รายงานสรุปบทเรียน

ชื่อโครงการฝึกอบรม : หลักสูตร "การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Awareness) สำหรับผู้ใช้งานระบบสารสนเทศของกรมพัฒนาที่ดิน"

วันที่เข้ารับการอบรม : วันที่ ๑๙ – ๒๐ กุมภาพันธ์ ๒๕๖๙

สถานที่ : ห้องปฏิบัติการฝึกอบรมคอมพิวเตอร์และภูมิสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ชั้น ๑ กรมพัฒนาที่ดิน

จัดโดย : ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมพัฒนาที่ดิน

ผู้จัดทำรายการ : นางสาวกนิษฐา ปิติฤทธิ์ นักวิชาการเงินและบัญชีปฏิบัติการ

วัตถุประสงค์ : เพื่อการพัฒนาความรู้ ความเข้าใจเกี่ยวกับการป้องกันภัยทางไซเบอร์ และความเสี่ยงที่จะเกิดความเสียหายต่อระบบสารสนเทศขององค์กรจากการใช้งาน เกิดความตระหนักถึงภัยคุกคามไซเบอร์ที่เกิดขึ้นในปัจจุบัน แนวทางการป้องกัน แก้ไขปัญหาได้อย่างถูกต้อง นำความรู้ไปประยุกต์ใช้ในการทำงานได้ และเกิดความรู้ความเข้าใจรวมถึงสร้างความตระหนักถึงความเสี่ยงจากการใช้งานข้อมูลส่วนบุคคล

สรุปเนื้อหาการฝึกอบรม :

มีความรู้ ความเข้าใจเกี่ยวกับการป้องกันภัยทางไซเบอร์ และความเสี่ยงที่จะเกิดความเสียหายต่อระบบสารสนเทศขององค์กรจากการใช้งาน ดังนี้

Cyber Security คือ ความมั่นคงปลอดภัยทางไซเบอร์ ที่ต้องการป้องกันและการรักษาความปลอดภัยของระบบคอมพิวเตอร์ ระบบเครือข่าย และข้อมูลที่เกี่ยวข้อง โดยประกอบไปด้วย ระบบสารสนเทศ (Information System) โปรแกรมประยุกต์ (Application) ข้อมูล (Data) ระบบคอมพิวเตอร์หรือเครื่องมือที่ใช้ในการเข้าระบบเครือข่าย (Mobile Phone, Tablet, TV, IoT) หน่วยบันทึกข้อมูลและอุปกรณ์เครือข่าย (Storage, Network Device) ศูนย์ข้อมูล (Data Center) รวมถึงกระบวนการบริหารจัดการด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับความปลอดภัย ของระบบคอมพิวเตอร์โดยเฉพาะระบบเครือข่ายอินเตอร์เน็ต

การนำเครื่องมือทางด้านเทคโนโลยี และกระบวนการ วิธีการปฏิบัติที่ถูกออกแบบไว้แล้ว เพื่อป้องกันรับมือ การโจมตีอุปกรณ์เครือข่าย โครงสร้างพื้นฐาน ทางสารสนเทศ ระบบ หรือโปรแกรม จากบุคคลที่สามโดยไม่ได้รับอนุญาต พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงทาง

Cyber Security ประกอบด้วย CIA Triad

๑. Confidentiality การรักษาความลับของข้อมูล คือ การระบุสิทธิ์ในการเข้าถึงข้อมูลตามแต่ละระดับชั้น ที่กำหนดไว้ เช่น พนักงานบริษัทเข้าถึงข้อมูลได้แค่ระดับที่หนึ่ง ส่วนผู้จัดการเข้าถึงข้อมูลได้ถึงระดับที่สาม

๒. Integrity การรักษาความถูกต้องของข้อมูล คือ การระบุสิทธิการแก้ไขข้อมูล และการรักษาความถูกต้อง ของข้อมูลให้มีความถูกต้องต่อเนื่อง เช่น ข้อมูลบัญชีธนาคาร

๓. Availability หรือ ความพร้อมใช้งานของข้อมูล คือ ข้อมูลต้องสามารถเข้าถึงได้ตลอดเวลา

รูปแบบภัยคุกคามทางไซเบอร์

๑. Malware คือ ซอร์ฟแวร์ หรือ Code ประเภทหนึ่ง ถูกเขียนโปรแกรมให้เข้าถึงในส่วนที่ต้องการ โดยการ คลิกติดตั้งหรือแค่ดาวโหลดลงบนอุปกรณ์ ตัวโปรแกรมก็สามารถทำงานได้เลยทันที สามารถติดต่อเป็นวงกว้างได้ คล้ายเชื้อไวรัสในมนุษย์ ขึ้นอยู่กับการออกแบบโปรแกรมของผู้ไม่ประสงค์ดี ชื่อเรียก Malware ครอบคลุมถึง ๑.๑) ไวรัส(Virus) ๑.๒) เวิร์ม (Worms) ๑.๓) โทรจัน(Trojans)

๒. Web-based attacks คือ การโจมตีเหยื่อผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์ปลอม หรือ Hack เว็บไซต์ ที่มีช่องโหว่ แล้วทำการเขียน Code ใหม่ลงไป เพื่อให้ Link เข้าไปสู่เว็บไซต์ที่เขียน Malware ไว้

๓. Phishing คือ การโจมตีเหยื่อผ่านทางช่องทางต่าง ๆ เช่น E-mail, Sms, เว็บไซต์ เป็นต้น โดยหลอกให้คลิก หรือกรอกรหัสผ่าน แล้วนำข้อมูลต่าง ๆ ไปทำธุรกรรม

๔. Web application attacks คือ การโจมตีเว็บไซต์โดยอาศัยช่องโหวต่าง ๆ หรือเว็บไซต์ที่ขาดการ Update แล้วมีช่องโหให้สามารถ Hack เข้ามาเปลี่ยนแปลงข้อมูลบางอย่างได้

๕. Spam คือ ผู้ไม่ประสงค์ดีทำการส่งข้อมูล ข้อความ หรือโฆษณาต่าง ๆ จำนวนมาก ผ่านช่องทางต่าง ๆ เช่น Sms, E-mail, เว็บไซต์ โดยที่ผู้รับไม่ได้อนุญาต เพื่อก่อกวนหรือสร้างความรำคาญ

๖. DDOS (Distributed Denial of Service) เป็นวิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์ หรือระบบให้บริการ โดยใช้เครื่องมือจำนวนมาก ยิ่งเข้าไปที่ระบบพร้อมกัน เพื่อให้ระบบใช้งานไม่ได้

๗. Data breach เกิดจากการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว หรือการโจมตีเพื่อขโมยข้อมูล ของเว็บไซต์หรือแอปพลิเคชัน หรือระบบที่ให้บริการต่าง ๆ เพื่อนำข้อมูลไปขายหรือเพื่อเรียกค่าไถ่ของข้อมูล ชุดนั้น ๆ

๘. Insider threat คือ หรือเรียกว่า “เกลือเป็นหนอน” เกิดจากบุคลากรภายในองค์กร อาจเกิดจากความตั้งใจหรือไม่ตั้งใจ เนื่องจากรู้ระบบภายในเป็นอย่างดี สามารถทำลายระบบได้โดยตรง ก่อให้เกิดความเสียหาย อย่างร้ายแรง

๙. Botnets หรือ Robot Network คือ โปรแกรมที่ถูกเขียนโดยผู้ไม่ประสงค์ดี ทำการแฝงตัว และ ติดตั้งอยู่ใน คอมพิวเตอร์หรืออุปกรณ์ต่าง ๆ รอรับคำสั่งจากผู้ไม่ประสงค์ดี ส่วนมากเจ้าของเครื่องจะไม่ทราบว่าโดน Botnets แฝงตัว เนื่องจากตัวโปรแกรมไม่ได้ทำงานตลอดเวลา

๑๐. Ransomware หรือ Malware ประเภทหนึ่ง มีจุดประสงค์คือการล็อคไฟล์ไม่ให้เจ้าของเครื่องใช้งานได้ เพื่อเรียกค่าไถในการปลดล็อคไฟล์นั้น ๆ

๑๑. Cryptojacking แฝงตัวมาจากเว็บหรือโปรแกรมที่หลีกเลี่ยงลิขสิทธิ์ ตัวโปรแกรมจะทำการขุดเหรียญ Crytocurrency โดยจะใช้ CPU และ GPU ของเป้าหมายในการทำงาน และสร้างรายได้คืนไปให้ผู้ไม่ประสงค์ดี Cybersecurity ในชีวิตประจำวัน

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ควรแยก User ของแต่ละบุคคล

๒. ควร Logout เมื่อไม่ใช้งานคอมพิวเตอร์

๓. ควรติดตั้ง Anti-Malware และ Update สม่ำเสมอ

๔. Update ระบบปฏิบัติการสม่ำเสมอ

๕. โปรแกรมต่าง ๆ ในเครื่อง ควร Update อย่างสม่ำเสมอ

๖. ไม่ควรจด Password และติด Password ไว้ที่จอ

๗. มีการใช้ Password ที่ดี และไม่ควรบอก Password แก่ผู้อื่น

การใช้ Password ที่ดี คือ

๑. มีความซับซ้อน เช่น ตัวอักษรเล็ก ใหญ่ ตัวเลข และอักขระพิเศษ

๒. ความยาวอย่างน้อย ๘ อักษร (ในอนาคตความยาวอย่างน้อย ๑๒-๑๘ อักษร)

๓. ควรเลี่ยงการใช้ Common password หรือ Default password หรือคาดเดาง่าย เช่น ๑๒๓๔๕๖, ๑๑๑๑๑๑, วดป.เกิด

๔. เปลี่ยน Password อย่างสม่ำเสมอ

๕. ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ

๖. ไม่บอก Password แก่ผู้อื่น

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัยในการใช้ E-mail

๑. ไม่เปิด E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน

๒. ไม่ควรเปิดไฟล์แนบจาก E-mail ที่น่าสงสัย

๓. ไม่คลิก Link ใน E-mail โดยไม่มีการตรวจเช็ค

๔. เรื่องที่มีความสำคัญทางธุรกรรม ให้เช็คผ่านช่องทางอื่น ๆ เพิ่มเติม Website

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางไม่แน่ชัด

๒. ไม่บันทึก Password บน Browser

๓. เว็บไซต์สำหรับทำธุรกรรมที่สำคัญ ต้องมี SSL (เป็นรูปกุญแจ การเข้ารหัสระหว่างต้นทางและปลายทาง) และใช้งานผ่าน HTTPS เท่านั้น

๔. ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งาน เช่น Google chrome

๕. Update Version Browser อย่างสม่ำเสมอ

๖. ในกรณีใช้งานเครื่องคอมพิวเตอร์ที่ไม่ใช่ของตนเอง ให้ใช้งาน Browser ในโหมด Safe Web Browsing

๗. ติดตั้ง Anti-Malware และ Update สม่ำเสมอ

Messaging สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่ควรบันทึก Password ไว้ที่โปรแกรม

๒. กรณีไม่ใช่คอมพิวเตอร์ส่วนตัว ไม่ควรบันทึกไฟล์ต่าง ๆ ไว้บนเครื่อง

๓. Update โปรแกรมอย่างสม่ำเสมอ

๔. ไม่กด Link หรือไฟล์แปลกๆ

Fake News ปัจจุบันข่าวปลอมถูกแพร่หลายเป็นอย่างมาก สามารถทำให้เกิดความเสียหายเป็นวงกว้างได้ โดยเฉพาะ ข่าวที่เผยแพร่ทาง Social วิธีสังเกต Fake News มีดังนี้

๑. มีการพาดหัวเกินจริง

๒. ระบุที่มาของข่าวไม่ได้

๓. ไม่ระบุวันที่ และเวลาที่เกิดเหตุการณ์

๔. สำนวนการเขียนออกแนวโฆษณา

Conference สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ใช้สถานที่เหมาะสมกับการ Conference

๒. ควรมีแต่ผู้ที่เกี่ยวข้องในการประชุม

๓. แชร์เอกสารต่าง ๆ อย่างระมัดระวัง

๔. ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน

๕. มีการ Update โปรแกรมอย่างสม่ำเสมอ

Cloud Storage

๑. แยก User ในการใช้งานของแต่ละบุคคล

๒. กำหนดผู้เข้าถึงไฟล์เฉพาะผู้เกี่ยวข้อง

๓. มีการตั้ง Password ที่ดี

Free wifi

๑. ไม่ควรใช้ Wifi ที่เปิดให้ใช้งานแบบไม่มีรหัสผ่าน

๒. หลีกเลี่ยงการใช้งาน Wifi ที่ไม่รู้ที่มา

ประโยชน์ที่ได้รับ :

๑. ทราบถึงภัยคุกคามและป้องกันการก่อเหตุทางโลกไซเบอร์ที่เกิดขึ้นในปัจจุบัน

๒. รู้เท่าทันต่อยุคสมัยที่มีการเปลี่ยนแปลงไป

๓. รู้จักแนวทางการป้องกันไม่ให้หลงเชื่อ และหรือส่งข้อมูลส่วนตัวไปยังปลายทางที่ไม่มีความน่าเชื่อถือ

๔. รู้จักแก้ไขปัญหาได้อย่างถูกต้อง

๕. เกิดความตระหนักถึงความเสี่ยงจากการใช้งานข้อมูลส่วนบุคคล

๖. นำความรู้ไปประยุกต์ใช้ในการทำงานได้ และนำมาปรับใช้กับงานที่ได้รับมอบหมายให้มีความมั่นคงและปลอดภัยมากยิ่งขึ้น