

สรุปผลการพัฒนาการเรียนรู้
ผ่านระบบ TDGA e-Learning
สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล (TDGA)

ชื่อ-สกุล (ภาษาไทย) นายพัทธดนย์ ทองด้วง

กลุ่ม/ฝ่าย กลุ่มสำรวจเพื่อทำแผนที่ สำนักงานพัฒนาที่ดินเขต ๓

หลักสูตร การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์

เนื้อหา

การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) ของ TDGA มุ่งเน้นการปรับเปลี่ยนพฤติกรรมของบุคลากรให้มีภูมิคุ้มกันทางดิจิทัล เนื่องจาก "คน" (Human Factor) มักเป็นจุดเปราะบางที่สุดในระบบความปลอดภัย และตกเป็นเป้าหมายหลักของการโจมตีทางไซเบอร์ความเข้าใจการบริหารความเสี่ยงและความปลอดภัยไซเบอร์ แบ่งหัวข้อได้ดังนี้

1. ภัยคุกคามและการโจมตีทางจิตวิทยา (Social Engineering) การหลอกลวงที่อาศัยจุดอ่อนทางอารมณ์ เช่น ความโลภ ความกลัว หรือความเร่งรีบ
 - Phishing / Spear Phishing: อีเมลหรือข้อความหลอกลวงเพื่อขโมยรหัสผ่านหรือหลอกให้ติดตั้งมัลแวร์ (Spear Phishing จะเจาะจงเป้าหมายรายบุคคล)
 - Smishing & Vishing: การหลอกลวงผ่าน SMS หรือการโทรศัพท์แอบอ้างเป็นเจ้าหน้าที่
 - Baiting & Pretexting: การใช้สิ่งล่อใจ (เช่น แฟลชไดรฟ์ที่วางทิ้งไว้) หรือการสร้างเรื่องราวสมมุติเพื่อขอข้อมูลสำคัญ
 - Ransomware: มัลแวร์เรียกค่าไถ่ที่มักแพร่กระจายผ่านไฟล์แนบหรือลิงก์แปลกปลอม
2. แนวปฏิบัติความปลอดภัยในการทำงานประจำวัน (Security Best Practices)
 - การจัดการรหัสผ่าน (Password Hygiene):
 - ใช้รหัสผ่านที่ซับซ้อน (ความยาวไม่ต่ำกว่า 12 ตัวอักษร ผสมตัวพิมพ์ใหญ่ เล็ก ตัวเลข และสัญลักษณ์)

- ไม่ใช้รหัสผ่านซ้ำกันในแต่ละระบบ
- เปิดใช้งานการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA)
- การใช้งานอีเมลและอินเทอร์เน็ต
 - ตรวจสอบชื่อผู้ส่ง โดเมน และ URL ก่อนคลิกลิงก์หรือดาวน์โหลดไฟล์แนบเสมอ
 - หลีกเลี่ยงการเข้าชมเว็บไซต์ที่ไม่ปลอดภัยหรือไม่ระบุ HTTPS
- ความปลอดภัยของอุปกรณ์ (Device Security):
 - ล็อกหน้าจอทุกครั้งที่ถูกจากโต๊ะทำงาน (Lock Screen Policy)
 - อัปเดตระบบปฏิบัติการ ซอฟต์แวร์ และแอนติไวรัสให้เป็นเวอร์ชันล่าสุดสม่ำเสมอ
 - ไม่เชื่อมต่อแฟลชไดรฟ์หรืออุปกรณ์ภายนอกที่ไม่ทราบแหล่งที่มา
- การเชื่อมต่อเครือข่าย
 - หลีกเลี่ยงการทำธุรกรรมหรือส่งข้อมูลสำคัญผ่าน Wi-Fi สาธารณะ
 - ใช้งาน VPN ขององค์กรเมื่อต้องทำงานนอกสถานที่ (Work from Anywhere)
- 3. การคุ้มครองข้อมูลสำคัญและข้อมูลส่วนบุคคล
 - Data Classification: แยกแยะระดับชั้นความลับของข้อมูล (ข้อมูลเปิดเผยได้, ข้อมูลภายใน, ข้อมูลลับ, ข้อมูลลับที่สุด)
 - Clean Desk & Clean Screen: ไม่วางเอกสารสำคัญทิ้งไว้บนโต๊ะ และไม่เปิดหน้าจอค้างไว้ในที่สาธารณะ
 - Data Privacy (PDPA Awareness): ตระหนักถึงความรับผิดชอบในการจัดเก็บ ใช้งาน และส่งต่อข้อมูลส่วนบุคคลตามกฎหมาย ไม่ส่งต่อข้อมูลหลุดสู่สาธารณะ
- 4. ขั้นตอนการรับมือและรายงานเหตุผิดปกติ (Incident Reporting)
 - รู้จุดผิดปกติ: สังเกตอาการเครื่องช้าผิดปกติ หน้าต่าง Pop-up แปลกๆ หรือไฟล์ถูกเข้ารหัส
 - ระบุความเสียหายเบื้องต้น: ตัดการเชื่อมต่ออินเทอร์เน็ต (ถอดสาย LAN / ปิด Wi-Fi) ทันที
 - แจ้งเตือนทันที: รายงานเหตุการณ์ต่อทีม IT Support, เจ้าหน้าที่ความปลอดภัยไซเบอร์ หรือผู้บังคับบัญชาตามช่องทางที่องค์กรกำหนด ห้ามพยายามแก้ไขเองหากไม่มั่นใจ

การสร้างวัฒนธรรมตระหนักรู้ไม่ใช่แค่การจัดอบรมเพียงครั้งเดียว แต่เป็นการปลูกฝัง วัฒนธรรมความปลอดภัย (Cybersecurity Culture) เพื่อให้บุคลากรทุกคนทำหน้าที่เป็น "Human Firewall" ป้องกันองค์กรจากภัยคุกคามในทุกขั้นตอนการทำงาน

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

พิทรदनย์ กองด้วง

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน
การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์
(Cybersecurity Awareness)

จำนวนชั่วโมงการเรียนรู้ 1:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 6 สิงหาคม 2569

A. H.

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล



76ddc836

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
Digital Government Development Agency (Public
Organization) (DGA)
Date: 2024-08-06T13:49:55.224+07:00