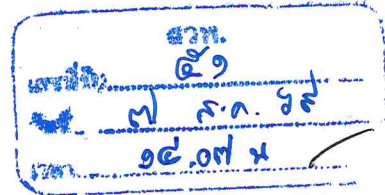




บันทึกข้อความ



ส่วนราชการ กลุ่มพัฒนาโครงสร้างพื้นฐานที่ ๑ สำนักวิศวกรรมเพื่อการพัฒนาที่ดิน โทร. ๑๒๘๓

ที่ กษ ๐๘๐๔.๐๖/๓๔๐

วันที่ ๗ สิงหาคม ๒๕๖๔

(21)

เรื่อง รายงานผลการเรียนรู้จากการพัฒนาผ่านระบบออนไลน์ (TDGA E-learning) ของสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล Thailand Digital Government Academy

เรียน ผอ. สวพ. ผ่าน ผอ.กพร.๑

ตามที่ ข้าพเจ้าได้เข้าอบรมการพัฒนาผ่านระบบออนไลน์ (TDGA E-learning) ของสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล Thailand Digital Government Academy และของสำนักงานคณะกรรมการข้าราชการพลเรือน ตามตัวชี้วัดความสำเร็จของการพัฒนาความรู้ของบุคลากรในหน่วยงาน ข้าพเจ้าได้ผ่านการอบรมหลักสูตร ดังนี้

๑. หลักสูตร Cybersecurity Awareness : การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ ของ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) โดยการอบรมผ่านสื่ออิเล็กทรอนิกส์ (TDGA e-learning)

๒. หลักสูตร เรียนรู้วิชา ปัญญาประดิษฐ์กับการทำงาน (Working with AI) ของ สำนักงานคณะกรรมการข้าราชการพลเรือน (สำนักงาน กพ.) โดยการอบรมผ่านสื่ออิเล็กทรอนิกส์ (OCSC Learning Portal)

รายละเอียดตามเอกสารแนบท้าย

จึงเรียนมาเพื่อโปรดพิจารณา

(นายธีรนนท์ ศิลาโนย)

นายช่างโยธาอาวุโส

- ทราบ

- ผบ. (สวพ.) ทบรวม

(นายจักรกฤษณ์ มีใย)

ผู้อำนวยการสำนักวิศวกรรมเพื่อการพัฒนาที่ดิน

(นายชัยวัฒน์ จะวิเสน)

ผู้อำนวยการกลุ่มพัฒนาโครงสร้างพื้นฐานที่ ๑

สรุปผลการเรียนรู้

๑. หัวข้อการพัฒนาความรู้

เรียนรู้ เรื่อง Cybersecurity Awareness : การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์

๒. เนื้อหาโดยสังเขป

หลักสูตรการสร้างความรู้ความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) ของ Thailand Digital Government Academy (TDGA) มีเนื้อหาโดยสรุป เนื้อหาของหลักสูตรมุ่งสร้างความตระหนักรู้ เสริมสร้างทักษะพื้นฐาน และปลูกฝังพฤติกรรมการใช้งานเทคโนโลยีอย่างปลอดภัย ควบคู่กับการใช้ AI อย่างมีความรับผิดชอบ เพื่อสนับสนุนการพัฒนาศักยภาพการรู้เท่าทันภัยคุกคามทางไซเบอร์ของหน่วยงานดิจิทัลที่มั่นคง ปลอดภัย และสร้างความเชื่อมั่นให้แก่ประชาชนผู้รับบริการอย่างยั่งยืน

โดยมีหัวข้อการเรียนรู้ดังนี้

๒.๑ Cybersecurity คืออะไร คือการรักษาความมั่นคงปลอดภัยทางไซเบอร์ หมายถึง การปกป้องระบบคอมพิวเตอร์ เครือข่าย อุปกรณ์ และข้อมูลจากการเข้าถึง การโจมตี หรือการเปลี่ยนแปลงที่ไม่ได้รับอนุญาต

๒.๒ ความรู้พื้นฐานของ Cybersecurity หลักการ CIA Triad ประกอบด้วย Confidentiality (ความลับ), Integrity (ความถูกต้องแม่นยำ) และ Availability (ความพร้อมใช้งานของระบบและข้อมูล) การบริหารจัดการความเสี่ยง: การประเมิน ระบุ และระงับภัยคุกคามเพื่อลดผลกระทบต่อองค์กรและบุคคล

๒.๓ รูปแบบภัยคุกคามของ Cybersecurity Phishing & Social Engineering คือการหลอกลวงผ่านอีเมล ข้อความ หรือสื่อสังคมออนไลน์เพื่อหลอกลวงเอาข้อมูลสำคัญหรือรหัสผ่าน Malware & Ransomware: มัลแวร์และมัลแวร์เรียกค่าไถ่ที่เข้ามาล็อกไฟล์หรือทำลายระบบคอมพิวเตอร์

๒.๔ ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน การตั้งรหัสผ่านที่มั่นคงปลอดภัย (Strong Password) และการเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ การเปิดใช้งานระบบยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) การระมัดระวังการคลิกลิงก์หรือดาวน์โหลดไฟล์จากแหล่งที่น่าเชื่อถือ

สาระสำคัญที่ได้เรียนรู้ จากบทเรียนนี้คือ Cybersecurity ไม่ใช่เพียงเรื่องของเทคโนโลยีหรือหน้าที่เฉพาะของฝ่ายไอทีเท่านั้น แต่เป็นความรับผิดชอบร่วมกันของทุกคนในยุคดิจิทัล หัวใจสำคัญเริ่มจากการเข้าใจความสำคัญของข้อมูล การรู้เท่าทันภัยคุกคามในรูปแบบต่างๆ เช่น Phishing และ Malware รวมถึงการสร้างพฤติกรรมความปลอดภัยในชีวิตประจำวันอย่างเป็นประจำ ไม่ว่าจะเป็นการใช้รหัสผ่านที่รัดกุม การยืนยันตัวตนแบบสองชั้น หรือการตรวจสอบความถูกต้องของข้อมูลก่อนคลิกลิงก์หรือแชร์ การมีสติและตระหนักรู้จึงเป็นเกราะป้องกันด่านแรก (Human Firewall) ที่มีประสิทธิภาพที่สุดในการลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์ทั้งระดับบุคคลและองค์กร

๓. ประโยชน์ที่ได้รับ เพิ่มความเข้าใจและความเท่าทัน: เข้าใจรูปแบบภัยคุกคามทางไซเบอร์ในยุคปัจจุบันและกลอุบายของมิจฉาชีพได้ชัดเจนยิ่งขึ้น สร้างพฤติกรรมความปลอดภัย: สามารถปรับเปลี่ยนพฤติกรรมการใช้งานอุปกรณ์ดิจิทัลและอินเทอร์เน็ตให้มีความรอบคอบและปลอดภัย ลดความเสี่ยงการถูกโจรกรรมข้อมูล: รู้วิธีการปกป้องข้อมูลส่วนบุคคล รหัสผ่าน และบัญชีใช้งานจากภัยคุกคามทางไซเบอร์มีความพร้อมในการรับมือเหตุการณ์: รู้วิธีปฏิบัติตัวเบื้องต้นเมื่อสงสัยว่าระบบหรืออุปกรณ์ถูกบุกรุกหรือติดมัลแวร์

๔. แนวคิดในการนำไปใช้ในการพัฒนางานของตนเองและหน่วยงาน

การยกระดับมาตรการความปลอดภัยข้อมูล: ร่วมปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศของหน่วยงานอย่างเคร่งครัด การเฝ้าระวังและแจ้งเตือนภัย (Incident Reporting): สังเกตความผิดปกติของระบบ เช่น อีเมลหลอกลวง (Phishing) และแจ้งทีม IT ทันที การปกป้องข้อมูลสำคัญของราชการ/องค์กร: ระวังการส่งต่อข้อมูลชั้นลับ ข้อมูลส่วนบุคคล และการสำรองข้อมูล (Backup) อย่างสม่ำเสมอ การสร้างวัฒนธรรมความปลอดภัย (Cybersecurity Culture): ถ่ายทอดความรู้และส่งเสริมให้เพื่อนร่วมงานมีความตระหนักรู้และระมัดระวังในการใช้งานระบบร่วมกัน

๕. ใบประกาศนียบัตร

๕.๑ หลักสูตร Cybersecurity Awareness : การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ ของ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) โดยการอบรมผ่านสื่ออิเล็กทรอนิกส์ (TDGA e-learning)



๕.๒ หลักสูตร เรียนรู้วิชา ปัญญาประดิษฐ์กับการทำงาน (Working with AI) ของ สำนักงานคณะกรรมการข้าราชการพลเรือน (สำนักงาน ก.พ.) โดยการอบรมผ่านสื่ออิเล็กทรอนิกส์ (OCSC Learning Portal)

