

แบบรายงานผลการพัฒนาความรู้ของข้าราชการ สำนักงานพัฒนาที่ดินเขต 12
รอบการประเมินที่ 2 / 2569 ตั้งแต่วันที่ 1 เมษายน 2566 – 30 กันยายน 2569

ประจำปีงบประมาณ พ.ศ. 2569

ชื่อ-นามสกุล นายอาดิศ อะกุลยาตา ตำแหน่ง นักวิชาการเกษตรปฏิบัติการ
ศูนย์/สพด./กลุ่ม/ฝ่าย สถานีพัฒนาที่ดินนราธิวาส
หัวข้อการพัฒนา การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness)
วิธีการพัฒนา E-Learning
วันที่พัฒนา 31 กรกฎาคม 2569 สถานที่ สถานีพัฒนาที่ดินนราธิวาส
หน่วยงานที่จัดอบรม สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัลภายใต้การดำเนินงานของสำนักงาน
พัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

สรุปสาระสำคัญ

ในยุคดิจิทัลที่เทคโนโลยีสารสนเทศเข้ามามีบทบาทสำคัญในการทำงาน การศึกษา และการใช้ชีวิตประจำวัน ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) จึงเป็นเรื่องที่ทุกคนควรให้ความสำคัญ เนื่องจากภัยคุกคามทางไซเบอร์มีการพัฒนาอย่างต่อเนื่องและส่งผลกระทบต่อบุคคล องค์กร และหน่วยงานภาครัฐ หลักสูตรการสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ของ TDGA มุ่งเน้นให้ผู้เรียนเข้าใจพื้นฐานของความมั่นคงปลอดภัยไซเบอร์ รู้จักภัยคุกคามที่พบบ่อย และสามารถนำแนวทางการป้องกันไปประยุกต์ใช้ในชีวิตประจำวันได้อย่างเหมาะสม

๑. ความรู้พื้นฐานของ Cybersecurity

Cybersecurity คือ การป้องกันระบบคอมพิวเตอร์ เครือข่าย อุปกรณ์ และข้อมูลจากการเข้าถึง การใช้งาน การเปลี่ยนแปลง หรือการทำลายโดยไม่ได้รับอนุญาต เป้าหมายสำคัญของ Cybersecurity คือการรักษาองค์ประกอบหลัก ๓ ประการ ได้แก่ ความลับของข้อมูล (Confidentiality) ความถูกต้องของข้อมูล (Integrity) และความพร้อมใช้งานของข้อมูล (Availability) หรือที่เรียกว่า CIA Triad นอกจากนี้ ผู้ใช้งานทุกคนมีบทบาทสำคัญในการรักษาความปลอดภัยของข้อมูล ไม่ใช่เพียงผู้ดูแลระบบเท่านั้น การปฏิบัติตามนโยบายด้านความปลอดภัยขององค์กร การใช้รหัสผ่านที่รัดกุม การอัปเดตระบบปฏิบัติการและซอฟต์แวร์อย่างสม่ำเสมอ รวมถึงการสำรองข้อมูล ถือเป็นพื้นฐานที่ช่วยลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์ได้อย่างมีประสิทธิภาพ

๒. รูปแบบภัยคุกคามของ Cybersecurity

ภัยคุกคามทางไซเบอร์มีหลายรูปแบบและมีความซับซ้อนมากขึ้น ตัวอย่างที่พบบ่อยได้แก่

๒.๑ Phishing คือการหลอกลวงผ่านอีเมล ข้อความ หรือเว็บไซต์ปลอม เพื่อขโมยข้อมูลส่วนบุคคล เช่น รหัสผ่าน ข้อมูลบัตรเครดิต หรือข้อมูลบัญชีธนาคาร

๒.๒ Malware คือโปรแกรมที่ถูกสร้างขึ้นเพื่อสร้างความเสียหายแก่ระบบ เช่น Virus, Worm, Trojan และ Ransomware ซึ่งอาจทำให้ข้อมูลสูญหายหรือถูกเรียกค่าไถ่

๒.๓ Social Engineering เป็นการใช้เทคนิคทางจิตวิทยาหลอกล่อให้ผู้ใช้งานเปิดเผยข้อมูลสำคัญหรือดำเนินการตามที่ถูกหลอกลวงที่ต้องการ

๒.๔ Password Attack เป็นการพยายามเดาหรือขโมยรหัสผ่านของผู้ใช้งานผ่านวิธีการต่าง ๆ เช่น Brute Force หรือ Credential Stuffing

๒.๕ การรั่วไหลของข้อมูล (Data Breach) เกิดจากการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต ซึ่งอาจส่งผลกระทบต่อความเป็นส่วนตัวและความเสียหายทางธุรกิจ

๒.๖ ผู้ใช้งานจึงควรตรวจสอบความน่าเชื่อถือของเว็บไซต์และผู้ส่งอีเมลก่อนเปิดลิงก์หรือดาวน์โหลดไฟล์แนบ รวมถึงหลีกเลี่ยงการเปิดเผยข้อมูลส่วนบุคคลแก่บุคคลที่ไม่น่าเชื่อถือ

๓. ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน

การสร้างความรู้ด้าน Cybersecurity เป็นสิ่งสำคัญ เพราะภัยคุกคามสามารถเกิดขึ้นได้กับทุกคน การป้องกันตนเองสามารถทำได้โดยเริ่มจากพฤติกรรมการใช้งานที่ปลอดภัย เช่น

๓.๑ ใช้รหัสผ่านที่มีความซับซ้อน และไม่ใช้รหัสผ่านเดียวกันในหลายระบบ

๓.๒ เปิดใช้งานการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA)

๓.๓ อัปเดตระบบปฏิบัติการ โปรแกรม และแอปพลิเคชันให้เป็นเวอร์ชันล่าสุดอยู่เสมอ

๓.๔ ไม่คลิกลิงก์หรือดาวน์โหลดไฟล์จากแหล่งที่ไม่น่าเชื่อถือ

๓.๕ สำรองข้อมูลที่สำคัญเป็นประจำ เพื่อป้องกันความเสียหายจาก Ransomware หรือเหตุการณ์ไม่คาดคิด

๓.๖ ระมัดระวังการใช้งาน Wi-Fi สาธารณะ และหลีกเลี่ยงการทำธุรกรรมทางการเงินผ่านเครือข่ายที่ไม่มีความปลอดภัย

๓.๗ ไม่เปิดเผยข้อมูลส่วนบุคคลหรือข้อมูลสำคัญบนสื่อสังคมออนไลน์เกินความจำเป็น

การมีความรู้และตระหนักถึงความเสี่ยง จะช่วยลดโอกาสในการตกเป็นเหยื่อของอาชญากรรมทางไซเบอร์ และช่วยสร้างวัฒนธรรมด้านความมั่นคงปลอดภัยให้เกิดขึ้นทั้งในระดับบุคคลและองค์กร

สรุปจากการเรียนหลักสูตร Cyber Security Awareness ของ TDGA ทำให้เข้าใจว่าความมั่นคงปลอดภัยไซเบอร์ไม่ใช่หน้าที่ของผู้เชี่ยวชาญด้านไอทีเพียงอย่างเดียว แต่เป็นความรับผิดชอบของผู้ใช้งานทุกคน การเรียนรู้พื้นฐานด้าน Cybersecurity การรู้เท่าทันรูปแบบของภัยคุกคาม และการปฏิบัติตามแนวทางการใช้งานที่ปลอดภัยในชีวิตประจำวัน จะช่วยลดความเสี่ยงจากการโจมตีทางไซเบอร์ ปกป้องข้อมูลส่วนบุคคลและข้อมูลขององค์กรได้อย่างมีประสิทธิภาพ พร้อมทั้งส่งเสริมการใช้งานเทคโนโลยีดิจิทัลอย่างปลอดภัยและยั่งยืน