75% และประเทศไทยก็อยู่ในกลุ่มที่มีความเสี่ยงสูง ดังรูปที่ 4

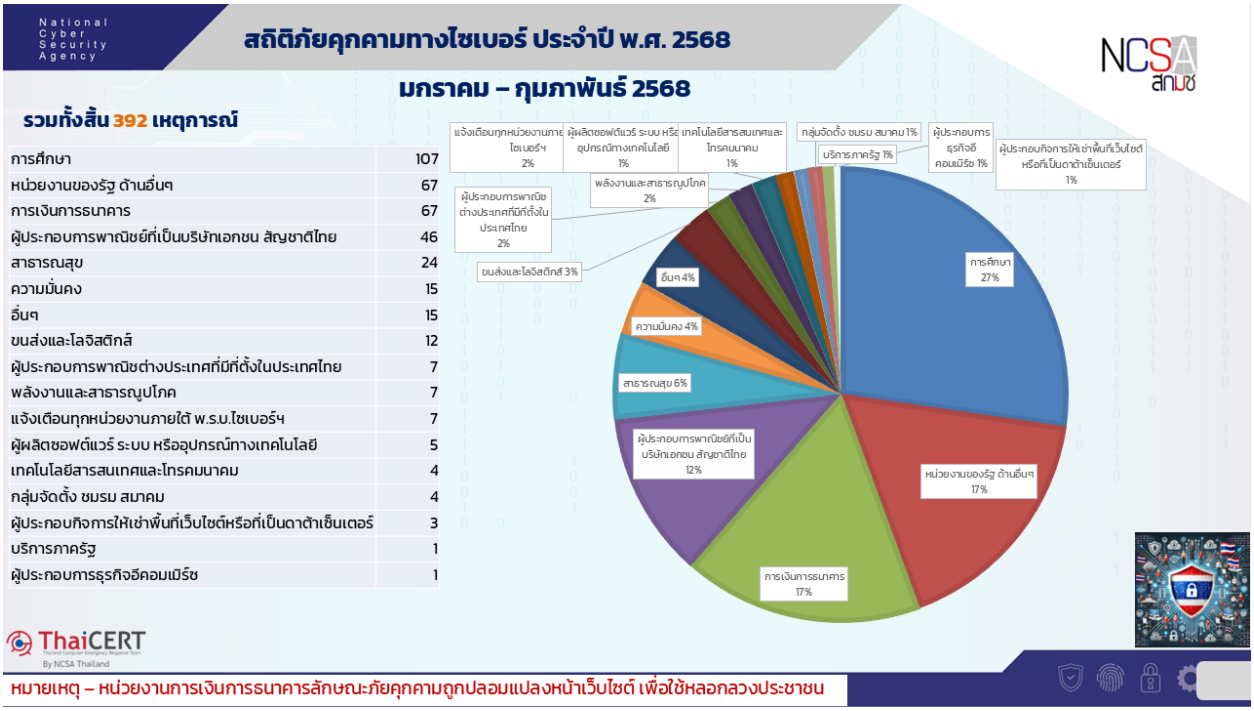


รูปที่ 3 การเพิ่มขึ้นของการโจมตีทางไซเบอร์ในปี 2024 เทียบกับปี 2023 แยกตามกลุ่มอุตสาหกรรม



รูปที่ 4 Heat map ความเสี่ยงด้านภัยคุกคามทางไซเบอร์ (สีเข้มหมายถึงเสี่ยงสูง)

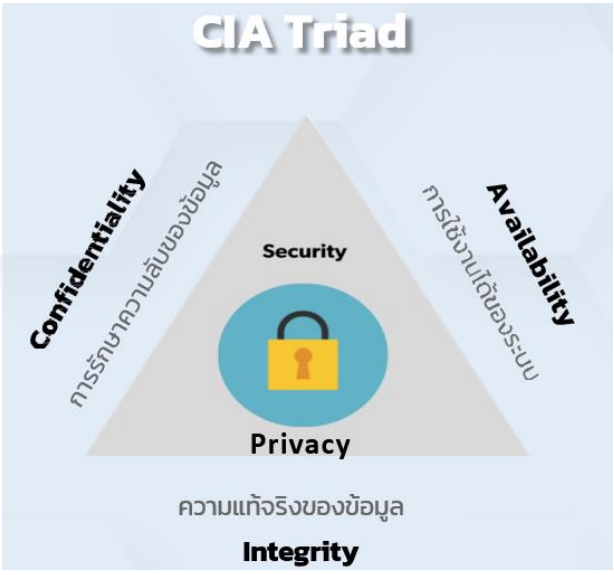
เมื่อพิจารณาเฉพาะประเทศไทย ตามข้อมูลของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) (https://ncsa.or.th/policy/threat-statistics) สถิติภัยคุกคามทางไซเบอร์ในเดือนมกราคม-กุมภาพันธ์ 2568 ดังรูปที่ 5 พบว่า องค์กรด้านการศึกษาเป็นเป้าหมายหลักของการโจมตีเช่นกัน โดยพบการโจมตี 107 เหตุการณ์ จากการโจมตีทั้งหมด 392 เหตุการณ์ คิดเป็น 27% ของเหตุการณ์ทั้งหมดที่เกิดขึ้น รองลงมาคือหน่วยงานอื่นของรัฐ และหน่วยงานการเงินการธนาคาร



รูปที่ 5 สถิติภัยคุกคามทางไซเบอร์ เดือนมกราคม-กุมภาพันธ์ 2568

ภัยคุกคามทางไซเบอร์ไม่ได้มีเพียงการโจมตีระบบสารสนเทศหรือระบบอินเทอร์เน็ตเท่านั้น แต่นับรวมถึงการหลอกลวงต่างๆ ที่เกิดขึ้นในโลกออนไลน์ด้วย ซึ่งปัจจุบันเป็นเหตุการณ์ที่เกิดขึ้นได้ง่ายและพบเจอได้ในชีวิตประจำวัน สถิติคดีออนไลน์ในช่วงปี 2565-2567 จากเว็บไซต์ Thai Police Online โดยศูนย์แจ้งความออนไลน์ มีคดีออนไลน์กว่า 7.7 แสนเรื่อง ซึ่งมีคดีประมาณครึ่งหนึ่งของคดีทั้งหมดเป็นการหลอกลวงซื้อขายสินค้าหรือบริการ รายละเอียดดังรูปที่ 6 โดยเก็บข้อมูลจากช่องทางการแจ้งความคดีออนไลน์ 3 ช่องทาง คือ ThaiPoliceOnline.go.th, Walk in แจ้งที่หน่วยงาน และสายด่วน 1441

รูปที่ 6 สถิติคดีออนไลน์สะสม 1 มีนาคม 2565 – 31 ธันวาคม 2567



รูปที่ 7 CIA Triad แนวคิดในการรักษาความมั่นคงปลอดภัยของข้อมูล

2. แนวคิดในการรักษาความมั่นคงปลอดภัยของข้อมูล

CIA Triad เป็นแนวคิดพื้นฐานของการรักษาความปลอดภัยของข้อมูล (ดังรูปที่ 7) เพื่อให้มั่นใจว่าข้อมูลมีการรักษาความลับ ถูกต้องสมบูรณ์ และสามารถใช้งานได้ตลอดเวลา โดยต้องใช้เทคนิคและมาตรการที่เหมาะสมในการป้องกันภัยคุกคามทางไซเบอร์ โดย CIA Triad มีองค์ประกอบสำคัญ 3 ประการ ได้แก่

1) Confidentiality (**การรักษาความลับของข้อมูล**)

การรักษาความลับของข้อมูล หมายถึง การควบคุมการเข้าถึงข้อมูลและอนุญาตให้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้นสามารถเข้าถึงข้อมูลได้ตามระดับความลับที่กำหนด ซึ่งสามารถบังคับใช้งานได้ผ่านการเข้ารหัส (Encryption) การควบคุมสิทธิ์การเข้าถึง (Access Control) และการพิสูจน์ตัวตน (Authentication)

ตัวอย่างของข้อมูลที่ต้องการความลับสูง

- ข้อมูลเงินเดือนของพนักงาน: ควรเข้าถึงได้เฉพาะฝ่ายทรัพยากรบุคคล (HR) และผู้บริหารที่เกี่ยวข้องเท่านั้น
- ข้อมูลทางการแพทย์ของผู้ป่วย: จำกัดการเข้าถึงเฉพาะแพทย์และเจ้าหน้าที่ทางการแพทย์ที่ได้รับอนุญาต
- เบอร์โทรศัพท์ของพนักงาน: อาจเป็นข้อมูลภายในที่พนักงานสามารถเข้าถึงได้แต่ไม่เผยแพร่ต่อบุคคลภายนอก

2) Integrity (**การรักษาความถูกต้องของข้อมูล**)

การรักษาความถูกต้องของข้อมูล หมายถึง การป้องกันการเปลี่ยนแปลง แก้ไข หรือลบข้อมูล โดยไม่ได้รับอนุญาต และต้องมั่นใจว่าข้อมูลยังคงมีความถูกต้องครบถ้วนในทุกช่วงเวลา

ตัวอย่างของข้อมูลที่ต้องมีความถูกต้องสูง

- ข้อมูลบัญชีธนาคาร: ต้องมั่นใจว่าข้อมูลยอดเงินคงเหลือของลูกค้าถูกเปลี่ยนแปลงตามธุรกรรมที่กระทำผ่านกระบวนการที่ถูกต้องและได้รับอนุญาต
- ข้อมูลทางการแพทย์: ต้องเป็นข้อมูลที่ถูกต้องและไม่มีการแก้ไขโดยไม่ได้รับอนุญาต เพราะอาจมีผลกระทบต่อการรักษาผู้ป่วย
- ข้อมูลในระบบฐานข้อมูลขององค์กร: ต้องป้องกันไม่ให้เกิดการแก้ไขที่ไม่ได้รับอนุญาตหรือจากบุคคลภายนอก

3) Availability (**ความพร้อมใช้งานของข้อมูล**)

ข้อมูลต้องสามารถเข้าถึงได้ทุกครั้งที่จำเป็นต้องใช้งาน และระบบต้องสามารถรองรับการให้บริการอย่างต่อเนื่องแม้จะเผชิญกับภัยคุกคามทางไซเบอร์

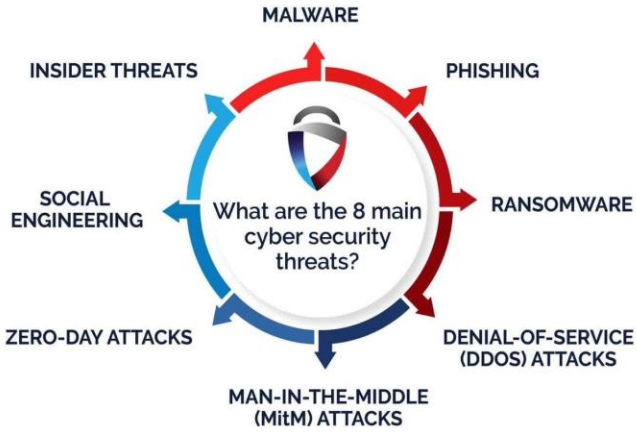
ตัวอย่างของข้อมูลที่ต้องมีความพร้อมใช้งานสูง

- ระบบธุรกรรมธนาคารออนไลน์: ต้องพร้อมให้บริการตลอด 24 ชั่วโมง
- เว็บไซต์ภาครัฐที่สำคัญ: เช่น เว็บไซต์ของหน่วยงานภาครัฐที่รายงานสถานการณ์โรคระบาดที่กำลังเผชิญอยู่
- ฐานข้อมูลทะเบียนนักศึกษา: ต้องมีระบบสำรองข้อมูลเพื่อให้สามารถกู้คืนข้อมูลได้ในกรณีเกิดเหตุไม่คาดคิด

การป้องกันตามหลัก CIA Triad ต้องคำนึงถึงความสมดุลในการใช้งานด้วย เนื่องจากการควบคุมที่มากเกินไปอาจทำให้ผู้ใช้รู้สึกไม่สะดวก แต่กลับกันหากควบคุมน้อยเกินไปอาจทำให้เกิดความเสียหายได้ง่าย เช่น การเข้าสู่ระบบด้วยรหัสผ่านและตามด้วยการยืนยันตัวตนด้วย ThaID อีกครั้ง ทำให้ผู้อื่นปลอมแปลงได้ยาก แต่ผู้ใช้งานอาจรู้สึกวุ่นวายในการตรวจสอบการเข้าสู่ระบบหลายขั้นตอน เป็นต้น

3. ประเภทของภัยคุกคามทางไซเบอร์

ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในปัจจุบันมีความหลากหลายและซับซ้อนมากขึ้น โดยภัยคุกคามอาจมาจากหลายแหล่งทั้งจากภายในและภายนอกองค์กร ส่งผลกระทบต่อความปลอดภัยของข้อมูลและระบบต่างๆ ภัยคุกคามทางไซเบอร์สามารถแบ่งออกเป็น 8 ประเภทหลัก ดังรูปที่ 8 ซึ่งแต่ละประเภทมีลักษณะและวิธีการโจมตีที่แตกต่างกัน ดังนี้



รูปที่ 8 ประเภทของภัยคุกคามทางไซเบอร์

1) Malware (มัลแวร์)

มัลแวร์ (Malicious Software) คือโปรแกรมที่ถูกออกแบบมาเพื่อก่อให้เกิดความเสียหายต่อข้อมูล ขโมยข้อมูล หรือทำให้ระบบคอมพิวเตอร์ทำงานผิดปกติ มัลแวร์มีหลายรูปแบบ ได้แก่

- ไวรัส (Virus): เป็นซอฟต์แวร์ที่สามารถแนบตัวเองเข้ากับไฟล์โปรแกรมหรือเอกสาร เมื่อไฟล์ดังกล่าวถูกเปิดใช้งาน ไวรัสจะทำงานและแพร่กระจายไปยังไฟล์หรือระบบอื่น ๆ โดยต้องอาศัยการกระทำของผู้ใช้ในการเปิดไฟล์ที่ติดไวรัส
- เวิร์ม (Worm): คล้ายกับไวรัสแต่แตกต่างตรงที่สามารถแพร่กระจายผ่านเครือข่ายคอมพิวเตอร์ได้โดยอัตโนมัติ โดยไม่ต้องอาศัยการกระทำของผู้ใช้หรือแนบตัวเองกับไฟล์ใด ๆ
- โทรจัน (Trojan Horse): เป็นโปรแกรมที่ถูกออกแบบให้ดูเหมือนไม่เป็นอันตราย แต่แฝงฟังก์ชันที่เป็นอันตราย เช่น การเปิดช่องโหว่ให้แฮ็กเกอร์เข้าถึงระบบ การขโมยข้อมูล หรือการควบคุมอุปกรณ์ของเหยื่อจากระยะไกล

- สปายแวร์ (Spyware): เป็นซอฟต์แวร์ที่แอบดักจับข้อมูลของผู้ใช้โดยไม่ได้รับอนุญาต เช่น การบันทึกการกดแป้นพิมพ์ (Keylogging) เพื่อดักจับรหัสผ่านหรือข้อมูล การติดตามพฤติกรรมการท่องเว็บไซต์ หรือการขโมยข้อมูลส่วนบุคคล

มัลแวร์แต่ละประเภทมีวิธีการแพร่กระจายและเป้าหมายที่แตกต่างกัน ดังนั้น การติดตั้งโปรแกรม Anti Virus และการใช้งานอย่างระมัดระวังจึงเป็นสิ่งสำคัญ

2) Phishing (ฟิชชิง)

ฟิชชิง (Phishing) เป็นการหลอกลวงทางจิตวิทยา เพื่อหลอกลวงให้เหยื่อเปิดเผยข้อมูลสำคัญ เช่น รหัสผ่าน ข้อมูลบัตรเครดิต หรือข้อมูลส่วนบุคคลอื่น ๆ โดยมักใช้ช่องทางการสื่อสาร เช่น อีเมล เว็บไซต์ หรือข้อความ ที่ปลอมแปลงให้ดูเหมือนมาจากแหล่งที่เชื่อถือได้ เช่น ธนาคาร หน่วยงานภาครัฐ หรือองค์กรที่เหยื่อคุ้นเคย

- Spear Phishing: การโจมตีฟิชชิงที่มีเป้าหมายเฉพาะเจาะจง ผู้โจมตีจะใช้ข้อมูลของเหยื่อ เช่น ชื่อ ตำแหน่งงาน หรือความสัมพันธ์กับองค์กร ในการสร้างข้อความที่น่าเชื่อถือและทำให้เหยื่อตกเป็นเป้าหมายได้ง่าย
- Whaling: เป็น Spear Phishing ที่มุ่งเป้าไปที่ผู้บริหารระดับสูงขององค์กร โดยมักใช้ข้อความที่เกี่ยวข้องกับธุรกรรมทางการเงินหรือข้อมูลสำคัญขององค์กร

เพื่อป้องกันฟิชชิง ควรตรวจสอบที่มาของอีเมลหรือข้อความทุกครั้ง หลีกเลี่ยงการคลิกลิงก์หรือดาวน์โหลดไฟล์แนบจากแหล่งที่ไม่น่าเชื่อถือ และใช้ระบบยืนยันตัวตนหลายชั้น (Multi-Factor Authentication) เพื่อเพิ่มความปลอดภัย

3) Ransomware (แรนซัมแวร์)

แรนซัมแวร์ (Ransomware) เป็นมัลแวร์ที่เข้ารหัสไฟล์หรือจำกัดการเข้าถึงระบบของเหยื่อ และเรียกค่าไถ่เพื่อแลกกับการปลดล็อกไฟล์หรือคืนสิทธิ์การใช้งานระบบ โดยมักแพร่กระจายผ่านอีเมลฟิชชิง ลิงก์ที่เป็นอันตราย หรือไฟล์ที่ดาวน์โหลดจากแหล่งที่ไม่น่าเชื่อถือ

- Crypto Ransomware (เช่น Cryptolocker): เป็นแรนซัมแวร์ที่เข้ารหัสไฟล์ทั้งหมดในเครื่องของเหยื่อ ทำให้ไม่สามารถเปิดใช้งานไฟล์ได้ เว้นแต่จะจ่ายค่าไถ่เพื่อรับกุญแจถอดรหัส
- Locker Ransomware: แทนที่จะเข้ารหัสไฟล์ แรนซัมแวร์ประเภทนี้จะล็อกหน้าจอหรือระบบของเหยื่อ ทำให้ไม่สามารถเข้าถึงอุปกรณ์ได้จนกว่าจะจ่ายค่าไถ่

เนื่องจากการจ่ายค่าไถ่ไม่ได้รับประกันว่าเหยื่อจะได้ไฟล์คืน จึงควรมีมาตรการป้องกันที่รัดกุมและเตรียมพร้อมรับมือกับการโจมตีจากแรนซัมแวร์อยู่เสมอ

4) Denial of Service (DoS) หรือ Distributed Denial of Service (DDoS) Attacks

การโจมตี DoS และ DDoS เป็นการโจมตีที่มุ่งทำให้ระบบหรือบริการออนไลน์ไม่สามารถให้บริการได้ตามปกติ โดยการส่งปริมาณคำขอจำนวนมากไปยังเซิร์ฟเวอร์หรือระบบเป้าหมายจนทรัพยากรของระบบถูกใช้งานจนหมด ส่งผลให้บริการช้าลงหรือหยุดทำงาน

- DoS (Denial of Service): การโจมตีที่มาจากแหล่งเดียว เช่น อุปกรณ์หรือเซิร์ฟเวอร์เครื่องเดียวที่ส่งคำขอจำนวนมากไปยังเป้าหมายเพื่อทำให้ระบบล่ม
- DDoS (Distributed Denial of Service): เป็นรูปแบบที่ซับซ้อนกว่าการโจมตี DoS โดยใช้เครือข่ายของอุปกรณ์หลายเครื่อง (เช่น Botnet) ซึ่งถูกควบคุมโดยแฮ็กเกอร์ เพื่อสร้างปริมาณคำขอจำนวนมากส่งไปยังเป้าหมายเพื่อทำให้ระบบล่ม ทำให้ยากต่อการป้องกันและระบุแหล่งที่มาของการโจมตี

การป้องกัน DoS และ DDoS มีความสำคัญอย่างมาก โดยเฉพาะกับธุรกิจออนไลน์ที่ต้องให้บริการตลอดเวลา การเตรียมความพร้อมและใช้มาตรการป้องกันล่วงหน้าจะช่วยลดความเสียหายที่อาจเกิดขึ้นจากการโจมตีเหล่านี้ได้

5) **Man-in-the-Middle (MitM) Attacks (การโจมตีแบบคนกลาง)**

การโจมตีแบบ MitM (Man-in-the-Middle) เกิดขึ้นเมื่อผู้โจมตีแอบแทรกตัวเข้าระหว่างการสื่อสารระหว่างสองฝ่าย เพื่อดักฟัง แก้ไข หรือปลอมแปลงข้อมูลที่ถูกส่งผ่าน โดยที่ทั้งผู้ส่งและผู้รับไม่รู้ตัว การโจมตีประเภทนี้สามารถเกิดขึ้นได้ในเครือข่าย Wi-Fi สาธารณะ หรือผ่านช่องโหว่ของโปรโตคอลการเข้ารหัสที่ไม่ปลอดภัย

- Session Hijacking: การโจมตีที่ผู้ไม่หวังดีขโมย Session ID ของผู้ใช้ที่ล็อกอินอยู่แล้ว เพื่อนำไปใช้เข้าถึงบัญชีหรือข้อมูลสำคัญโดยไม่ต้องใช้รหัสผ่าน
- SSL Stripping: การโจมตีที่บังคับลดระดับความปลอดภัยของการเชื่อมต่ออินเทอร์เน็ตจาก HTTPS (ที่มีการเข้ารหัส) เป็น HTTP (ที่ไม่มีการเข้ารหัส) ทำให้ข้อมูลสำคัญ เช่น รหัสผ่าน หมายเลขบัตรเครดิต หรือข้อมูลส่วนตัว ถูกดักจับได้โดยง่าย

ควรหลีกเลี่ยงการใช้เครือข่าย Wi-Fi สาธารณะ โดยเลือกใช้ VPN (Virtual Private Network) แทน ซึ่งจะทำงานโดยปกปิด IP Address ของผู้ใช้และเข้ารหัสข้อมูล ส่งข้อมูลอย่างปลอดภัยและไม่เปิดเผยตัวตนผ่านเครือข่ายสาธารณะ นอกจากนี้ควรเปิดการตั้งค่าบังคับใช้ HTTPS บนเบราว์เซอร์

6) **Zero-Day Exploits (การโจมตีช่องโหว่ Zero-Day)**

Zero-Day Exploits คือช่องโหว่ที่ผู้โจมตีใช้ประโยชน์จากข้อบกพร่องในซอฟต์แวร์หรือระบบที่ยังไม่ถูกค้นพบหรือยังไม่มีการแก้ไข ช่องโหว่เหล่านี้สามารถใช้โจมตีระบบต่าง ๆ โดยที่ผู้ใช้หรือผู้พัฒนาโปรแกรมไม่รู้ตัว

- Zero-Day Vulnerabilities: ช่องโหว่ที่ผู้พัฒนาซอฟต์แวร์ยังไม่ค้นพบหรือค้นพบแล้วแต่ยังไม่มีมาตรการแก้ไข
- Zero-Day Attack: การโจมตีที่ใช้ช่องโหว่ Zero-Day เพื่อเจาะระบบ ขโมยข้อมูล หรือดำเนินการที่เป็นอันตรายก่อนที่ผู้พัฒนาซอฟต์แวร์จะสามารถพัฒนาแพตช์ (Patch) ป้องกันได้ ทำให้ลูกค้าที่ซื้อซอฟต์แวร์นั้นมาใช้งานสามารถถูกโจมตีได้โดยที่ไม่ทราบถึงปัญหา

เนื่องจาก Zero-Day Exploits เป็นการโจมตีที่ไม่สามารถคาดการณ์ล่วงหน้าได้ จึงควรอัพเดทซอฟต์แวร์และระบบปฏิบัติการอย่างสม่ำเสมอ และใช้มาตรการป้องกันเชิงรุกจะช่วยลดความเสี่ยงจากภัยคุกคามประเภทนี้

7) Social Engineering (**วิศวกรรมสังคม**)

Social Engineering (วิศวกรรมสังคม) คือเทคนิคการหลอกลวงทางจิตวิทยาที่ผู้โจมตีใช้เพื่อชักจูงให้เหยื่อเปิดเผยข้อมูลสำคัญ ดำเนินการบางอย่าง หรือให้สิทธิ์เข้าถึงระบบโดยไม่รู้ตัว การโจมตีประเภทนี้มักอาศัยความเชื่อใจ ความเร่งด่วน หรือการปลอมแปลงตัวตนเพื่อให้เหยื่อตอบสนองโดยไม่ทันคิด

- Pretexting: ผู้โจมตีสร้างสถานการณ์หรือเรื่องราวเท็จเพื่อหลอกให้เหยื่อเปิดเผยข้อมูล เช่น แอบอ้างเป็นเจ้าหน้าที่ธนาคารหรือฝ่ายไอทีเพื่อขอข้อมูลบัญชีหรือรหัสผ่าน
- Baiting: การใช้สิ่งล่อลวงให้เหยื่อดำเนินการบางอย่าง เช่น คลิกลิงก์เพื่อดาวน์โหลดไฟล์ที่แฝงมัลแวร์ หรือเสียบแฟลชไดรฟ์(ที่แจกฟรีหรือแกล้งวางลืมไว้)ที่ติดมัลแวร์ โดยคิดว่าเป็นของที่มีประโยชน์

Social Engineering ใช้ความอยากรู้หรือความโลภของเหยื่อเป็นเครื่องมือ ดังนั้นการ “คิดก่อนคลิก” และใช้แหล่งข้อมูลที่เชื่อถือได้ คือวิธีป้องกันที่ดีที่สุด

8) Insider Threats (**ภัยคุกคามจากภายในองค์กร**)

ภัยคุกคามจากภายในองค์กร เป็นความเสี่ยงที่เกิดจากพนักงานหรือบุคคลที่มีสิทธิ์เข้าถึงข้อมูลและระบบขององค์กร ใช้สิทธิ์นั้นในการขโมยข้อมูล ทำลายระบบ หรือเปิดเผยข้อมูลลับ ซึ่งอาจเกิดจากความตั้งใจหรือความประมาท

- Malicious Insider: บุคคลที่มีเจตนาไม่ดี ทำการขโมยข้อมูล ทำลายระบบ หรือขายข้อมูลให้กับคู่แข่ง สร้างความเสียหายให้กับองค์กร
- Negligent Insider: บุคคลที่ประมาทหรือขาดความรู้ด้านความปลอดภัย เช่น การใช้รหัสผ่านที่อ่อนแอ การแชร์ข้อมูลสำคัญโดยไม่ตั้งใจ หรือตกเป็นเหยื่อของวิศวกรรมสังคม

ภัยคุกคามจากภายในเป็นหนึ่งในความเสี่ยงที่องค์กรต้องให้ความสำคัญ เนื่องจากบุคคลภายในมีสิทธิ์เข้าถึงข้อมูลอยู่แล้ว การใช้มาตรการป้องกันที่เหมาะสมจะช่วยลดโอกาสเกิดความเสียหายจากภัยคุกคามประเภทนี้

4. ผลกระทบจากภัยคุกคามทางไซเบอร์ต่อมหาวิทยาลัย

ภัยคุกคามทางไซเบอร์สามารถสร้างความเสียหายต่อมหาวิทยาลัยในหลายด้าน ทั้งในด้านโครงสร้างพื้นฐาน ระบบงาน ข้อมูล ผู้ใช้บริการ และชื่อเสียงของมหาวิทยาลัย ซึ่งภัยคุกคามทางไซเบอร์ที่เกิดขึ้นอาจทำให้เกิดความเสียหายระดับร้ายแรงได้ ตารางที่ 1 แสดงผลกระทบระดับร้ายแรง เทียบเคียงกับประกาศจากหน่วยงานสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (สกมช.)

ตารางที่ 1 ผลกระทบจากภัยคุกคามทางไซเบอร์ต่อมหาวิทยาลัย (ระดับร้ายแรง)

ด้านของผลกระทบ	คำอธิบาย
ผลกระทบต่อโครงสร้างพื้นฐาน (อุปกรณ์หรือระบบงาน)	การประทุษร้ายต่อคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่ถูกใช้สำหรับให้บริการหลัก ดังนี้ (1)ระบบคอมพิวเตอร์ (2)โครงสร้างสำคัญทางสารสนเทศ แสดงให้เห็นได้ว่าผู้โจมตีมีความมุ่งหมายที่จะทำให้โครงสร้างพื้นฐานสำคัญของมหาวิทยาลัยเสียหายจนไม่สามารถทำงานหรือให้บริการได้
ผลกระทบต่อข้อมูล	มีเหตุอันควรเชื่อได้ว่าผู้โจมตีมีความมุ่งหมายให้เกิดการประทุษร้ายต่อข้อมูลที่ใช้สำหรับระบบคอมพิวเตอร์ หรือโครงสร้างสำคัญทางสารสนเทศ ซึ่งส่งผลให้บริการหลักไม่สามารถทำงานหรือให้บริการได้
แนวโน้มในการกู้คืนระบบ	ไม่สามารถกู้คืนระบบคอมพิวเตอร์ หรือโครงสร้างสำคัญทางสารสนเทศที่ใช้สำหรับให้บริการหลักได้ตามแผนการกู้คืน
ผลกระทบต่อผู้ใช้บริการ	อาจส่งผลกระทบต่อผู้ใช้บริการทั้งหมด
ผลกระทบต่อชื่อเสียง	ทำให้ชื่อเสียงของหน่วยงานหรือมหาวิทยาลัยเสียหายในระดับจังหวัด ประเทศ หรือนานาชาติ

จากที่กล่าวมาทั้งหมดข้างต้น แสดงให้เห็นว่าภัยคุกคามทางไซเบอร์สามารถส่งผลกระทบในหลายมิติ ตั้งแต่ระบบโครงสร้างพื้นฐาน ข้อมูลสำคัญ ผู้ใช้บริการ ตลอดจนชื่อเสียงของมหาวิทยาลัย การรับมือกับภัยเหล่านี้ไม่ได้เป็นหน้าที่ของหน่วยงานด้านเทคโนโลยีเพียงอย่างเดียว แต่ต้องอาศัยความร่วมมือจากทุกภาคส่วน ไม่ว่าจะเป็นผู้บริหาร คณาจารย์ บุคลากร นักศึกษา และพันธมิตรจากหน่วยงานภายนอกที่อาจเข้าถึงระบบงานในส่วนที่เกี่ยวข้อง (เช่น บริษัทผู้รับจ้างพัฒนาหรือติดตั้งซอฟต์แวร์)

แนวทางป้องกันที่มีประสิทธิภาพต้องประกอบด้วยการตระหนักรู้ถึงภัยคุกคาม การบังคับใช้นโยบายด้านความมั่นคงปลอดภัยทางไซเบอร์ และการเตรียมแผนกู้คืนระบบให้สามารถกลับมาดำเนินงานได้อย่างรวดเร็วเมื่อเกิดเหตุการณ์ไม่คาดคิด ทั้งนี้ การป้องกันเชิงรุกและการบริหารความเสี่ยงที่ดีจะช่วยลดผลกระทบให้น้อยที่สุด และช่วยให้มหาวิทยาลัยสามารถดำเนินงานได้อย่างมั่นคงและปลอดภัยในยุคดิจิทัล

5. กฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล

กฎหมายที่ใช้เป็นแนวทางสำคัญในการเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย ทั้งในระดับองค์กรและบุคคล เพื่อให้การใช้เทคโนโลยีสารสนเทศเป็นไปอย่างปลอดภัย หลักๆ มี 3 ฉบับ

1) **พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และ 2560**

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ มีวัตถุประสงค์เพื่อป้องกัน ปราบปราม และลงโทษการกระทำผิดที่เกี่ยวข้องกับระบบคอมพิวเตอร์และข้อมูลอิเล็กทรอนิกส์ เช่น การเข้าถึงระบบโดยไม่ได้รับอนุญาต การเผยแพร่ข้อมูลปลอม และการโจมตีทางไซเบอร์ นอกจากนี้ยังครอบคลุมถึงความผิดเกี่ยวกับเนื้อหาที่ไม่เหมาะสมหรือเป็นภัยต่อความมั่นคง การละเมิดกฎหมายนี้อาจมีโทษทั้งจำคุกและปรับ ขึ้นอยู่กับลักษณะและความรุนแรงของการกระทำผิด องค์กรและบุคคลทั่วไปควรตระหนักถึงข้อกฎหมายนี้เพื่อป้องกันการละเมิดโดยไม่ตั้งใจ คลิกที่นี่เพื่อไปยังแหล่งศึกษาข้อมูลเพิ่มเติม

2) **พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562**

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เป็นกฎหมายที่มีเป้าหมายในการเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ โดยกำหนดมาตรการป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคงของชาติและการให้บริการสาธารณะ กฎหมายฉบับนี้กำหนดให้หน่วยงานที่มีโครงสร้างพื้นฐานสารสนเทศที่สำคัญ (Critical Information Infrastructure - CII) เช่น การเงิน พลังงาน คมนาคม และสาธารณสุข ต้องดำเนินมาตรการด้านความปลอดภัยไซเบอร์ตามมาตรฐานที่กำหนด นอกจากนี้ยังให้อำนาจแก่หน่วยงานที่เกี่ยวข้องในการเฝ้าระวัง ตรวจสอบ และดำเนินมาตรการตอบโต้เมื่อเกิดเหตุการณ์ทางไซเบอร์ที่อาจเป็นภัยต่อความมั่นคงของประเทศ

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้สรุปเนื้อหา พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีรายละเอียดดังต่อไปนี้

- **ทำไมต้องมี พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562**

เพื่อปกป้องระบบคอมพิวเตอร์และโครงข่าย IT ของโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศหรือบริการที่สำคัญของประเทศมีความมั่นคงปลอดภัยสามารถให้บริการได้ตามปกติ และหน่วยงานสามารถรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที

- **สาระสำคัญ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562**

(1) กำหนดให้โครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานภาครัฐมีมาตรฐานและมีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์
(2) มีการเฝ้าระวังภัยคุกคามและมีแผนรับมือเพื่อกู้คืนระบบให้กลับมาทำงานได้ตามปกติ
(3) มีการร่วมมือและประสานงานกันกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เมื่อมีภัยร้ายแรงที่ทำให้การให้บริการที่สำคัญไม่สามารถทำงานได้จนทำให้ประชาชนเดือดร้อน

- **หน่วยงานหลักที่เกี่ยวข้องกับ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562**

(1) หน่วยงานควบคุมหรือกำกับดูแล ทำหน้าที่ดูแลการดำเนินการของหน่วยงานรัฐหรือโครงสร้างพื้นฐานสำคัญให้มีมาตรฐาน เช่น ธนาคารแห่งประเทศไทยกำกับดูแลสถาบันการเงิน กระทรวง อว. กำกับดูแลมหาวิทยาลัย

(2) สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ทำหน้าที่เป็นศูนย์กลางเฝ้าระวังความปลอดภัยไซเบอร์ของประเทศ และให้การช่วยเหลือในการป้องกันและรับมือเมื่อเกิดภัยคุกคามในระดับร้ายแรง

- **ประโยชน์ที่ประชาชนได้รับจาก พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562**

(1) ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญมีความปลอดภัยสามารถให้บริการได้ต่อเนื่อง
(2) มีแนวทางในการรับมือภัยคุกคามทางไซเบอร์ไม่ให้เกิดผลกระทบเป็นวงกว้างและกลับมาทำงานได้อย่างรวดเร็ว
(3) มีการจัดตั้งหน่วยงานขึ้นมาดูแลมาตรฐานด้านความปลอดภัยไซเบอร์และให้ความช่วยเหลือแก่หน่วยงานโครงสร้างพื้นฐานสำคัญ
(4) เมื่อเกิดภัยคุกคามร้ายแรง การเข้าไปแก้ไขปัญหาที่ต้องเข้าถึงทรัพย์สินจะต้องใช้คำสั่งศาลเพื่อคุ้มครองสิทธิ์

คลิกที่นี่เพื่อศึกษาสรุปกฎหมายรองที่สำคัญโดย สกมช.

3) **พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ.** 2562

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (The Personal Data Protection Act B.E. 2562 หรือเรียกย่อว่า PDPA) มีผลบังคับใช้ตั้งแต่วันที่ 1 มิถุนายน 2565 โดยหน่วยงานหลักที่ดำเนินการตาม พ.ร.บ. คือ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส. หรือ PDPC) มีวัตถุประสงค์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งส่งเสริมและสนับสนุนให้เกิดการพัฒนาด้านการคุ้มครองข้อมูลส่วนบุคคลของประเทศ

PDPA ถือเป็นกฎหมายที่ทุกคนควรทราบและตระหนักรู้ถึงสิทธิในข้อมูลส่วนบุคคลของตนเอง โดยเฉพาะอย่างยิ่งองค์กรธุรกิจต่างๆ ที่มีการเก็บข้อมูลส่วนบุคคลของ พนักงาน ลูกค้า ผู้ใช้งาน และผู้ใช้บริการขององค์กร

- **ข้อมูลส่วนบุคคลภายใต้การคุ้มครองของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ.** 2562 แบ่งออกเป็น 2 ประเภท

(1) ข้อมูลส่วนบุคคลทั่วไป (Personal Data) อาจมีการเรียกว่า ข้อมูลส่วนบุคคลปกติ หรือ ข้อมูลส่วนบุคคลพื้นฐาน ได้แก่
   a. ชื่อ-นามสกุล เบอร์โทรศัพท์ อีเมลส่วนตัว ที่อยู่ปัจจุบัน
   b. เลขบัตรประชาชน เลขหนังสือเดินทาง เลขใบอนุญาตขับขี่
   c. ข้อมูลทางการศึกษา ข้อมูลทางการเงิน ข้อมูลทางการแพทย์
   d. ทะเบียนรถยนต์ โฉนดที่ดิน ทะเบียนบ้าน
   e. วันเดือนปีเกิด สัญชาติ น้ำหนักส่วนสูง
   f. ข้อมูลอื่นๆ บนอินเทอร์เน็ตที่สามารถระบุตัวตนได้ เช่น Username/Password, Cookies IP address, GPS Location

(2) ข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data) อาจมีการเรียกว่า ข้อมูลส่วนบุคคลที่ละเอียดอ่อน เป็นข้อมูลที่ต้องระวังการใช้ข้อมูลมากเป็นพิเศษ ได้แก่

a. เชื้อชาติ เผ่าพันธุ์
b. ความคิดเห็นทางการเมือง
c. ความเชื่อในลัทธิ ศาสนา หรือปรัชญา
d. พฤติกรรมทางเพศ
e. ประวัติอาชญากรรม
f. ข้อมูลสหภาพแรงงาน
g. ข้อมูลด้านสุขภาพ ความพิการ เช่น โรคประจำตัว การฉีดวัคซีน ใบรับรองแพทย์
h. ข้อมูลพันธุกรรม
i. ข้อมูลชีวภาพ เช่น ลายนิ้วมือ แบบจำลองใบหน้า ข้อมูลม่านตา

- **บุคคลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562**

(1) เจ้าของข้อมูลส่วนบุคคล (Data Subject) คือ บุคคลที่ข้อมูลนั้นระบุไปถึง โดยข้อมูลอาจเป็นข้อมูลที่อยู่ในตัวหรือเกี่ยวข้องเชื่อมโยงไปถึงบุคคลที่เป็นเจ้าของข้อมูลนั้น

(2) ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) คือบุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เช่น หน่วยงานของรัฐหรือเอกชนที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของประชาชนหรือลูกค้าที่มาใช้บริการ

(3) ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) คือ บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล เช่น ผู้ให้บริการ Cloud service เป็นต้น

(4) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) คือ ผู้ที่ได้รับมอบหมายเพื่อทำหน้าที่ให้คำแนะนำ หรือตรวจสอบ การคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานหรือองค์กรให้เป็นไปตามกฎหมาย

- **บทลงโทษตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562**

(1) โทษทางอาญา: จำคุกสูงสุดไม่เกิน 6 เดือนถึง 1 ปี หรือปรับสูงสุดไม่เกิน 500,000 ถึง 1 ล้านบาท หรือทั้งจำทั้งปรับ

(2) โทษทางแพ่ง: ค่าสินไหมทดแทน + ค่าสินไหมเพื่อการลงโทษอีกไม่เกิน 2 เท่า

(3) โทษทางปกครอง: ปรับไม่เกิน 1 หรือ 3 หรือ 5 ล้านบาท

ภายหลังคำสั่งคณะกรรมการผู้เชี่ยวชาญ (กชช.) ได้ออกประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์การพิจารณาออกคำสั่งลงโทษปรับทางปกครองของคณะกรรมการผู้เชี่ยวชาญ (ฉบับที่ 2) พ.ศ. 2567 ร่วมกับ พ.ร.บ. คุ้มครอง

ข้อมูลส่วนบุคคล และกฎหมายรองที่เกี่ยวข้อง ส่งผลให้ค่าปรับกรณีโทษทางปกครองสามารถปรับผู้กระทำผิดได้ รวม 7 ล้านบาท มีผลนับตั้งแต่วันที่ 9 พฤษภาคม 2567 โดยค่าปรับแบ่งเป็น 3 ส่วนคือ

(1) กรณีไม่แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) ค่าปรับ 1 ล้านบาท (มาตรา 85) โดยมีจุดพิจารณาที่สำคัญคือ

- เข้าข่ายเป็นกิจการขนาดใหญ่ที่มีการประมวลผลข้อมูลส่วนบุคคลเป็นกิจกรรมหลัก
- มีการจัดจำหน่ายสินค้าแก่ผู้บริโภคทั่วประเทศและมีข้อมูลจำนวนมาก (100,000 รายขึ้นไป)
- จากกิจกรรมดังกล่าวทำให้เข้าข่ายต้องแต่งตั้ง DPO ตามมาตรา 41(2) แต่ไม่ได้มีการแต่งตั้งในช่วงที่เกิดเหตุ

(2) กรณีไม่มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม ค่าปรับ 3 ล้านบาท (มาตรา 83) โดยมีจุดพิจารณาที่สำคัญคือ

- มาตรการควบคุมการเข้าถึงข้อมูลส่วนบุคคล (Access Control)
- การกำหนดสิทธิในการเข้าถึงหรือใช้งาน (Authorization)

(3) กรณีไม่แจ้งเหตุละเมิดข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด ค่าปรับ 3 ล้านบาท (มาตรา 83) โดยมีจุดพิจารณาที่สำคัญคือ

- หลังจากเกิดเหตุละเมิด ไม่มีการแจ้งเหตุภายใน 72 ชั่วโมงตามที่กฎหมายกำหนด โดยองค์กรอาจชี้แจงเหตุผลความจำเป็นและรายละเอียดที่เกี่ยวข้องเพื่อแสดงให้เห็นว่ามีเหตุจำเป็นที่ไม่อาจหลีกเลี่ยงได้ที่ทำให้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้า โดยจะต้องแจ้งแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) โดยเร็ว ทั้งนี้ ต้องไม่เกิน 15 วันนับแต่ทราบเหตุ

- **10 เรื่องที่ประชาชนต้องรู้เกี่ยวกับ** PDPA

(1) ข้อมูลส่วนบุคคล คือ ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม (มาตรา 6)

(2) ผู้ควบคุมข้อมูลส่วนบุคคล ต้องเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งไว้ก่อนหรือแจ้งในขณะเก็บรวบรวม (มาตรา 21)

(3) ผู้ควบคุมข้อมูลส่วนบุคคล ต้องเก็บรวบรวมข้อมูลส่วนบุคคลเท่าที่จำเป็น ภายใต้วัตถุประสงค์อันชอบด้วยกฎหมาย (มาตรา 22)

(4) ความยินยอม เป็นเพียงฐานหนึ่งของการประมวลผลข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่กำหนดฐานทางกฎหมายที่ใช้ในการประมวลผลข้อมูล (มาตรา 26)

(5) ในการขอความยินยอม ผู้ควบคุมข้อมูลส่วนบุคคลต้องคำนึงถึงความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลเป็นสำคัญ (มาตรา 19 วรรคสี่)

(6) เจ้าของข้อมูลส่วนบุคคล มีสิทธิ ดังนี้

a. สิทธิในการถอนความยินยอม ในกรณีที่เคยให้ความยินยอมไว้ (มาตรา 19 วรรคห้า)

b. สิทธิได้รับการแจ้งให้ทราบรายละเอียด (Privacy Notice) (มาตรา 23)

c. สิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล (มาตรา 30)

d. สิทธิขอให้โอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่น (มาตรา 31)

e. สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (มาตรา 32)

f. สิทธิขอให้ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ (มาตรา 33)

g. สิทธิขอให้ระงับการใช้ข้อมูลส่วนบุคคล (มาตรา 34) ในกรณีที่เกิดเหตุการละเมิด

h. สิทธิขอให้แก้ไขข้อมูลส่วนบุคคล (มาตรา 35)

i. สิทธิที่จะได้รับแจ้งเหตุละเมิดเมื่อข้อมูลรั่วไหล (มาตรา 37)

(7) PDPA ใช้กับการประมวลผลข้อมูลส่วนบุคคลของบุคคลที่อยู่ในประเทศไทย ไม่ว่าจะมีสัญชาติใดก็ตาม (มาตรา 5)

(8) ในกรณีที่เหตุการละเมิดข้อมูลส่วนบุคคล มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบ พร้อมกับแนวทางการเยียวยาโดยไม่ชักช้า (มาตรา 37(4))

(9) ผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่จัดทำบันทึกรายการกิจกรรมเพื่อให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) สามารถตรวจสอบได้ โดยสามารถบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้

(10) เจ้าของข้อมูลส่วนบุคคล มีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญ (กชช.) ในกรณีที่มีการฝ่าฝืนหรือไม่ปฏิบัติตาม PDPA (มาตรา 73)

- **พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ระบุให้องค์กรทำอะไรบ้าง**

(1) องค์กรจะต้องมีความรู้ด้านกฎหมาย และต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลในการเก็บข้อมูล

(2) มีมาตรการรักษาความปลอดภัยและการรักษาความลับของข้อมูลที่รัดกุมตามมาตรฐานสากล เพื่อไม่ให้มีการรั่วไหล

(3) ธุรกิจจะต้องโปร่งใส ต้องมีการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนที่จะทำการเก็บข้อมูล

(4) จะต้องมีการแจ้งจุดประสงค์ และระยะเวลาในการเก็บข้อมูล หรืออาจมีนโยบายการจัดเก็บข้อมูลว่าองค์กรจะจัดเก็บข้อมูลเพื่อนำไปใช้ทำอะไรและเก็บนานเท่าใด

(5) การเก็บข้อมูลจะต้องเป็นไปตามมาตรฐานและต้องเก็บเท่าที่จำเป็น เพื่อแสดงว่ามีการปฏิบัติตามข้อบังคับ PDPA อย่างถูกต้อง

- **การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล**

การหลุดรั่วของข้อมูลส่วนบุคคล เมื่อมีการรายงานเหตุละเมิดข้อมูล ให้รายงานต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) สามารถแจ้งได้ที่อีเมล saraban@pdpa.or.th ระบุชื่อเรื่อง “[แจ้งเหตุละเมิด]” โดยพิจารณาเหตุการละเมิดข้อมูลดังนี้

(1) มีความเสี่ยงต่อสิทธิของเจ้าของข้อมูล ให้บันทึกเหตุไว้เป็นข้อมูลอ้างอิง

(2) มีความเสี่ยงต่อสิทธิของเจ้าของข้อมูล ให้รายงาน สคส. ภายใน 72 ชั่วโมง นับแต่ทราบเหตุเท่าที่สามารถทำได้

(3) มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลให้รายงาน สคส. ภายใน 72 ชั่วโมง นับแต่ทราบเหตุเท่าที่สามารถทำได้ และแจ้งเหตุให้เจ้าของข้อมูลทราบพร้อมแนวทางการเยียวยาโดยไม่ชักช้า

การแจ้งเหตุต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) มีรายละเอียดดังนี้

(1) ลักษณะการละเมิดข้อมูลส่วนบุคคล โดยระบุจำนวนเจ้าของข้อมูล จำนวนรายการของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด

(2) ช่องทางติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) หรือบุคคลที่ได้รับมอบหมายให้ประสานงาน

(3) ข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้นจากการละเมิด

(4) ข้อมูลเกี่ยวกับมาตรการป้องกัน ระงับเหตุละเมิด หรือเยียวยาความเสียหาย

แหล่งข้อมูลศึกษาเพิ่มเติม คลิกที่นี่เพื่ออ่านกฎหมายคุ้มครองข้อมูลส่วนบุคคล กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

มหาวิทยาลัยวลัยลักษณ์ได้มีการประกาศนโยบายการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2565 คลิกที่นี่เพื่ออ่านรายละเอียด

6. กรณีศึกษาการหลอกลวงทางออนไลน์

การหลอกลวงทางออนไลน์มีหลากหลายรูปแบบ โดยรูปแบบที่นิยมและเป็นคดีออนไลน์จำนวนมาก ได้แก่

6.1 **หลอกลวงซื้อขายสินค้าหรือบริการ (แบบไม่เป็นขบวนการ)** คดีออนไลน์ที่มากที่สุดอยู่ในกลุ่มนี้

ลักษณะกลโกง

- หลอกโอนเงิน ไม่มีสินค้าส่งจริง หรือสินค้าไม่ตรงปก หรือได้รับของชำรุด-เสียหาย
- ซื้อสินค้าแบรนด์เนมแท้ แต่ได้ของปลอม
- นักรับหิ้วของเชิดเงิน

วิธีการป้องกัน

- เช็กร้าน ควรเช็กประวัติร้านค้าและประวัติการขายให้รอบด้าน ปัจจุบันมีธุรกิจรับจ้างเพิ่มยอดผู้ติดตามเพื่อความน่าเชื่อถือ หากดูแต่ยอดผู้ติดตามอาจไม่เพียงพอ

- เช็กบัญชี ควรนำเลขบัญชีและชื่อเจ้าของบัญชีมาตรวจเพื่อดูว่าเจ้าของบัญชีเคยมีประวัติการโกงมาก่อนหรือไม่ สามารถตรวจสอบได้ที่ https://www.blacklistseller.com/ หรือ https://checkgon.go.th/
- เช็กรีวิว ดูรีวิวจากลูกค้าที่เคยสั่งของไปแล้วว่าสินค้ามีคุณภาพตรงกับที่เราต้องการหรือไม่ ทางร้านมีบริการอย่างไร แต่ควรระวังเรื่องการจ้างรีวิวเช่นกัน
- สังเกตเพจปลอม โดยดูจากยอดผู้ติดตาม และควรกดเข้าไปดูว่าผู้ติดตามมีแต่ต่างชาติหรือไม่

6.2. **หลอกให้โอนเงินเพื่อทำงาน** เป็นรูปแบบที่หลอกให้โอนเงินเพื่อจะได้งาน ได้อาชีพเสริม รวมไปถึงได้ค่าธรรมเนียมต่างๆ เช่น หลอกให้แพ็กสินค้า หลอกให้ดู YouTube

ลักษณะกลโกง

- มิจฉาชีพโทรชวนทำงานออนไลน์ หรือบอกว่าแค่กดใจในแอปพลิเคชันก็ได้เงิน
- ผู้เสียหายหลงเชื่อทำงานซึ่งอาจได้เงินปันผลตอบแทนจริงในระยะแรกเท่านั้น
- ผู้เสียหายถูกดึงเข้ากลุ่มแอปพลิเคชันไลน์ชวนทำภารกิจ
- ใช้ภารกิจยอดเงินสูงมาล่อ เช่น โอนเงินเป็นรอบเพื่อจองภารกิจ ถ้าทำภารกิจสำเร็จจะได้เงินสูงกว่ายอดที่โอนไป
- หลอกล่อให้โอนเงินก่อนเพื่อถอนเงินเครดิตของผู้เสียหาย

ข้อควรระวัง

- มีสติไม่หลงเชื่อ ถ้าทำงานต้องได้เงิน ไม่ใช่โอนเงินไปก่อนจึงจะได้เงิน
- โทรศัพท์ติดต่อเพื่อตรวจสอบข้อมูลกับทางบริษัทที่ถูกอ้าง
- สังเกตว่ามีเครื่องหมายบัญชีทางการหรือไม่
- ตรวจสอบชื่อบัญชีก่อนโอนเงินทุกครั้ง
- ตรวจสอบความน่าเชื่อถือผ่านเว็บไซต์ https://market.sec.or.th/LicenseCheck/Search

6.3 **หลอกให้กู้เงิน**

ลักษณะกลโกง

- หลอกให้กู้เงินผ่านแอปพลิเคชัน หรือโพสต์ตามแพลตฟอร์มโซเชียลมีเดียชื่อดัง โดยใช้โปรไฟล์รูปคนดังเพื่อหลอกให้จ่ายค่าธรรมเนียมก่อน
- หลอกให้ติดตั้งแอปพลิเคชันแล้วกู้เงินแต่ไม่ได้เงิน หรือติดตั้งแอปพลิเคชันแล้วทำให้ข้อมูลรั่วไหลจนกลายเป็นผู้ค้ำประกัน
- หลอกให้กู้เงินแล้วโดนหักดอกเบี้ยเลย เช่น กู้เงิน 5,000 บาท แต่ได้เงินแค่ 3,500 บาท ดอกเบี้ยสูงกว่ากฎหมายกำหนด

วิธีการป้องกัน

- สังเกตจากรีวิวของแอปพลิเคชันนั้นให้อ่านด้วยว่ามีผู้รีวิวว่าอย่างไร อย่าดูแค่จำนวนดาวของแอปพลิเคชัน
- เช็กแหล่งเงินกู้ให้มั่นใจว่ามีตัวตนอยู่จริง

- อ่านเงื่อนไขการกู้ให้ละเอียดก่อนตัดสินใจกู้
- อย่าหลงเชื่อคำโฆษณาง่ายๆ เพียงให้กู้เงินเยอะ วงเงินสูง
- อย่าให้ข้อมูลส่วนตัวเกินความจำเป็น เช่น รหัสหลังบัตรประชาชน
- ห้ามโอนเงินก่อนเด็ดขาด

6.4 **หลอกให้ลงทุนผ่านระบบคอมพิวเตอร์** การหลอกให้ลงทุนสร้างความเสียหายเป็นมูลค่ากว่าสองหมื่นสองพันล้านบาทในช่วงปี 2565-2567

ลักษณะกลโกง

- โฆษณาโดยใช้รูปคนดังและชวนเข้ากลุ่มเพื่อแนะนำการลงทุน ซึ่งในกลุ่มจะมีหน้าม้าที่คอยโพสต์รูปความสำเร็จ
- มักจะให้ผลตอบแทนที่สามารถถอนเงินได้ในครั้งแรก ๆ ที่ลงทุน เมื่อลงทุนมากขึ้น จะมีแค่ตัวเลขแต่ไม่สามารถถอนเงินได้ หากต้องการถอนเงิน ต้องโอนเงินเข้าไปเพิ่ม และจะติดปัญหาถอนเงินไม่ได้ ต้องเพิ่มเงินเรื่อย ๆ หากไม่เพิ่มจะโดนค่าปรับหรือทำให้ยอดเงินลดลง

วิธีการป้องกัน

- การลงทุนควรตรวจสอบแหล่งลงทุนว่ามีความน่าเชื่อถือหรือไม่
- หากให้ทำการติดตั้งแอปพลิเคชันให้ตรวจสอบข้อมูลรีวิวของแอปพลิเคชันก่อนเสมอ
- ควรเลือกลงทุนในกองทุนที่มีตัวตนอยู่จริงแทนการลงทุนผ่านกลุ่มในแอปพลิเคชันต่าง ๆ

6.5 **ข่มขู่ทางโทรศัพท์** (Call Center)

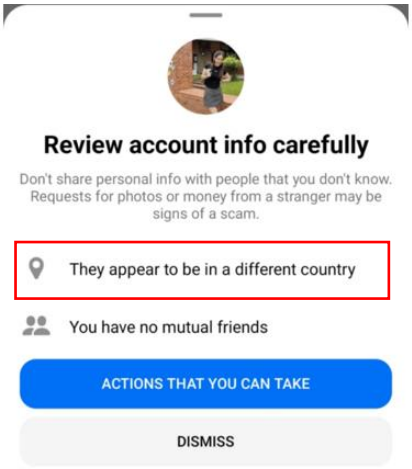
ลักษณะกลโกง

- อ้างเป็นเจ้าพนักงานของรัฐ เช่น มีพัสดุผิดกฎหมาย หรือเงินในบัญชีเป็นเงินที่ฉ้อโกงมา ทำให้เหยื่อตื่นกลัวและถูกหลอกได้ง่าย
- มักจะเน้นย้ำให้อยู่คนเดียว อย่าบอกคนอื่นในช่วงที่มีการข่มขู่

วิธีจัดการ Call center แอบอ้างเป็นเจ้าหน้าที่

- กรณีอ้างเป็นเจ้าหน้าที่ธนาคาร ให้ติดต่อสอบถาม Call center ของธนาคารโดยตรง
- กรณีอ้างเป็นหน่วยงานรัฐ ให้โทรสอบถามหน่วยงานนั้นโดยตรง
- กรณีอ้างว่ารับแจ้งความหรือสอบสวนทางโทรศัพท์ ให้นัดเจ้าหน้าที่ ณ สถานที่ราชการด้วยตนเอง
- หากขอให้สนทนาทาง Video Call ให้มีสติ สังเกต ภาพ เสียง ปาก และท่าทางว่ามีความผิดปกติหรือไม่
- อย่าเชื่อจากเครื่องแบบว่าเป็นเจ้าหน้าที่ เพราะมีการปลอมแปลงชุดเจ้าหน้าที่ได้เช่นกัน
- อย่าตื่นเต้นเมื่อมีการโทรเข้ามาและบอกข้อมูลส่วนตัวของเราได้อย่างถูกต้อง เช่น ชื่อ เลขบัตรประชาชน เนื่องจากมีข้อมูลรั่วไหลเยอะในปัจจุบัน
- หากเผลอคุยหรือรับสายไปแล้ว ควรสืบหาความจริง เช่น ลองโทรกลับไปเบอร์ที่โทรเข้ามา เพราะส่วนใหญ่ Call center จะใช้เครื่องที่โทรออกได้อย่างเดียว

- อย่าเพิ่มผู้ไม่รู้จักเป็นเพื่อนในแอปพลิเคชันไลน์โดยเด็ดขาดเพราะมีโอกาสโดนหลอกได้ง่าย
- หากเพิ่มเป็นเพื่อนทางแอปพลิเคชันไลน์ ให้สังเกตว่าโปรไฟล์ดังกล่าวมีการแจ้งเตือนว่ามีการใช้งานอยู่ในต่างประเทศหรือไม่ ตัวอย่างดังรูปที่ 9



รูปที่ 9 การแจ้งเตือนโดยแอปพลิเคชันไลน์เมื่อพบว่ามีการใช้งานจากต่างประเทศ

6.6 **การหลอกลวงในรูปแบบ** Romance Scam เป็นการหลอกให้รัก เป็นกลลวงที่สร้างความเสียหายให้กับเหยื่อจำนวนมาก โดยมักเริ่มสร้างความสัมพันธ์ผ่านแอปพลิเคชัน หรือโซเชียลมีเดีย ใช้โปรไฟล์หล่อ/สวย ทำให้เหยื่อหลงเชื่อและเกิดการโอนเงินไปให้

<u>ข้อสังเกต</u>

- การโอ้อวดฐานะหรือการเล่าถึงปัญหาทางการเงิน
- การแสดงความรักหรือความสนใจอย่างรวดเร็ว
- เริ่มคุยได้ไม่นานแต่ต้องการติดต่อโดยตรงผ่านช่องทางอื่น หรือเปลี่ยนช่องทางการติดต่อใหม่
- การหลีกเลี่ยงพบเจอตัวจริง (แต่มีหลายกรณีที่ยอมให้เจอตัวจริง)
- การพยายามขอข้อมูลส่วนตัวหรือขอสนทนาทาง Video Call เพื่อเก็บภาพหรือวิดีโอไว้แบล็กเมลในภายหลัง หรือเพื่อนำไปสอน AI ให้ปลอมแปลงเป็นเราแล้วนำไปหลอกคนอื่นต่อ
- ขอให้ช่วยโอนเงินจ่ายค่าดำเนินการต่างๆ โดยอาจหลอกว่าจะแบ่งเงินให้ในภายหลัง เช่น มรดก หรือเงินรางวัล

<u>วิธีการป้องกัน/รับมือ</u>

- ตรวจสอบตัวตนของคู่สนทนา เช่น ค้นหาชื่อโปรไฟล์ เลขบัญชี เบอร์โทรศัพท์
- อย่าแชร์ข้อมูลส่วนตัวมากเกินไป และหากมีการขอความช่วยเหลือทางการเงิน ให้สงสัยไว้ก่อนว่าอาจเป็นการหลอกลวง
- ทำตามแนวทางของศูนย์ต่อต้านข่าวปลอมประเทศไทย คือ ไม่รัก ไม่แคร์ ไม่เชื่อ ไม่รีบ ไม่โอน

ความผิดในการสวมรอยเป็นคนอื่นเพื่อหลอกให้รัก

มีความผิดตามมาตรา 16 พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 ซึ่งระบุไว้ว่า ใครเอาภาพคนอื่นที่ตัดต่อหรือดัดแปลงแล้วไปลงโซเชียลให้คนทั่วไปเข้าถึงได้ เจตนาทำให้เสียชื่อเสียง หรือดูหมิ่น เกลียดชัง หรือเดือดร้อน ถือว่าเป็นการกระทำความผิด มีโทษจำคุกไม่เกิน 3 ปี ปรับไม่เกิน 60,000 บาท หรือทั้งจำทั้งปรับ

6.7 ข่าวปลอม

ข่าวปลอมเป็นอีกประเภทหนึ่งของการหลอกลวงที่ทำให้เกิดความเข้าใจคลาดเคลื่อนและสร้างความเสียหายได้ ดังนั้นไม่ควรแชร์ข่าวปลอมให้บุคคลอื่น สามารถตรวจสอบข้อมูลข่าวปลอมได้ที่เว็บไซต์ https://www.antifakenewscenter.com/

วิธีการสังเกต

- สังเกตพาดหัว เรียกร้องความสนใจ ทำให้ตื่นตระหนัก ไม่น่าเชื่อถือ
- สังเกต URL มีการเปลี่ยน URL เพียงเล็กน้อยจากหน่วยงานจริงเพื่อเลียนแบบ
- พบความไม่ปกติ เช่น มักสะกดผิด หรือวางเลย์เอาต์ไม่ปกติ
- พิจารณารูปภาพ ใช้รูปหรือคลิปที่ไม่เป็นความจริง หรือไม่เกี่ยวกับเนื้อหา
- ตรวจสอบวันที่ ลำดับเหตุการณ์ไม่สมเหตุผล หรือเปลี่ยนวันที่ของเหตุการณ์
- ตรวจสอบหลักฐาน ไม่พบการยืนยันความถูกต้อง หรือใช้ผู้ที่ไม่น่าเชื่อถือมายืนยัน
- ดูรายงานจากที่อื่น ถ้าไม่มีรายงานข่าวจากแหล่งที่น่าเชื่อเลย ให้สงสัยว่าเป็นข่าวปลอม
- เป็นเรื่องตลกหรือไม่ ดูที่มาว่าเขาถนัดทำเรื่องล้อเลียนไหม และน้ำเสียงเป็นเรื่องตลกหรือไม่

6.8 หลอกเก็บข้อมูลใบหน้าและเสียง

ปัจจุบันใบหน้ามีความสำคัญ เพราะสามารถนำไปใช้ยืนยันตัวตนได้ จึงอาจเกิดการหลอกให้สนทนาทาง Video call เพื่อเก็บข้อมูลใบหน้า

ตัวอย่างการหลอกเก็บข้อมูล

- มิจฉาชีพ Call center หลอกให้เปิดกล้องสนทนาผ่าน Video call
- ชวนให้เพิ่มเป็นเพื่อนทางแอปพลิเคชันไลน์ที่ปลอมตัวมาหลอกว่าจะโอนเงินคืนให้ โดยขอข้อมูลส่วนตัวเพื่อยืนยันตัวตนและเก็บภาพใบหน้า
- แอบอ้างเป็นตำรวจบังคับให้เปิดกล้องเพื่อขอบันทึกภาพ และการสนทนาโดยอ้างว่าบันทึกข้อมูลไว้เป็นหลักฐาน
- การโทรมาจีบ ชักชวนไปเป็นดารา หรือเสนอผลประโยชน์ที่เกินจริง หลอกให้เปิดกล้องเพื่อดูหน้าตาและสัดส่วน

สรุปวิธีป้องกันการหลอกลวงทางออนไลน์

- ตั้งข้อสงสัยกับข้อเสนอที่ดีเกินจริง
- ตรวจสอบข้อมูลบริษัทและบุคคลให้ละเอียด
- เรียนรู้จากข่าวสารกลโกงที่เป็นข่าวสารอยู่ในปัจจุบัน
- อย่าตัดสินใจด้วยอารมณ์ ปรึกษาผู้เชี่ยวชาญ
- ไม่รับโทรศัพท์หมายเลขที่ไม่รู้จัก หรือหากมีโทรศัพท์ติดต่อมาอ้างเป็นหน่วยงานราชการเพื่อสอบถามข้อมูลส่วนตัว ให้คิดว่าเป็นมิจฉาชีพไว้ก่อน
- ไม่คลิกลิงก์ใน SMS โดยตั้งสติทุกครั้งที่อ่าน SMS อย่ารีบกดรับลิงค์ที่แนบมาเป็นอันขาด และตรวจสอบข้อมูลกับธนาคารหรือหน่วยงานที่อ้างว่าเป็นเจ้าของ SMS นั้นโดยใช้ช่องทางปกติ เช่น เว็บไซต์ หรือโทรศัพท์ติดต่อโดยตรง
- ไม่รับเป็นเพื่อนกับบุคคลแปลกหน้าในช่องทางโซเชียลมีเดีย โดยให้สังเกตโปรไฟล์ปลอม ได้แก่ โปรไฟล์ที่เพิ่งสร้างได้ไม่นาน มีเพื่อนน้อย ไม่มีเพื่อนมากด Like หรือลองนำภาพโปรไฟล์ไปค้นหาใน Google เพื่อสังเกตว่าแอบอ้างเป็นบุคคลอื่นหรือไม่

7. Security Checklist

Security Checklist เป็นแนวทางสำคัญที่ช่วยให้สามารถป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้อย่างเป็นระบบ โดยประกอบด้วยรายการตรวจสอบด้านต่าง ๆ ดังนี้ การตั้งค่าความปลอดภัยของระบบ การบริหารจัดการสิทธิ์เข้าถึงข้อมูล การใช้ซอฟต์แวร์ป้องกันภัยคุกคาม การสำรองข้อมูล และการจัดการเหตุการณ์ด้านความปลอดภัย การปฏิบัติตามรายการตรวจสอบเหล่านี้ช่วยเสริมสร้างแนวทางป้องกันเชิงรุก ลดความเสี่ยงจากการถูกโจมตี และเพิ่มประสิทธิภาพในการตอบสนองต่อภัยคุกคาม

7.1 การใช้เครื่องคอมพิวเตอร์

- ✅ Log out ทุกครั้ง เมื่อไม่ได้ใช้งานหรือเมื่อลุกออกจากเครื่อง
- ✅ ตั้งค่าล็อกหน้าจออัตโนมัติ หากไม่ได้ใช้งานเครื่องเป็นระยะเวลาหนึ่ง
- ✅ อัปเดตระบบปฏิบัติการ (OS) และซอฟต์แวร์ เป็นประจำ หรือเปิดใช้งานการอัปเดตอัตโนมัติ
- ✅ ติดตั้งและอัปเดตโปรแกรมป้องกันไวรัส เพื่อให้ได้รับการป้องกันที่ทันสมัยที่สุด
- ✅ เปิด Windows Firewall หรือระบบ Firewall อื่นๆ ที่มาพร้อมกับซอฟต์แวร์ป้องกันไวรัส
- ✅ ไม่ดาวน์โหลดและติดตั้งโปรแกรมจากแหล่งที่ไม่น่าเชื่อถือ
- ✅ ลบโปรแกรมที่ไม่จำเป็นออกจากเครื่อง เพื่อลดความเสี่ยงจากมัลแวร์
- ✅ สำรองข้อมูลสำคัญลงใน External Drive หรือ Cloud Storage เป็นประจำ

✅ ไม่เสียบ USB Flash Drive หรืออุปกรณ์ภายนอกที่ไม่รู้แหล่งที่มา

✅ ระวังอีเมลฟิชชิง (Phishing Emails) อย่าคลิกลิงก์หรือดาวน์โหลดไฟล์แนบที่น่าสงสัย

✅ ใช้เครือข่าย WiFi ที่ปลอดภัย หลีกเลี่ยงการใช้ WiFi สาธารณะสำหรับธุรกรรมสำคัญ

✅ เปิดใช้งานฟีเจอร์การเข้ารหัสข้อมูล (Encryption) ถ้ามีข้อมูลสำคัญบนเครื่อง

✅ ใช้บัญชีผู้ใช้ที่ไม่ใช่สิทธิ์ Admin เป็นค่าเริ่มต้น เพื่อลดความเสี่ยงจากมัลแวร์

7.2 **การใช้โทรศัพท์มือถือและแท็บเล็ต**

✅ ตั้งรหัสล็อกหน้าจอ (Passcode, Face ID หรือ Fingerprint) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

✅ อัปเดตระบบปฏิบัติการ (OS) และแอปพลิเคชัน อย่างสม่ำเสมอ หรือตั้งค่าการอัปเดตอัตโนมัติ

✅ ติดตั้งแอปพลิเคชันเฉพาะจากแหล่งที่เชื่อถือได้ เช่น App Store หรือ Google Play Store

✅ ติดตั้งแอปพลิเคชันป้องกันไวรัสสำหรับมือถือ และตั้งค่าการอัปเดตอัตโนมัติ

✅ ตรวจสอบและกำหนดสิทธิ์การเข้าถึงแอปพลิเคชัน (App Permissions) ให้เหมาะสม

✅ ปิดการแจ้งเตือนข้อความที่มีข้อมูลสำคัญ เช่น ไม่แสดง OTP บนหน้าจอที่ล็อกอยู่

✅ หลีกเลี่ยงการบันทึกข้อมูลสำคัญลงในโทรศัพท์ เช่น รหัสผ่านหรือข้อมูลการเงิน

✅ สำรองข้อมูลสำคัญไว้ที่ Cloud หรืออุปกรณ์อื่นเป็นประจำ

✅ ใช้เครือข่าย WiFi ที่ปลอดภัย หลีกเลี่ยงการเชื่อมต่อ WiFi สาธารณะโดยไม่มี VPN (Virtual Private Network)

✅ ไม่เชื่อมต่ออุปกรณ์กับที่ชาร์จ USB สาธารณะ ป้องกันการถูกขโมยข้อมูล (Juice Jacking)

✅ เปิดใช้งานฟีเจอร์ Find My Device เพื่อช่วยติดตามและลบข้อมูลเมื่ออุปกรณ์สูญหาย

✅ ไม่ Root หรือ Jailbreak เครื่อง เพราะอาจทำให้ระบบปลอดภัยน้อยลง

7.3 **การใช้งาน** Wi-Fi

✅ เปลี่ยนรหัสผ่านของ Wi-Fi Router ไม่ใช้รหัสผ่านที่เป็นค่าเริ่มต้นจากโรงงาน

✅ เปลี่ยนชื่อ Wi-Fi (SSID) และตั้งรหัสผ่านที่คาดเดายาก หากเป็นไปได้ให้ซ่อน SSID

✅ ตั้งค่าความปลอดภัยของ Wi-Fi เป็น WPA3 หรือ WPA2 (Wi-Fi Protected Access) หลีกเลี่ยงการใช้ WEP (Wired Equivalent Privacy) ซึ่งไม่ปลอดภัย

✅ หลีกเลี่ยงการเชื่อมต่อ Public Wi-Fi หรือ Free Hotspot โดยเฉพาะที่ไม่มีรหัสผ่าน

✅ หากจำเป็นต้องใช้ Wi-Fi สาธารณะ ให้ใช้ VPN เพื่อเข้ารหัสข้อมูลขณะใช้งาน

✅ ปิด Wi-Fi เมื่อไม่ใช้งาน เพื่อป้องกันการเชื่อมต่ออัตโนมัติไปยังเครือข่ายไม่ปลอดภัย

✅ อัปเดตเฟิร์มแวร์ของ Wi-Fi Router เป็นประจำ เพื่อลดช่องโหว่ด้านความปลอดภัย

✅ ปิด WPS (Wi-Fi Protected Setup) เพราะอาจถูกเจาะระบบได้ง่าย

✅ ตรวจสอบอุปกรณ์ที่เชื่อมต่อ Wi-Fi Router เป็นระยะ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

✅ องค์กรอาจกำหนดให้อุปกรณ์เฉพาะที่ได้รับอนุญาตสามารถเชื่อมต่อกับเครือข่ายได้ เช่น ใช้ MAC Address Filtering

7.4 การใช้อินเทอร์เน็ตของมหาวิทยาลัย

- ✅ เชื่อมต่อเฉพาะ Wi-Fi หรือ LAN ที่ได้รับอนุญาตจากมหาวิทยาลัย และตรวจสอบ SSID หรือตรวจสอบ URL ของหน้า Login ว่าเป็นของจริงก่อนเชื่อมต่อ (https://authen.wu.ac.th)
- ✅ ไม่แชร์รหัสผ่าน Wi-Fi หรือบัญชีผู้ใช้กับผู้อื่น เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
- ✅ หลีกเลี่ยงการใช้ VPN หรือ Proxy ที่ไม่ได้รับอนุญาต ซึ่งอาจละเมิดนโยบายของมหาวิทยาลัยและก่อให้เกิดความเสี่ยงต่อความปลอดภัย
- ✅ ไม่ดาวน์โหลดไฟล์หรือซอฟต์แวร์ละเมิดลิขสิทธิ์ หรือไฟล์ที่น่าสงสัยที่อาจมีมัลแวร์แฝงมา
- ✅ ไม่เข้าเว็บไซต์ต้องห้ามหรือผิดกฎหมาย เช่น เว็บไซต์พนัน สื่อลามก หรือเว็บไซต์ที่มีความเสี่ยงต่อมัลแวร์
- ✅ หลีกเลี่ยงการส่งข้อมูลสำคัญผ่านเครือข่ายที่ไม่เข้ารหัส (HTTP) เช่น การส่งรหัสผ่านหรือข้อมูลส่วนตัว (ควรใช้ HTTPS)
- ✅ Log out ออกจากระบบทุกครั้งหลังใช้งานบนเครื่องสาธารณะ เช่น ห้องปฏิบัติการคอมพิวเตอร์หรืออุปกรณ์ในห้องเรียนของมหาวิทยาลัย
- ✅ หากพบพฤติกรรมที่น่าสงสัย เช่น ระบบเครือข่ายผิดปกติ หรือพบการโจมตีทางไซเบอร์ ให้แจ้งเจ้าหน้าที่ IT ทราบทันที

7.5 การเข้าถึงเว็บไซต์

- ✅ ใช้ Web Browser ที่ได้มาตรฐานและอัปเดตเวอร์ชันสม่ำเสมอ เช่น Chrome, Firefox, Edge
- ✅ ไม่บันทึกรหัสผ่านลงใน Web Browser เพื่อป้องกันการขโมยข้อมูล
- ✅ อย่าหลงเชื่อข้อเสนอที่ดูดีเกินจริง เช่น ของฟรี เงินรางวัล หรือข้อความเร่งด่วนที่กดดันให้รีบตัดสินใจกดรับ
- ✅ ไม่คลิกลิงก์จากแหล่งที่ไม่น่าเชื่อถือ โดยเฉพาะจากโซเชียลมีเดีย อีเมล หรือข้อความที่ไม่รู้จัก
- ✅ ตรวจสอบว่าเว็บไซต์ใช้ HTTPS เสมอ โดยเฉพาะเมื่อต้องกรอกข้อมูลสำคัญ เช่น การทำธุรกรรมออนไลน์
- ✅ ไม่ใช้บัญชีอีเมลของมหาวิทยาลัยสมัครบริการที่ไม่เกี่ยวข้องกับงาน และไม่ใช้รหัสผ่านเดียวกันกับอีเมลมหาวิทยาลัย
- ✅ อย่าให้ข้อมูลส่วนตัวบนเว็บไซต์ที่ไม่น่าเชื่อถือ เช่น เบอร์โทรศัพท์ เลขบัตรประชาชน หรือเลขบัญชี
- ✅ ปิดการใช้งาน Autofill บน Browser เพื่อลดความเสี่ยงจากมัลแวร์ที่อาจขโมยข้อมูล
- ✅ ใช้ตัวจัดการรหัสผ่าน (Password Manager) ที่น่าเชื่อถือ แทนการจดจำรหัสผ่านไว้ใน Browser

7.6 วิธีตรวจสอบเพจจริง-เพจปลอม

- ✅ ดูจาก Meta verified (เครื่องหมาย Check กาถูกสีฟ้า)
- ✅ คลิกดูที่ about, page transparency ว่าถูกเปลี่ยนชื่อหรือไม่
- ✅ ตรวจสอบว่า Admins ของเพจมาจากประเทศอะไร
- ✅ มี Reviews ต่อเนื่องหรือไม่
- ✅ ตรวจสอบใน Google map เพื่อยืนยันว่าเว็บไซต์และเบอร์ติดต่อตรงกัน
- ✅ ตรวจสอบบัญชีธนาคารต้องสงสัย เบอร์ต้องสงสัย เว็บ/ลิงก์ปลอม SMS หลอกลวง ก่อนโอนเงินที่เว็บไซต์ https://checkgon.go.th/

7.7 แอปพลิเคชันออนไลน์

- ✅ ดาวน์โหลดแอปพลิเคชันจากแหล่งที่เชื่อถือได้ เช่น App Store หรือ Google Play Store หลีกเลี่ยงการติดตั้งแอปพลิเคชันจากไฟล์ APK หรือแหล่งที่ไม่น่าเชื่อถือ
- ✅ ตรวจสอบสิทธิ์การเข้าถึงของแอปพลิเคชัน (App Permissions) ไม่ให้แอปพลิเคชันเข้าถึงข้อมูลที่ไม่จำเป็น เช่น รายชื่อผู้ติดต่อหรือตำแหน่งที่ตั้งโดยไม่จำเป็น
- ✅ ตั้งค่าการยืนยันตัวตนแบบสองชั้น (2FA) สำหรับบัญชีที่สำคัญ เช่น อีเมล แอปพลิเคชันของธนาคาร หรือแอปพลิเคชันที่เกี่ยวข้องกับงาน
- ✅ ไม่บันทึกรหัสผ่านไว้ในแอปพลิเคชันหรือ Browser อาจใช้แอปพลิเคชันจัดการรหัสผ่าน (Password Manager) ที่เชื่อถือได้แทน
- ✅ หมั่นอัปเดตแอปพลิเคชันให้เป็นเวอร์ชันล่าสุด เพื่อปิดช่องโหว่ด้านความปลอดภัย
- ✅ หลีกเลี่ยงการล็อกอินบัญชีสำคัญผ่านเครือข่ายสาธารณะหรืออุปกรณ์ของผู้อื่น
- ✅ ตรวจสอบข้อมูลรีวิวและข้อมูลผู้พัฒนาแอปพลิเคชันก่อนติดตั้ง เพื่อหลีกเลี่ยงแอปพลิเคชันที่อาจมีมัลแวร์แฝงอยู่
- ✅ ไม่ใช้แอปพลิเคชันที่ขอข้อมูลส่วนตัวโดยไม่จำเป็น เช่น หมายเลขบัตรประชาชน หรือข้อมูลธนาคาร โดยไม่ทราบวัตถุประสงค์ที่ชัดเจน
- ✅ Log out จากบัญชีเมื่อเลิกใช้งาน โดยเฉพาะแอปพลิเคชันที่เกี่ยวข้องกับการเงินหรือข้อมูลสำคัญ

7.8 การใช้คอมพิวเตอร์หรืออุปกรณ์พกพาสาธารณะ

🔷 ก่อนใช้งาน

- ✅ ตรวจสอบว่าอุปกรณ์ไม่มีฮาร์ดแวร์แปลกปลอม เช่น Keylogger หรือ Skimmer บริเวณคีย์บอร์ดและพอร์ต USB
- ✅ หลีกเลี่ยงการใช้อุปกรณ์ที่ไม่ได้รับการดูแลจากองค์กรที่น่าเชื่อถือ
- ✅ หลีกเลี่ยงการใช้ Wi-Fi สาธารณะที่ไม่มีการเข้ารหัส ให้เลือกใช้ VPN เพื่อป้องกันการดักจับข้อมูล
- ✅ ตรวจสอบว่าอุปกรณ์ไม่มีซอฟต์แวร์แปลกปลอม หรือโปรแกรมที่ดูน่าสงสัยเปิดทำงานอยู่
- ✅ ใช้คีย์บอร์ดบนหน้าจอ (On-Screen Keyboard) เมื่อต้องป้อนรหัสผ่านสำคัญ

🔷 ระหว่างการใช้งาน

- ✅ ใช้โหมด Incognito/Private Browsing เพื่อลดการเก็บข้อมูลส่วนตัว
- ✅ หลีกเลี่ยงการเข้าสู่ระบบบัญชีสำคัญ เช่น อีเมล ธนาคาร หรือแพลตฟอร์มที่เกี่ยวข้องกับข้อมูลความปลอดภัยสูง
- ✅ อย่ากดยอมรับการบันทึกรหัสผ่าน อย่าเปิดใช้งานฟีเจอร์ Auto-fill
- ✅ ปิดการซิงก์ข้อมูลบัญชี เช่น Google Sync หรือ iCloud Keychain
- ✅ หลีกเลี่ยงการเปิดเอกสารหรือดาวน์โหลดไฟล์ที่อาจมีข้อมูลสำคัญบนอุปกรณ์สาธารณะ
- ✅ หากต้องพิมพ์ข้อมูลสำคัญ เช่น เลขบัตรเครดิต ให้ใช้ Virtual Keyboard หรือ Copy & Paste แทนการพิมพ์โดยตรง

🔷 **หลังใช้งาน**

✅ Log out ออกจากระบบทุกบัญชีที่ใช้ โดยเฉพาะบัญชีที่มีข้อมูลสำคัญ

✅ ล้างประวัติการเข้าชม (Clear browsing history) รวมถึง Cookies และ Cache

✅ รีสตาร์ทอุปกรณ์ (หากทำได้) เพื่อรีเซ็ตเซสชันการใช้งาน

✅ ตรวจสอบอุปกรณ์อื่น ๆ (เช่น โทรศัพท์) ว่ามีการแจ้งเตือนการล็อกอินจากตำแหน่งที่ไม่รู้จักหรือไม่

✅ หากจำเป็นต้องใช้ Flash drive ให้ตรวจสอบไวรัสก่อนใช้งานเมื่อนำกลับมาใช้บนอุปกรณ์ส่วนตัว

✅ เปลี่ยนรหัสผ่านทันทีหากพบสิ่งผิดปกติหรือสงสัยว่าอาจถูกแฮ็ก

🔷 **ข้อควรจำ**:

หากหลีกเลี่ยงไม่ได้ จำเป็นต้องใช้เครื่องสาธารณะ ควรลดความเสี่ยงด้วยวิธีป้องกันเบื้องต้น เช่น ใช้ OTP Authentication หรือเปลี่ยนรหัสผ่านทันทีหลังใช้งาน

7.9 ข้อควรปฏิบัติเมื่อเจอ “อีเมลฟิชชิ่ง”

✅ ระวังอีเมลที่มีลิงก์ให้คลิก โดยเฉพาะหากมีเนื้อหาดังต่อไปนี้

- ขอให้ยืนยันตัวตนหรือรีเซ็ตรหัสผ่าน
- แจ้งให้ตรวจสอบหรืออัปเดตบัญชีของคุณ
- ขอข้อมูลบัตรเครดิต หมายเลขบัตรประชาชน หรือข้อมูลส่วนตัวอื่น ๆ
- ขอให้ดาวน์โหลดไฟล์หรือซอฟต์แวร์จากแหล่งที่ไม่น่าเชื่อถือ

✅ อย่าคลิกลิงก์หรือเปิดไฟล์แนบโดยไม่ตรวจสอบก่อน ควรเปิดโหมด Preview เอกสารแนบไว้ก่อน

- หากได้รับอีเมลขอให้ล็อกอินเข้าสู่ระบบหรือรีเซ็ตรหัสผ่านโดยที่คุณไม่ได้ร้องขอ ให้สงสัยไว้ก่อนว่าอาจเป็นฟิชชิ่ง
- ตรวจสอบ URL ของลิงก์โดยเลื่อนเมาส์ไปวางเหนือข้อความก่อนคลิก หากพบว่าลิงก์ไม่ตรงกับเว็บไซต์ทางการ ให้หลีกเลี่ยง
- อย่าให้ข้อมูลส่วนตัว เช่น รหัสผ่าน หรือเลขบัตรเครดิต ผ่านลิงก์ในอีเมลที่ไม่น่าเชื่อถือ

✅ โปรดจำไว้ว่าองค์กรที่น่าเชื่อถือมักไม่ขอข้อมูลส่วนตัวผ่านช่องทางอีเมล

- บริษัทที่เชื่อถือได้มักไม่ส่งอีเมลที่แนบลิงก์ให้ลูกค้ากรอกข้อมูลส่วนตัว
- หากได้รับอีเมลที่น่าสงสัย ควรติดต่อบริษัทโดยตรงผ่านช่องทางที่เป็นทางการ เช่น เว็บไซต์หลัก หรือหมายเลขโทรศัพท์ที่ตรวจสอบได้

✅ **สังเกตสัญญาณเตือนของอีเมลฟิชชิ่ง**

- ใช้ภาษาที่ผิดปกติ มีข้อผิดพลาดทางไวยากรณ์ หรือใช้คำไม่เป็นทางการ
- ส่งมาจากโดเมนอีเมลที่ดูผิดปกติ หรือคล้ายกับของจริงแต่ไม่เหมือนกัน เช่น @kasikorn-bank.com แทนที่จะเป็น @kasikornbank.com
- มีข้อความเร่งด่วนหรือข่มขู่ว่าบัญชีของคุณจะถูกปิดหากไม่ดำเนินการทันที

7.10 **แนวทางปฏิบัติและคำแนะนำการป้องกันแรนซัมแวร์**

✅ หลีกเลี่ยงการเปิดอีเมลที่ต้องสงสัย

✅ สำรองข้อมูลโดยการใช้กฎ 3-2-1 Backup rule

- Backup ข้อมูล 3 ชุด เช่น เก็บต้นฉบับบนเครื่องคอมพิวเตอร์ และอุปกรณ์อื่นๆ อีก 2 ชุดเสมอ
- ใช้ 2 เทคโนโลยีในการสำรองข้อมูลเป็นอย่างน้อยเสมอ เพื่อจะได้ไม่เสียหายด้วยสาเหตุเดียวกัน เช่น ใช้ External Hard disk และ Flash drive
- มีการสำรองข้อมูล 1 ชุดไปยังที่อื่น สถานที่อื่น หรือแบบออฟไลน์เสมอ

✅ ติดตั้งซอฟต์แวร์ป้องกันไวรัสที่มีประสิทธิภาพ และ Update patch ซอฟต์แวร์เพื่อให้ได้รับการรักษาความปลอดภัยที่ทันสมัยล่าสุดอยู่เสมอ

✅ กำหนดสิทธิในการใช้งานระบบของผู้ใช้แต่ละคน เช่น จำกัดสิทธิในการติดตั้งโปรแกรมหรือแอปพลิเคชัน

✅ ลดช่องทางการเข้าถึง (Attack surface) เนื้อหาที่สำคัญ เช่น จากเครือข่ายภายใน หรือ Websites หรือ Applications

7.11 **วิธีตั้งรหัสผ่านที่ปลอดภัย**

✅ รหัสผ่านควรประกอบด้วยตัวอักษรตัวใหญ่ ตัวอักษรตัวเล็ก และตัวเลขที่สลับลำดับกัน หรืออาจผสมอักขระพิเศษลงไปด้วยเพื่อเพิ่มความปลอดภัย (ยิ่งหลากหลาย ยิ่งถอดรหัสได้ยากขึ้น)

✅ ควรตั้งรหัสผ่านให้มีความยาวอย่างน้อย 8 ตัวอักษรขึ้นไป และทดสอบความแข็งแรงของรหัสผ่าน (มหาวิทยาลัยมีแผนให้ผู้ใช้ตั้งรหัสผ่านใหม่ 12 ตัวอักษรขึ้นไป)

✅ ไม่ควรตั้งรหัสผ่านเป็นเบอร์โทรศัพท์ หรือคำที่เกี่ยวข้องกับตัวเรา เช่น ชื่อ นามสกุล เบอร์โทรศัพท์ หรือข้อมูลอื่น ๆ ของตนเองหรือญาติพี่น้อง

✅ การตั้งรหัสผ่านที่ไม่มีความหมายชัดเจนมีความปลอดภัยมากกว่าการใช้คำที่มีความหมาย เช่น do&12sS@d2

✅ รหัสผ่านควรมีการเปลี่ยนอย่างน้อย 1 ครั้งภายใน 2-3 เดือน

✅ หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับหลาย ๆ บัญชี เพื่อลดความเสี่ยงจากการถูกเจาะเข้าถึงบัญชีอื่น ๆ

✅ ไม่ควรเลือกบันทึกรหัสผ่านอัตโนมัติในเบราว์เซอร์ เพราะสามารถถูกเข้าถึงและขโมยข้อมูลได้ง่าย อาจเลือกใช้ตัวจัดการรหัสผ่าน (Password Manager) ที่น่าเชื่อถือแทน

✅ ใช้ระบบยืนยันตัวตนหลายขั้น (Multi-Factor Authentication) เพื่อเพิ่มความปลอดภัย

7.12 **การป้องกันมัลแวร์และไวรัสคอมพิวเตอร์**

✅ อัปเดตระบบปฏิบัติการและซอฟต์แวร์อย่างสม่ำเสมอ เพื่อลดช่องโหว่ด้านความปลอดภัย

✅ ติดตั้งและอัปเดตโปรแกรมป้องกันไวรัส และเปิดใช้งานการสแกนอัตโนมัติ

✅ เปิดใช้งานไฟร์วอลล์ (Firewall) เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

✅ ไม่ดาวน์โหลดหรือติดตั้งโปรแกรมจากแหล่งที่ไม่น่าเชื่อถือ เช่น เว็บไซต์เถื่อน หรือไฟล์แนบจากอีเมลที่ไม่รู้จัก

✅ ระมัดระวังการคลิกลิงก์หรือไฟล์แนบในอีเมล โดยเฉพาะอีเมลที่ไม่ทราบที่มา

✅ สำรองข้อมูลสำคัญอย่างสม่ำเสมอ เพื่อป้องกันข้อมูลสูญหายในกรณีติดมัลแวร์

✅ ไม่เสียบ Flash drive หรืออุปกรณ์ USB ที่ไม่น่าเชื่อถือโดยไม่ได้สแกนไวรัสก่อน

✅ หลีกเลี่ยงการใช้ซอฟต์แวร์เถื่อน เพราะอาจมีมัลแวร์แฝงมา

✅ ปิดการใช้งาน Macro ในไฟล์เอกสาร โดยเฉพาะจากแหล่งที่ไม่น่าเชื่อถือ

✅ ใช้รหัสผ่านที่แข็งแรง และไม่ใช้รหัสผ่านเดิมซ้ำกันในหลายระบบ

✅ ระมัดระวังการใช้งานเว็บไซต์ หลีกเลี่ยงเว็บไซต์ที่ไม่มี HTTPS หรือแสดงพฤติกรรมไม่น่าไว้ใจ

✅ ตั้งค่าการจำกัดสิทธิ์ของบัญชีผู้ใช้ ไม่ใช้บัญชีที่มีสิทธิ์ Admin โดยไม่จำเป็น

✅ ปิดการใช้งาน Remote Desktop Protocol (RDP) หากไม่มีความจำเป็น เพื่อป้องกันการเข้าถึงจากแฮ็กเกอร์

✅ อัปเดตและตรวจสอบส่วนขยายของ Browser เช่น Google Chrome Extension เพื่อป้องกันการติดมัลแวร์จากปลั๊กอินที่ไม่พึงประสงค์

8. Digital Footprint และการปกป้องข้อมูลส่วนบุคคล

ข้อมูลที่เกิดขึ้นบนโลกออนไลน์ที่เกิดจากการใช้อินเทอร์เน็ตหรือแอปพลิเคชันต่าง ๆ เช่น โพสต์บนโซเชียลมีเดีย ข้อความในฟอรัม การค้นหาผ่าน Google หรือการชำระเงินออนไลน์ ข้อมูลเหล่านี้สามารถถูกติดตามและบันทึกไว้ ซึ่งสามารถสร้างการระบุบุคคลและติดตามพฤติกรรมของบุคคลได้ตลอดเวลา

- **Active Digital Footprint**: ข้อมูลที่ผู้ใช้สร้างขึ้นโดยตรง เช่น การโพสต์ข้อความ ภาพ หรือการแสดงความคิดเห็นบนเว็บไซต์และโซเชียลมีเดีย
- **Passive Digital Footprint**: ข้อมูลที่ถูกบันทึกจากพฤติกรรมการใช้งาน เช่น การเก็บข้อมูลการท่องเว็บ หรือการใช้ข้อมูลจากคุกกี้ (Cookies) ของเว็บไซต์

<u>แนวทางการปกป้องข้อมูล</u>

(1) **ตั้งค่าความเป็นส่วนตัว** (Privacy Settings)
   - ตรวจสอบการตั้งค่าความเป็นส่วนตัวในบัญชีโซเชียลมีเดีย เช่น Facebook, Instagram, X เพื่อจำกัดผู้ที่สามารถเห็นข้อมูลส่วนตัวของเรา
   - ปรับการตั้งค่าความเป็นส่วนตัวของแอปพลิเคชันในโทรศัพท์มือถือเพื่อไม่ให้ข้อมูลส่วนตัวถูกแชร์โดยไม่จำเป็น

(2) **การใช้รหัสผ่านที่แข็งแรง**
   - สร้างรหัสผ่านที่มีความซับซ้อน รวมทั้งใช้รหัสผ่านที่แตกต่างกันสำหรับแต่ละบัญชี
   - เปิดใช้งานการยืนยันตัวตนแบบสองขั้นตอน (Two-factor Authentication) เพื่อเพิ่มความปลอดภัย

(3) **หลีกเลี่ยงการแชร์ข้อมูลที่ไม่จำเป็น**
   - ไม่แชร์ข้อมูลส่วนตัวที่ไม่จำเป็นบนโซเชียลมีเดีย เช่น หมายเลขโทรศัพท์, ที่อยู่, หรือข้อมูลบัตรเครดิต
   - หลีกเลี่ยงการกรอกข้อมูลที่ไม่จำเป็นในเว็บไซต์ที่ไม่รู้จักหรือไม่น่าเชื่อถือ

(4) **ใช้** VPN (Virtual Private Network)

- ใช้ VPN ในการเชื่อมต่ออินเทอร์เน็ตเพื่อปกป้องข้อมูลที่ส่งผ่านเครือข่ายและลดความเสี่ยงจากการติดตามหรือแฮ็กเกอร์
- VPN จะช่วยปกปิด IP Address และทำให้ข้อมูลการท่องเว็บของเราไม่สามารถติดตามได้

(5) **ตรวจสอบสิทธิ์การเข้าถึงข้อมูล** (Permissions)

- ตรวจสอบสิทธิ์ที่แอปพลิเคชันหรือเว็บไซต์ขอเข้าถึงข้อมูลส่วนบุคคล เช่น การเข้าถึงตำแหน่งที่ตั้ง, รายชื่อผู้ติดต่อ, หรือข้อมูลการใช้งาน
- หากพิจารณาแล้วการทำงานของแอปพลิเคชันไม่จำเป็นต้องใช้ข้อมูลเหล่านั้น ควรปฏิเสธการอนุญาต

(6) **ใช้การค้นหาที่เป็นส่วนตัว** (Private Search Engines)

- เลือกใช้เครื่องมือค้นหาที่ไม่ติดตามข้อมูลการค้นหาของเรา เช่น DuckDuckGo หรือ StartPage เพื่อป้องกันการบันทึกข้อมูลการค้นหาของเรา

(7) **ตรวจสอบบัญชีและแอปพลิเคชันที่เชื่อมโยงกับบัญชีของคุณ**

- ตรวจสอบแอปพลิเคชันและบริการต่าง ๆ ที่เชื่อมโยงกับบัญชีออนไลน์ของเราอย่างสม่ำเสมอ และตัดการเชื่อมโยงที่ไม่จำเป็น
- หากพบว่ามีแอปพลิเคชันหรือบริการที่ไม่น่าเชื่อถือ ควรลบหรือยกเลิกการเชื่อมต่อทันที

(8) **ลบข้อมูลที่ไม่จำเป็น**

- ลบโพสต์ ข้อความ หรือข้อมูลส่วนบุคคลที่อาจเผลอโพสต์ไปในโซเชียลมีเดียหรือเว็บไซต์ต่าง ๆ
- ใช้บริการลบข้อมูลออนไลน์ที่เก็บข้อมูลส่วนตัวออกไปหากจำเป็น

(9) **ระมัดระวังเมื่อใช้** Wi-Fi **สาธารณะ**

- หลีกเลี่ยงการทำธุรกรรมหรือส่งข้อมูลสำคัญผ่าน Wi-Fi สาธารณะ โดยเฉพาะข้อมูลที่มีความเสี่ยงสูง เช่น ข้อมูลการเงินหรือข้อมูลส่วนบุคคล

(10) **การตรวจสอบและจัดการกับข้อมูลจากคุกกี้** (Cookies)

- ตรวจสอบนโยบายการใช้คุกกี้ของเว็บไซต์ที่เราท่องเว็บและปิดการใช้งานคุกกี้ที่ไม่จำเป็น

แหล่งข้อมูลอ้างอิง:

World Economic Forum. (2025). Global risks report 2025. https://www.weforum.org/publications/global-risks-report-2025

Check Point Research. (2024, October 17). A closer look at Q3 2024: 75% surge in cyber attacks worldwide. https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์. เอกสารประกอบการอบรมยกระดับภาคธุรกิจเพื่อป้องกันและรับมือภัยคุกคามทางไซเบอร์ และคุ้มครองข้อมูลส่วนบุคคล โครงการ “ยกระดับภาคธุรกิจเพื่อป้องกันและรับมือภัยคุกคามทางไซเบอร์”.

Check Point Research. (2025). The state of cyber security 2025. https://www.checkpoint.com/security-report/

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. สถิติภัยคุกคามทางไซเบอร์. https://ncsa.or.th/policy/threat-statistics

สำนักงานตำรวจแห่งชาติ. สถิติคดีออนไลน์. https://www.thaipoliceonline.go.th/

Thailand National Cyber Academy. ช่อง YouTube: Thailand National Cyber Academy. https://www.youtube.com/@THNCAbyNCSA

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยแห่งชาติ. เอกสารเผยแพร่ และคลังความรู้. https://www.ncsa.or.th/home

ราชกิจจานุเบกษา. (2562). พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562. https://www.dga.or.th/document/106069/

ราชกิจจานุเบกษา. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์. https://www.dga.or.th/upload/download/file_ce8c32197b28a5d438136a3bd8252b7c.pdf

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. กฎหมายคุ้มครองข้อมูลส่วนบุคคล. https://www.mdes.go.th/mission/detail/2319-กฎหมายคุ้มครองข้อมูลส่วนบุคคล

Digital Council of Thailand. (2020). สรุปสาระสำคัญพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. https://www.dct.or.th/upload/downloads/1612025563SummaryPDPA_DigitalCouncilofThailand.pdf

ราชกิจจานุเบกษา. (2565). มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕. https://www.ratchakitcha.soc.go.th/DATA/PDF/2565/E/140/T_0028.PDF

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล. เว็บไซต์ทางการ. https://www.pdpc.or.th/

T-REG. (2022). สรุป ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565. https://t-reg.co/blog/news/guideline-for-data-breach-report-pdpa-law/

Everyday Marketing. การหลุดรั่วของข้อมูลส่วนบุคคลในประเทศไทย และแนวทางเบื้องต้นในการปฏิบัติให้สอดคล้องกับกฎหมาย PDPA. https://everydaymarketing.co/knowledge/leakage-of-personal-information/

คณะกรรมการการรักษาความมั่นคงปลอดภัยแห่งชาติ. สื่อประชาสัมพันธ์ด้านภัยคุกคามทางไซเบอร์. https://www.facebook.com/NCSA.Thailand

ศูนย์ต่อต้านข่าวปลอม ประเทศไทย. เว็บไซต์ศูนย์ต่อต้านข่าวปลอม. https://www.antifakenewscenter.com/