รายงานสรุปบทเรียน

ชื่อหลักศูตร/โครงการ : การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์
วันที่เข้ารับการอบรม : ๒๐ กุมภาพันธ์ ๒๕๖๙
สถานที่ : กรมพัฒนาที่ดิน
จัดโดย : สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ผู้จัดทำรายงาน : นายพิทักษ์ ใจอารีย์ ตำแหน่ง นักวิชาการเงินและบัญชีปฏิบัติการ

วัตถุประสงค์

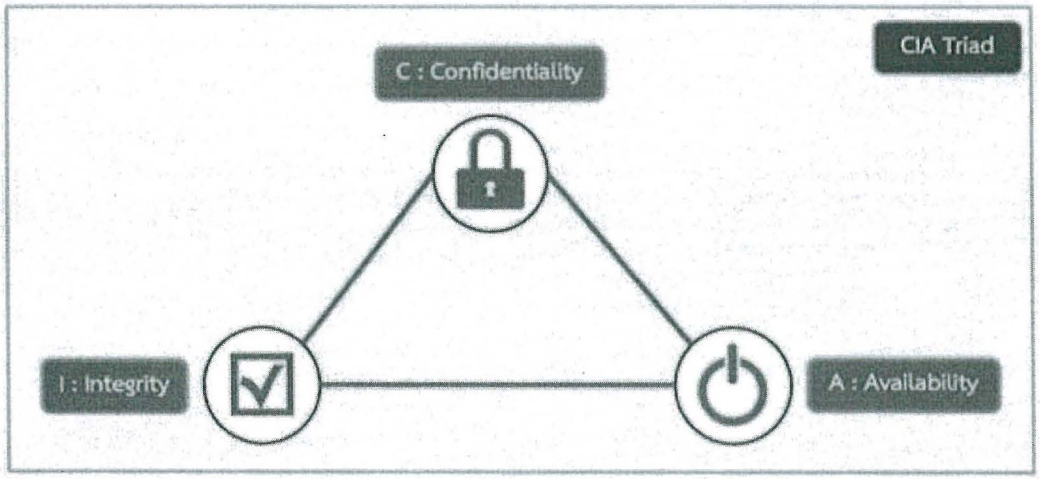
เพื่อให้หน่วยงานหรือเจ้าหน้าที่ปฏิบัติงานได้มีความตระหนักรู้ในด้านความปลอดภัยทางไซเบอร์ ซึ่งจะช่วยลดความเสี่ยงจากเหตุการณ์ด้านความปลอดภัยทางไซเบอร์และช่วยป้องกันความรั่วไหลของข้อมูล การเรียนรู้ดังกล่าวไม่เพียงหยุดยั้งผู้ก่อภัยคุกคามเท่านั้น แต่ยังส่งเสริมให้องค์กรที่มุ่งเน้นความปลอดภัยสูงยิ่งขึ้น ลดความเสี่ยงและสร้างความมั่นใจในความปลอดภัยของข้อมูลบุคคลและหน่วยงาน

สรุปเนื้อหาการฝึกอบรม : การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์

๑. Cybersecurity คืออะไร

Cybersecurity หรือ ความมั่นคงปลอดภัยไซเบอร์ คือ การนำเครื่องมือทางด้านเทคโนโลยี และ กระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์ เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจาก บุคคลที่สามโดยไม่ได้รับอนุญาตในปัจจุบันหน่วยงานภาครัฐ และภาคเอกชนได้เริ่มให้ความสำคัญในเรื่องของความ มั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้น รวมถึงรูปแบบ ของการโจมตีทางด้านไซเบอร์มีความหลากหลายมากยิ่งขึ้น และสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้นเรื่อย ๆ

๒. ความรู้พื้นฐานของ Cybersecurity พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์ (CIA)



C: Confidentiality การรักษาความลับ คือหลักการป้องกันข้อมูลไม่ให้ถูกเข้าถึงเปิดเผย หรือรั่วไหลไปยังบุคคลที่ไม่ได้รับอนุญาต เพื่อให้มั่นใจว่าข้อมูลสำคัญจะถูกใช้โดยผู้มีสิทธิ์เท่านั้น เช่น

- ข้อมูลส่วนเงินเดือนของพนักงานในบริษัท จัดเป็น ความลับสูงสุด ผู้ที่สามารถเข้าถึงได้ คือ ผู้จัดการส่วน ทรัพยากรบุคคลเท่านั้น
- เบอร์โทรของพนักงานในบริษัท จัดเป็น ข้อมูลภายในเท่านั้น ผู้ที่สามารถเข้าถึงได้ คือ พนักงานบริษัท ทุกคน

I: Integrity การรักษาความถูกต้องของข้อมูล คือการระบุสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องต่อเนื่อง เช่น

- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

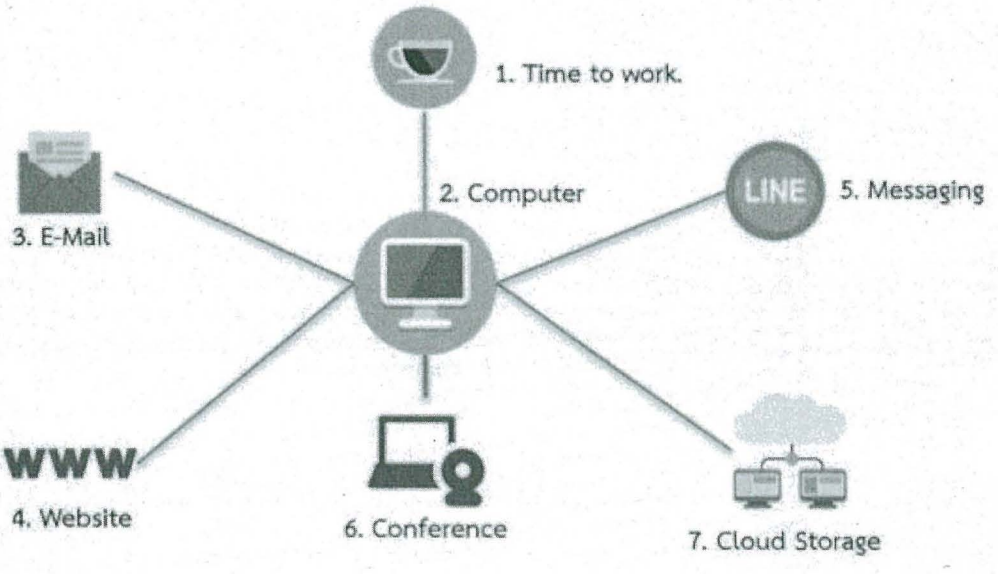
A: Availability ความพร้อมใช้งานของข้อมูล คือการที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล เช่น

- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

๓. รูปแบบภัยคุกคามของ Cybersecurity

- Malware
- Web-based attacks
- Phishing
- Web application attacks
- Spam
- DDoS
- Data breach
- Insider threat
- Botnets
- Ransomware
- Cryptojacking

๔. ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน



สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑) การใช้งานคอมพิวเตอร์

- ควรมีการแยก User ใช้งานกันของแต่ละบุคคล
  ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์
- ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ
- มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
- มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ
- ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ
- มีการใช้ Password ที่ดี และ ไม่ควรบอก Password แก่ผู้อื่น

๒) การใช้ Password ที่ดี

- มีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ (! @ $ #)
- มีความยาวของ Password อย่างน้อย ๘ ตัวอักษร
- ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือ สิ่งที่สามารถคาดเดา ได้ง่าย เช่น password ๑๒๓๔๕๖ วันเกิด หมายเลขโทรศัพท์
- มีการเปลี่ยน Password อย่างสม่ำเสมอ • ใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้
- ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ
- ไม่ควรบอก Password แก่ผู้อื่น

๓) การใช้ E-mail

- ไม่เปิด E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน
- ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน
- ไม่คลิก Link ใน E-Mail โดยไม่มีการตรวจเช็ค
- เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่างๆ ควรมีการเช็คผ่านทางช่องทางอื่นๆ เพิ่มเติม

๔) การใช้ Website

- ไม่เข้าเว็บไซที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง Social ต่างๆ
- ไม่ควรทำการบันทึก Password ต่างๆ บน Browser
- เว็บไซต์สำหรับทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น
- ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งาน เช่น Google Chrome, Mozilla Firefox เป็นต้น
- ควรมีการ Update Version ของ Browser อย่างสม่ำเสมอ
- ในกรณีเครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งาน Browser ในโหมด Safe Web
- ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ

๕) การใช้ Messaging

- ไม่ควรบันทึก Password ไว้ที่โปรแกรม
- กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัว ไม่ควรบันทึกไฟล์ต่างๆ ไว้บนเครื่อง
- มีความตระหนักก่อนเปิด Link หรือ ไฟล์ต่างๆ ที่ได้รับมา • มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ
- ไม่ควรแชร์ข้อมูลหรือข่าวสารต่างๆ โดยไม่ทราบที่มาของข้อมูล

๖) Fake News หรือ ข่าวปลอม เป็นภัยคุกคามใกล้ตัวประเภทหนึ่งที่มีความน่ากลัวอย่างมาก เนื่องจาก ข่าวสารปลอมที่นำมาเผยแพร่นั้นดูมีความน่าเชื่อถือซึ่งทำให้ผู้ที่รับข่าวสารหลงเชื่อ สามารถสร้างกระแส ปลุกปั่นได้ อย่างมีประสิทธิภาพ ส่วนใหญ่ใช้วิธีการเผยแพร่ผ่านทางช่องทางออนไลน์ เช่น LINE Facebook ทำให้มีการ กระจายข่าวได้อย่างรวดเร็วมากยิ่งขึ้น วิธีการสังเกตข่าวปลอม

- มีการพาดหัวข่าว หรือข้อความที่เกินจริง เพื่อสร้างความน่าสนใจ
- ระบุที่มาของข่าวไม่ได้ • มักจะไม่ระบุวันที่ และเวลาที่เกิดเหตุการณ์
- สำนวนการเขียนออกแนวการโฆษณา

๗) การใช้ Conference

- ใช้สถานที่เหมาะสมกับการ Conference
- ในการประชุม Conference ควรมีแต่ผู้ที่เกี่ยวข้อง
- แชร์เอกสารต่างๆ อย่างระมัดระวัง • ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน
- มีการ Update Version ของโปรแกรม Conference อย่างสม่ำเสมอ
- ควรมีการขออนุญาตผู้เข้าร่วมประชุม conference ก่อนที่จะบันทึกภาพและเสียงในการประชุม

๘) การใช้ Cloud Storage

- แยก User ในการใช้งานของแต่ละบุคคล
- ควรกำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็นเท่านั้น
- ปิดการเข้าถึงไฟล์ หรือปิดการแชไฟล์เมื่อไม่มีความจำเป็น
- ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ
- มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ
- มีการตั้ง Password ที่ดี และไม่บอก Password แก่ผู้อื่น

๙) การใช้ WIFI • ไม่ควรใช้งาน WIF! ที่เปิดให้ใช้บริการแบบไม่มีรหัสผ่าน

- หลีกเลี่ยงการใช้งาน WIFI ที่ไม่รู้ที่มาในการให้บริการ

๑๐) การใช้ Mobile

- เปิดการใช้งาน PIN / Password, Face scan หรือ Fingerprint ในการเข้าใช้งานอุปกรณ์
- ไม่ติดตั้ง Application ที่น่าสงสัยหรือไม่รู้แหล่งที่มา
- กำหนด Application permission ให้เหมาะสม
- มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
- มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

๑๑) การใช้ Internet Connection

- เปลี่ยน Default Password ของ Router ที่มาจากโรงงาน
- เปลี่ยน SSID และรหัสผ่านของ WIFI ที่กำหนดมาจากผู้ให้บริการ
- กำหนดผู้ที่สามารถเข้าใช้งาน Internet เท่าที่จำเป็น

ประโยชน์ที่ได้รับ

ผู้เข้าอบรมได้รู้เกี่ยวกับภัยคุกคามไซเบอร์ที่เกิดขึ้นในการทำงานและมีความรู้เกี่ยวกับวิธีการป้องกันภัยคุกคาม ไซเบอร์ให้ปลอดภัยจากภัยคุกคามในรูปแบบต่าง ๆ และสามารถนำความรู้มาประยุกต์ใช้ในการทำงานและชีวิตในปัจจุบัน