รอบ2
ปีงบประมาณ
พ.ศ.2567

สรุปบทเรียนจากการพัฒนาความรู้

หลักสูตร
การสร้างความมั่นคงปลอดภัยทางไซเบอร์

จัดทำโดย นางสาวอุบลลักษณ์ เทียมทัด

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

เจตนารมณ์ เพื่อกำหนดให้ การคุ้มครองข้อมูลส่วนบุคคล มีประสิทธิภาพในการเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจากการถูกล่วงละเมิด มิให้มีการกระทำได้โดยง่าย

เหตุผลและความจำเป็นในการจำกัดสิทธิและเสรีภาพของบุคคล

เพื่อให้มีมาตรการเยียวยาเจ้าของข้อมูล ส่วนบุคคลจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคลที่มีประสิทธิภาพ เนื่องจาก

1. ในปัจจุบัน มีการล่วงละเมิดสิทธิความเป็นส่วนตัว ของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล
2. ความก้าวหน้าของเทคโนโลยี ทำให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว ทำได้โดยง่าย สะดวกและรวดเร็ว ก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวม

การเก็บรวบรวมข้อมูลส่วนบุคคล

เก็บรวบรวมได้เท่าที่จำเป็น ภายใต้วัตถุประสงค์อันชอบด้วยกฎหมาย ต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียด ดังต่อไปนี้

- วัตถุประสงค์ของการเก็บรวบรวม
- แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบว่าต้องให้ข้อมูล เพื่อปฏิบัติตามกฎหมายหรือสัญญา
- ระยะเวลาในการจัดเก็บ ข้อมูลส่วนบุคคล
- ประเภทของข้อมูลหรือหน่วยงาน ซึ่งข้อมูลส่วนบุคคล ที่เก็บรวบรวมอาจจะถูกเปิดเผย
- ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อและวิธีการติดต่อ
- สิทธิของเจ้าของข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน Sensitive Personal Data

- เชื้อชาติ เผ่าพันธุ์
- ความคิดเห็นทางการเมือง
- ความเชื่อในลัทธิศาสนาหรือปรัชญา
- พฤติกรรมทางเพศ
- ประวัตอาชญากรรม
- ข้อมูลสุขภาพความพิการ
- ข้อมูลสหภาพแรงงาน
- ข้อมูลพันธุกรรม
- ข้อมูลชีวภาพ
- ข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด

ข้อยกเว้น การเก็บรวบรวม ข้อมูลส่วนบุคคล โดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

- การจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุ เพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติ ต้องจัดให้มีมาตรการป้องกันที่เหมาะสม
- เพื่อป้องกันหรือระงับอันตราย ต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล
- เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญา
- เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ/ปฏิบัติหน้าที่ในการใช้อำนาจรัฐ
- เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมาย ของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลหรือนิติบุคคลอื่น
- เป็นการปฏิบัติตามกฎหมาย ของผู้ควบคุมข้อมูลส่วนบุคคล

ข้อห้ามในการเก็บรวบรวมข้อมูลส่วนบุคคล จากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง

1. ได้แจ้งถึงการเก็บรวบรมข้อมูลส่วนบุคคลจากแหล่งอื่น ให้แก่เจ้าของข้อมูลส่วนบุคคล ทราบโดยไม่ชักช้า แต่ต้องไม่เกินสามสิบวันนับแต่วันที่เก็บรวบรวม และได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
2. เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอม

การใช้หรือเปิดเผยข้อมูลส่วนบุคคล

1. ห้ามใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอม เว้นแต่ เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอม

2. บุคคลหรือนิติบุคคลที่ได้รับข้อมูลส่วนบุคคลมาจากผู้ควบคุมข้อมูลส่วนบุคคล จะต้องไม่ใช้หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งไว้ในการขอรับข้อมูลส่วนบุคคลนั้น
3. การใช้หรือเปิดเผยข้อมูลส่วนบุคคล ที่ได้รับยกเว้นไม่ต้องขอความยินยอม ผู้ควบคุมข้อมูลส่วนบุคคต้องบันทึกการใช้หรือเปิดเผยนั้นไว้ด้วย

สิทธิของเจ้าของข้อมูลส่วนบุคคล

1. สิทธิที่ได้รับการแจ้งให้ทราบ ก่อนหรือในขณะที่เก็บรวบรวมข้อมูลส่วนบุคคล เช่น เก็บข้อมูลอะไรบ้าง, วัตถุประสงค์การเก็บข้อมูล, การนำไปใช้หรือส่งต่อวิธีเก็บข้อมูลอย่างไร, ระยะเวลาการจัดเก็บข้อมูล, การเปลี่ยนแปลงแก้ไข เพิกถอนข้อมูลส่วนบุคคล เป็นต้น
2. สิทธิขอเข้าถึงข้อมูลส่วนบุคคล การเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาของข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยิมได้ โดยสิทธินี้จะต้องไม่ขัดต่อกฎหมายหรือคำสั่งศาล หรือส่งผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น
3. สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคล ที่เกี่ยวกับตนเมื่อใดก็ได้ แต่ต้องไม่ขัดด้วยกฎหมาย หรือขัดต่อสิทธิการเรียกร้องตามกฎหมาย
4. สิทธิขอให้ลบหรือทำลาย สิทธิขอทำให้เป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลถูกขอให้ลบ หรือทำบาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลเจ้าของได้ โดยผู้ควบคุมข้อมูลส่วนบุคคลจะต้องเป็นผู้รับผิดชอบดำเนินการทั้งในทางเทคโนโลยีและค่าใช้จ่ายเอง
5. สิทธิในการเพิกถอนความยินยอม ถ้าเจ้าของข้อมูลเคยให้ความยินยอมในการใช้ข้อมูลไป การยกเลิกจะต้องไม่ขัดต่อข้อจำกัดสิทธิในการถอนความยินยอมทางกฎหมาย หรือสัญญาที่ได้ให้ความยินยอมไปก่อนหน้านี้
6. สิทธิขอให้ระงับการใช้ข้อมูล ไม่ว่าจะเป็นการเปลี่ยนใจไม่ต้องให้ข้อมูล หรือเปลี่ยนใจระงับการทำลายข้อมูลเมื่อครบกำหนดที่ต้องทำลาย
7. สิทธิในการขอให้แก้ไขข้อมูลส่วนบุคคล ให้มีความถูกต้อง เป็นปัจจุบัน และไม่ก่อให้เกิดความเข้าใจผิดได้ โดยการแก้ไขนั้นจะต้องเป็นไปด้วยความสุจริตและไม่ขัดต่อหลักกฎหมาย
8. สิทธิในการขอให้โอนข้อมูลส่วนบุคคล กรณีเจ้าของข้อมูลต้องการนำข้อมูลที่เคยให้ไว้กับผู้ควบคุมข้อมูลรายหนึ่งไปใช้กับผู้ควบคุมข้อมูลอีกราย โดยการใช้สิทธินั้นต้องไม่ขัดต่อกฎหมายสัญญา หรือละเมิดสิทธิเสรีภาพของบุคคลอื่น

ภัยอันตรายจากโลกไซเบอร์ในรูปแบบต่าง ๆ

การทำสงครามไซเบอร์ (Cyber Warfare) ส่งผลกระทบหลายด้านต่อประเทศ, องค์กร, และบุคคล ผลกระทบที่สำคัญ ได้แก่

1. ความเสียหายทางเศรษฐกิจ : การโจมตีทางไซเบอร์สามารถทำลายหรือหยุดยั้งการดำเนินงานของธุรกิจ ส่งผลให้เกิดความสูญเสียทางการเงินอย่างมหาศาล ตัวอย่าง เช่น การโจมตีแบบ ransomware ที่เข้ารหัสข้อมูลและเรียกร้อยค่าไถ่
2. ผลกระทบต่อความมั่นคงทางสังคมและการเมือง : การโจมตีทางไซเบอร์สามารถทำลายความไว้วางใจในรัฐบาลและสถาบันอื่น ๆ การแทรกแซงในกระบวนการเลือกตั้งหรือการประกาศข้อมูลก็สามารถสร้างความไม่สงบในสังคม
3. ความเสียหายต่อโครงสร้างพื้นฐาน : การโจมตีโครงสร้างพื้นฐานสำคัญ เช่น ระบบไฟฟ้า, น้ำ, การขนส่ง, และสื่อสาร สามารถสร้างผลกระทบร้ายแรงต่อชีวิตประจำวันและความปลอดภัยของประชาชน
4. ความเสียหายด้านข้อมูล : การโจมตีทางไซเบอร์สามารถนำไปสู่การขโมยข้อมูลสำคัญ เช่น ข้อมูลส่วนบุคคล, ข้อมูลทางการเงิน, หรือข้อมูลลับของรัฐบาล
5. ผลกระทบทางจิตวิทยาและสังคม : การโจมตีทางไซเบอร์สามารถสร้างความกลัว ความไม่แน่นอน และความไม่ไว้วางใจในเทคโนโลยีซึ่งส่งผลกระทบต่อการรับรู้และพฤติกรรมของประชาชน
6. ผลกระทบต่อกฎหมายและนโยบาย : การทำสงครามไซเบอร์ต้องการการตอบสนองทางกฎหมายและนโยบายใหม่ ๆ เพื่อป้องกันและจัดการกับความท้าทายเหล่านี้
7. การแข่งขันทางเทคโนโลยี : มีการแข่งขันเพื่อพัฒนาความสามารถทางไซเบอร์ทั้งในด้านการป้องกันและการโจมตี ส่งผลให้เกิด “การแข่งขันอาวุธไซเบอร์” ระหว่างประเทศต่าง ๆ

สถานการณ์ภัยคุกคามไซเบอร์ระดับโลก

Ransomware เป็นการโจมตีที่มีสัดส่วนสูงสุด 23 % ตามด้วน Data Theft และ Server Access ซึ่งมีสัดส่วน 13 % และ 10 % ตามลำดับ

1. Ransomware ไฟล์ถูกเข้ารหัสทำให้ผู้ใช้งานไม่สามารถเปิดไฟล์ได้ โดยผู้ใช้งานจะต้องจ่ายเงินตามข้อความ “เรียกค่าไถ่” เพื่อปลดล๊อคกู้ข้อมูลคืนมา
2. Data Theft ส่วนใหญ่เกิดจากบุคคลภายในองค์กรด้วยมองว่าข้อมูลเป็นสิทธิ์ของตนเนื่องจากเป็นผู้จัดทำขึ้น หรือจงใจละเมิดการเข้าถึงข้อมูลเพื่อเปิดเผยการประพฤติมิชอบของนายจ้างจากมุมมองของสังคม

3. Server Access การเข้าถึงระบบโดยไม่ได้รับอนุญาตซึ่งอาจจะมีจุดประสงค์ในการขโมยข้อมูล แก้ไขปรับเปลี่ยน หรือทำให้หยุดชะงัก ไม่สามารถให้บริการแก่ผู้ใช้งานได้

แรนซัมแวร์ (Ransomware)

มัลแวร์ประเภทหนึ่งที่ป้องกันหรือจำกัดสิทธิ์ผู้ใช้งานคอมพิวเตอร์ไม่ให้เข้าถึงระบบไฟล์ หรือเอกสารของตัวเอง โดยการล๊อกหน้าจอของระบบหรือล๊อกไฟล์ของผู้ใช้จนกว่าจะยอมจ่ายเงินค่าไถ่คืนมา จึงถูกเรียกอีกชื่อได้ว่า “มัลแวร์เรียกค่าไถ่”

การขโมยข้อมูลตัวตน (Identity Theft)

การขโมยข้อมูลตัวตน (Identity Theft) เป็นการที่ผู้ไม่ประสงค์ดี ได้นำข้อมูลและรูปภาพของบุคคลนั้นไปใช้โดยไม่ได้รับอนุญาต เพื่อหาผลประโยชน์และสร้างความน่าเชื่อถือในสังคม สาเหตุหนึ่งที่ผู้ไม่ประสงค์ดีนั้นสามารถขโมยข้อมูลตัวตนไปได้ คือ การเปิดเผยข้อมูลส่วนตัวลงบนสื่อสังคมออนไลน์มากเกินไป

การโจมตีในรูปแบบ Dos และ DDos (Countermeasures for DoS (DD0S)

Denial-of-Service (DoS)

- สร้างหลุมเพื่อทำการกรองข้อมูลและอนุญาตให้เส้นทางที่มีสิทธิ์ผ่าน
- ปิดกั้นหน่วยข้อมูลขาเข้าต่อหมายเลขพอร์ด
- ใช้ระบบตรวจจับการบุกรุกเพื่อตรวจจับและป้องกันการโจมตี

Distributed Dos (DDoS)

การป้องกันการโจมตีแบบ DDoS อาจพิจารณาใช้ Content Delivery Network (CDN) หรือเครือข่ายคอมพิวเตอร์แม่ข่ายขนาดใหญ่ ที่กระจายตัวกันอยู่ทั่วโลก ซึ่งเครื่องคอมพิวเตอร์แม่ข่ายเหล่านี้ จะเชื่อมต่อกันผ่านอินเทอร์เน็ต เพื่อทำหน้าที่ในการส่งข้อมูลให้ไปถึงผู้รับปลายทางให้เร็วที่สุด รวมทั้งเพิ่มประสิทธิภาพในการเข้าถึงข้อมูลเหล่านั้นได้ตลอดเวลา

การโจมตีในรูปแบบ InJection

ในการพัฒนาระบบ หากไม่มีการตรวจสอบข้อมูลที่ถูกนำเข้าไปประมวลผล ก็จะมีโอกาสทำให้ผู้ไม่ประสงค์ดีสามารถที่จะปรับแต่ง หรือแก้ไขข้อมูลนำเข้าเหล่านั้นให้อยู่ในรูปแบบภาษาที่ทำให้โปรแกรมทำงานผิดพลาดได้ เช่น การโจมตีที่เรียกว่า SQL Injection ที่ผู้ไม่ประสงค์ดีสามารถเข้าถึง แก้ไข หรือลบข้อมูลในฐานข้อมูลได้ ซึ่งรวมไปถึง ภาษา XML หรือ LDAP Protocol ที่ถูกนำมาใช้ในการเก็บข้อมูลต่าง ๆ

การโจมตีในรูปบบ Zero-Day Exploits

การโจมตี ในรูปแบบ Zero-Day มักจะเกิดขึ้นกับช่องโหว่ที่ถูกค้นพบ โดยผู้ไม่ประสงค์ดี โดยที่ผู้ผลิตซอฟต์แวร์ยังไม่ทราบว่าซอฟต์แวร์ของตนมีช่องโหว่ หรือบางกรณีอาจจะเกิดขึ้นโดยที่ผู้ผลิตซอฟต์แวร์รู้ดีว่าผลิตภัณฑ์ของตนมีช่องโหว่ แต่ยังไม่สามารถพัฒนาโปรแกรมปิดช่องโหว่ (Patch) ได้

ผู้ไม่ประสงค์ดีจะพัฒนาโปรแกรมที่ใช้ในการเจาะระบบออกมา เรียกว่า Zero-Day Exploit ซึ่งในบางครั้งจะมีการแจกจ่ายไปยังผู้ไม่ประสงค์ดีรายอื่น ๆ เพื่อนำไปโจมตีระบบหรืออาจเก็บไว้เพื่อจำหน่าย เพื่อใช้เป็นเครื่องมือในการโจมตีเป้าหมายที่เฉพาะเจาะจงต่อไป

พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์

ความรู้พื้นฐานของความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) ครอบคลุมถึงหลักการ, แนวทางปฏิบัติ, และเทคโนโลยีที่ใช้ในการปกป้องระบบ, เครือข่าย, โปรแกรม, และข้อมูลจากการโจมตีทางไซเบอร์

1. หลักการของความปลอดภัยไซเบอร์
    - ความลับ (Confifentiality) การรักษาข้อมูลให้เข้าถึงได้เฉพาะบุคคลหรือกลุ่มที่ได้รับอนุญาต
    - ความสมบูรณ์ (Integrity) การรักษาความถูกต้องและความเชื่อถือได้ของข้อมูล
    - ความพร้อมใช้งาน (Availability) การทำให้ข้อมูลและทรัพยากรเข้าถึงได้ตามที่ต้องการ

2. การระบุและจัดการภัยคุกคาม : การเข้าใจและระบุภัยคุกคามต่าง ๆ เช่น ไวรัส, มัลแวร์, การโจมตีทางเครือข่าย (network attacks), และการแฮ็ก

3. การป้องกันทางเทคนิค : การใช้ไฟร์วอลล์, แอนตี้ไวรัส, การเข้ารหัสข้อมูล, และระบบป้องกันการรุกราน (Intrusion Detection/Prevention System)

4. การจัดการความเสี่ยง : การประเมินผลและจัดการความเสี่ยงทางไซเบอร์ เพื่อหลีกเลี่ยง, ลด, หรือยอมรับความเสี่ยงตามความเหมาะสม

5. นโยบายและกฎหมาย : การมีนโยบายความปลอดภัยที่ชัดเจนและปฏิบัติตามกฎหมายที่เกี่ยวข้อง

6. การฝึกอบรมและสร้างความตระหนักรู้ : การสร้างความตระหนักรู้ด้านความปลอดภัยไซเบอร์ให้กับผู้ใช้และพนักงาน เพื่อป้องกันการโจมตีแบบ Phishing และ อื่นๆ

7. การเตรียมความพร้อมและการตอบสนองต่อเหตุการณ์ : การมีแผนการตอบสนองเหตุการณ์ไซเบอร์ เพื่อจัดการกับการโจมตีหรือละเมิดความปลอดภัยได้อย่างมีประสิทธิภาพ

การรักษาความปลอดภัยจากอีเมลปลอมแปลง Phishing Mail

การหลอกลวง (Phishing) เป็นการหลอกลวงของผู้โจมตีผ่านทางอีเมล หรือเว็บไซต์ที่คล้ายกับของจริง เพื่อให้เหยื่อเป้าหมาย กรอกข้อมูลส่วนตัวลงไป โดยส่วนใหญ่จะเป็นข้อมูลเกี่ยวกับการทำธุรกรรมกับธนาคาร หรือที่เกี่ยวข้องกับการใช้ข้อมูลส่วนตัว

วิธีการสังเกตว่าอีเมลหรือเว็บไซต์นั้นเป็น Phishing หรือไม่ มีดังนี้

- ตรวจสอบที่อยู่อีเมลว่าใครเป็นคนส่ง เป็นอีเมลที่รู้จักหรือไม่ หากพบว่าเป็นอีเมลที่ไม่รู้แหล่งที่มา ไม่ควรคลิกลิงก์ หรือเปิดไฟล์แนบในอีเมลนั้น
- ตรวจสอบ URL ของเว็บไซต์นั้นว่าเป็น URL ของเว็บไซต์ทางการหรือไม่ หากไม่ใช่ ไม่ควรกรอกข้อมูลลงในเว็บไซต์นั้น

ข้อควรปฏิบัติเมื่อเจอ “อีเมลฟิชชิ่ง”

1. ระวังหากจุดประสงค์ของลิงค์คือ
    - ยืนยันตัวตนของเรา
    - ให้ตรวจสอบบัญชีของคุณ
    - ให้ Update บัญชีของเรา
    - ระบุหมายเลขบัตรเครดิต หรือเลขประกันสังคมของเรา
    - ดาวน์โหลดซอฟต์แวร์
2. ปฏิบัติต่อเมลใดๆ ที่ขอให้เราคลิกลิงค์ด้วยความระมัดระวัง
    - อย่าตอบกลับ คำขอล็อคอินเข้าสู่ระบบ/รีเซ็ตรหัสผ่านที่มาจากอีเมล์ซึ่งเราไม่ได้เป็นผู้ริเริ่มหรือคาดหวัง
    - อย่าให้รายละเอียดส่วนตัวของเราผ่านทางอีเมล หรือลิงค์ในอีเมลใดๆ โดยเฉพาะอย่างยิ่งหากอีเมลนั้นไม่พึงประสงค์
3. บริษัทขนาดใหญ่มักไม่ส่งอีเมลพร้อมลิ้งค์แนบมาเพื่อให้ลูกค้าของบริษัทยืนยันรายละเอียดส่วนบุคคล

- หากมีข้อกังวลใด ๆ ควรโทรศัพท์ถึงบริษัทนั้นเป็นการส่วนตัวหรือไปที่สาขา และอธิบายรายละเอียดให้ทราบ

วิธีตั้งรหัสผ่านที่ปลอดภัย

1. รหัสผ่านต้องประกอบไปด้วย ตัวอักษรตัวใหญ่ ตัวอักษรตัวเล็กและตัวเลข ที่สลับลำดับกัน หรืออาจจะผสมอักขระพิเศษลงไปด้วยก็ได้ (ยิ่งหลากหลายยิ่งถอดรหัสได้ยากขึ้น)
2. ควรตั้งรหัสผ่านให้มีความยาวอย่างน้อย 8 ตัวอักษรขึ้นไป
3. ไม่ควรตั้งรหัสผ่านเป็นเบอร์โทรศัพท์หรือถ้อยคำใด ๆ ที่เกี่ยวกับเรา เช่น ตั้งรหัสผ่านโดยใช้ชื่อ เบอร์โทร และข้อมูลอื่นๆ ที่เกี่ยวกับตัวเราหรือญาติพี่น้อง เป็นต้น
4. การตั้งรหัสผ่านเป็นคำไม่มีความหมาย มีความปลอดภัยกว่าการตั้งรหัสเป็นคำที่มีความหมาย
5. รหัสผ่านควรมีการเปลี่ยนอย่างน้อย 1 ครั้ง ภายใน 2-3 เดือน
6. หลีกเลี่ยงการตั้งรหัสผ่านหลายๆบัญชี เป็นรหัสผ่านเดียวกัน เพื่อเป็นการลดความเสี่ยงที่จะโดนเจาะเข้าบัญชีอื่น ๆ ด้วย
7. ไม่ควรเลือกการจดจำรหัสผ่านอัตโนมัติในเบราว์เซอร์ เพื่ออย่าลืมว่ามันสามารถเข้ามาดูได้โดยง่าย

Security Checklist สำหรับการใช้เครื่องคอมพิวเตอร์

1. ควร Logout ทุกครั้งเมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์
2. มีการอัปเดตแพตซ์บนระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ หรือตั้งค่าอัปเดตอัตโนมัติไปเลย
3. มีการอัฟเดทซอฟต์แวร์ / โปรแกรมบนเครื่องอย่างสม่ำเสมอ เพื่อปิดช่องโหวในเวอร์ชั่นก่อนหน้า
4. มีการติดตั้งซอฟแวร์ป้องกันไวรัสบนเครื่องคอมพิวเตอร์และตั้งค่าการอัปเดตอัตโนมัติเพื่อรับข้อมูลการป้องกันใหม่ล่าสุด
5. เปิด Windows Firewall บน OS
6. ไม่ดาวน์โหลดโปรแกรมมาจากแหล่งที่ไม่น่าเชื่อถือ และหมั่นลบโปรแกรมที่ไม่จำเป็นออกไปบ้าง

Security Checklist สำหรับโทรศัพท์มือถือและแท็บเล็ต

1. เปิดการใช้งาน Passcode, Face ID และ Fingerprint ในการเข้าใช้งานอุปกรณ์ต่าง ๆ
2. มีการอับเดตแพตซ์บนระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ หรือตั้งค่าอับเดตอัตโนมัติไปเลย
3. มีการอับเดตซอฟต์แวร์ / โปรแกรมบนเครื่องอย่างสม่ำเสมอเพื่อปิดช่องโหวในเวอร์ชั่นก่อนหน้า
4. มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสแบบ Mobile และตั้งค่าการอับเดตอัตโนมัติเพื่อรับข้อมูลการป้องกันใหม่ล่าสุด
5. ไม่ติดตั้งแอปพลิเคชันที่น่าสงสัย หรือไม่ทราบผู้พัฒนาที่แน่ชัด

6. กำหนดสิทธิในการเข้าถึงแอปพลิเคชัน (Permission) ให้เหมาะสม
7. ปิดการแจ้งเตือนเกี่ยวกับรหัสความปลอดภัย เช่น OTP บนหน้าจอ
8. เลี่ยงการเก็บข้อมูลสำคัญเอาไว้ในโทรศัพท์มือถือ

Security Checklist สำหรับการใช้งาน Wi-Fi

1. เปลี่ยนรหัสผ่านของอุปกรณ์ Wi-Fi router
2. เปลี่ยน SSID และรหัสผ่านของ Wi-Fi ที่กำหนดมาจากผู้ใช้บริการและซ่อน SSID ถ้าหากเป็นไปได้
3. กำหนดผู้ที่สามารถเชื่อมต่อ Wi-Fi ที่บ้านของเราได้ เช่น การล๊อกให้เฉพาะเครื่องที่มี Mac address ที่กำหนดไว้ เข้าใช้งานได้เท่านั้น
4. ไม่เชื่อมต่อ Public Wi-Fi หรือ Free hotspot ที่เปิดให้ใช้งานฟรีแบบไม่มีรหัสผ่าน
5. หลีกเลี่ยงการใช้งาน Public Wi-fi ที่ไม่ทราบแหล่งที่มาในการเปิดให้บริการ
6. เมื่อออกจากบ้านควรปิดสัญญาณ Wi-Fi เพื่อป้องกันการเชื่อมต่อ Public Wi-Fi อัตโนมัติ

Security Checklist สำหรับการเข้าถึงเว็บไซต์

1. ใช้ Browser ที่ได้มาตรฐานและมีการอัปเดตเวอร์ชั่นของ Web Browser เสมอ
2. ไม่ทำการจดจำหรือบันทึกรหัสผ่าน (Password) การเข้าถึงเว็ปไซต์ต่าง ๆ บน Browser
3. ไม่มีอะไรได้มาฟรี ๆ ไม่ตื่นตระหนก ไม่หลงเชื่ออะไรง่าย ๆ
4. ไม่เข้าใช้งานเว็บไซต์ที่ได้รับการแชร์จากช่องทางที่ไม่แน่ชัด เช่น จากโซเชียลมีเดีย เป็นต้น
5. สังเกต HTTPS เสมอ เมื่อต้องเข้าใช้งานเว็บไซต์ที่เกี่ยวข้องกับการทำธุรกรรมต่าง ๆ หรือต้องมีการกรอกข้อมูลในการเข้าใช้งาน

แหล่งที่มา

หลักสูตร : การสร้างความมั่นคงปลอดภัยทางไซเบอร์
บรรยายโดย :
1. นางสาวดรุณี พิกุลทอง ผู้อำนวยการสำนักกฎหมาย
สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
2. นาวาโท ศักติพงษ์ สิบหมื่นเปี่ยม ผู้อำนวยการฝ่ายเฝ้าระวังภัยคุกคามทางไซเบอร์
สำนักงานปฏิบัติการศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สกมช
สถาบัน/หน่วยงาน/ระบบ : ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมพัฒนาที่ดิน
รูปแบบหลักสูตร : บรรยาย
ช่วงเวลาการฝึกอบรม : พฤษภาคม 2567