สรุปบทเรียนออนไลน์ของสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล(TDGA)
หลักสูตร การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ Cybersecurity Awareness

โดย นายขจรยศ สมสาย ตำแหน่ง เจ้าพนักงานการเกษตรอาวุโส
สถานีพัฒนาที่ดินร้อยเอ็ด สำนักงานพัฒนาที่ดินเขต ๔

หัวข้อการเรียนรู้

๑. CyberSecuity คืออะไร
๒. ความรู้พื้นฐานของ CyberSecuity
๓. รูปแบบภัยคุกคาม CyberSecurity
๔. ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

๑. CyberSecurity หรือ ความมั่นคงปลอดภัยทางไซเบอร์ คือการนำเครื่องมือทางด้านเทคโนโลยี และกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์ เครือข่าย, โครงสร้างพื้นฐานทางสารสนเทศ, ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากบุคคลที่สามโดยไม่ได้รับอนุญาตในปัจจุบันหน่วยงานภาครัฐ และภาคเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมายในการโจมตีมีความหลากกลายยิ่งขึ้น รวมถึงรูปแบบของการโจมตีทางด้านไซเบอร์มีความหลากหลายมากยิ่งขั้น และสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้นเรื่อยๆ

๒. ความรู้พื้นฐานของ CyberSecurity

พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์ : CIA

Confidentiaty : A หรือ การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ เช่น ข้อมูลส่วนเงินเดือนของพนักงานในบริษัท เบอร์โทรของพนักงานในบริษัท

Integrity : I หรือ การรักษาความถูกต้องของข้อมูล คือ การที่ระบุสิทธิของการแก้ไข และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น ข้อมูลธนาคารด้านการเงิน ข้อมูลที่อยู่ระบบคอมพิวเตอร์

Availability : A ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล เช่น ข้อมูลของธนาคารด้านการเงิน ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

๓. รูปแบบภัยคุกคามของ CyberSecurity

-Malware	-web-based attack
-spam	-DDos
-Data breach	-Insider threat
-Botnets	-Ransomware
-Cryptojacking	

๔. ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

Computer สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ควรมีการแยก User ใช้งานของแต่ละบุคคล
๒. ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์

๓. มีการ Updat Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
๔. ควรติดตั้ง Anti-Malware และมีการupdate อย่างสม่ำเสมอ
๕. มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ
๖. ไม่ควรจด Password และ ติด Password ไว้ที่หน้าจอ
๗. มีการใช้ Password ที่ดี และไม่ควรบอกPassword แก่ผู้อื่น

Password ควรหลีกเลี่ยงการใช้ common password หรือ สิ่งที่สามารถคาดเดาได้ง่าย Password123456

E-mail สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่เปิด E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน
๒. ไม่เปิดไฟล์ที่แนบมาจาก E-mail ที่น่าสงสัย
๓. ไม่คลิก Link ใน mail โดยไม่มีการตรวจเช็ค
๔. เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่างๆ

Website สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด
๒. ไม่ควรทำการบันทึก Password ต่างๆ บน Browser
๓. เว็บไซต์สำหรับทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น
๔. ควรติดตั้ง Anti-Maware และ Update อย่างสม่ำเสมอ

Messaging สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่ควรบันทึก Password ไว้ที่โปรแกรม
๒. กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัว ไม่ควรบันทึกไฟล์ต่างๆ ไว้บนเครื่อง
๓. มีความตระหนักก่อนเปิดปิด Link หรือ ไฟล์ต่างๆ ที่รับมา
๔. มีการ Updat version ของโปรแกรมอย่างสม่ำเสมอ

Fake New, Line official account, conference, cloud storge, Mobile, Internet connecting, Iot devices

สรุป การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ คือ ความปลอดภัย = ความสะดวกสบาย