หัวข้อการพัฒนา :
ความมั่นคงปลอดภัยทางไซเบอร์กับภัยคุกคามทางดิจิทัล (Cyber Security and Digital Awareness)

สรุปสาระสำคัญ

ความมั่นคงปลอดภัยทางไซเบอร์กับภัยคุกคามทางดิจิทัล (Cyber Security and Digital Awareness)

ความมั่นคงปลอดภัยทางไซเบอร์กับภัยคุกคามทางดิจิทัล(Cyber Security and Digital Awareness) เป็นหนึ่งในหลักสูตรการพัฒนาทักษะดิจิทัลข้าราชการและบุคลากรภาครัฐ (Digital Literacy) ของสำนักงาน ก.พ. มีเป้าหมายเพื่อให้ข้าราชการรู้เท่าทันภัยเงียบในโลกออนไลน์ และปกป้องข้อมูลของทางราชการไม่ให้รั่วไหล



1. ภัยคุกคามทางไซเบอร์ยอดฮิต (Digital Threats)

สิ่งที่เป็นความเสี่ยงสูงสุดของหน่วยงานรัฐ มักเกิดจากความไม่รู้หรือความประมาทของบุคคล (Human Error) เป็นหลัก

- Phishing (การตกเบ็ด/ตกทองออนไลน์): การส่งอีเมล ลิงก์ หรือ SMS ปลอมที่หน้าตาเหมือนของจริง (เช่น เลียนแบบหน้าเว็บธนาคาร หรือระบบสารบรรณกลาง) เพื่อหลอกให้เรากรอกรหัสผ่าน (Password) หรือเลขบัตรประชาชน

- Malware (ซอฟต์แวร์ประสงค์ร้าย): ย่อมาจาก Malicious Software มีหลายประเภท เช่น:

- Ransomware (มัลแวร์เรียกค่าไถ่): เข้ามาล็อกไฟล์ข้อมูลทั้งหมดในคอมพิวเตอร์หน่วยงาน แล้วขู่ให้จ่ายเงินเพื่อปลดล็อก (อันตรายต่อข้อมูลราชการมาก)

- Trojan Horse แฝงมากับโปรแกรมฟรีหรือไฟล์แนบเพื่อเปิดทางให้แฮกเกอร์เข้ามาควบคุมเครื่อง

- Social Engineering (วิศวกรรมสังคม): ไม่ใช้เทคนิคขั้นสูง แต่ใช้ "จิตวิทยา" หลอกลวง เช่น โทรศัพท์มาอ้างเป็นเจ้าหน้าที่ตำรวจ ดีเอสไอ หรือผู้บริหารระดับสูง เพื่อหลอกให้โอนเงินหรือขอข้อมูลลับ

2. หลักการรักษาความมั่นคงปลอดภัยข้อมูล (CIA Triad)

หัวใจสำคัญของ Cyber Security ที่ข้าราชการต้องรักษาไว้ให้ได้ มี 3 ข้อ ดังนี้

- Confidentiality (การรักษาความลับ): ข้อมูลลับของราชการ/ประชาชน ต้องเข้าถึงได้เฉพาะผู้ที่มีสิทธิ์เท่านั้น (เช่น การตั้งรหัสผ่าน, การจำกัดสิทธิ์เข้าถึงเน็ตเวิร์ก)

- Integrity (การรักษาความถูกต้องครบถ้วน): ข้อมูลต้องไม่ถูกแอบแก้ไขหรือเปลี่ยนแปลงระหว่างทาง ต้องถูกต้องตรงกับความเป็นจริง

- Availability (การพร้อมใช้งาน): ระบบและข้อมูลต้องพร้อมใช้งานเสมอเมื่อต้องการ เช่น เว็บไซต์ลงทะเบียนของรัฐต้องไม่ล่มเมื่อประชาชนใช้งาน

3. แนวปฏิบัติเพื่อความปลอดภัย (Cyber Hygiene)

สิ่งที่เน้นย้ำให้บุคลากรภาครัฐปฏิบัติ เพื่อลดความเสี่ยง

- การตั้งรหัสผ่าน (Password): ต้องเดายาก (Strong Password) มีความยาวอย่างน้อย 8-12 ตัวอักษร ประกอบด้วยตัวพิมพ์ใหญ่ พิมพ์เล็ก ตัวเลข และสัญลักษณ์พิเศษ และห้ามใช้รหัสเดียวกันกับทุกระบบ

- 2FA (Two-Factor Authentication): การยืนยันตัวตนแบบ 2 ชั้น (เช่น กรอกรหัสผ่านแล้ว ต้องใส่รหัส OTP จากมือถือด้วย) ซึ่งช่วยป้องกันได้มากแม้แฮกเกอร์จะรู้รหัสผ่านเราไปแล้ว

- การอัปเดตระบบ: ต้องอัปเดตระบบปฏิบัติการ (OS) และแอนตี้ไวรัสในเครื่องคอมพิวเตอร์หลวงให้เป็นเวอร์ชันล่าสุดเสมอ เพื่ออุดช่องโหว่ (Vulnerability)

- การใช้งาน Wi-Fi: หลีกเลี่ยงการเชื่อมต่อ Wi-Fi สาธารณะที่ไม่มีรหัสผ่านในการทำงานส่งข้อมูลราชการ หากจำเป็นต้องใช้ ควรเชื่อมต่อผ่าน VPN (Virtual Private Network) ของหน่วยงาน

4. กฎหมายดิจิทัลที่ควรรู้ (Digital Laws)

ในฐานะเจ้าหน้าที่รัฐ ต้องตระหนักถึงกฎหมายสำคัญ 2 ฉบับ ดังนี้

- พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์: เน้นลงโทษผู้ที่เข้าถึงระบบ/ข้อมูลโดยมิชอบ, การแก้ไขดัดแปลงข้อมูลผู้อื่น, และการนำเข้าข้อมูลเท็จที่ส่งผลกระทบต่อความมั่นคงหรือสร้างความตื่นตระหนก

- พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA): การเก็บรวมรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของประชาชน (เช่น ชื่อ ที่อยู่ เบอร์โทร เลขบัตรประชาชน) ในระบบของรัฐ ต้องได้รับความยินยอม และมีมาตรการรักษาความปลอดภัยที่เข้มงวด ห้ามทำรั่วไหลเด็ดขาด

การนำความรู้ไปใช้ประโยชน์

1. ประโยชน์ต่อตนเอง (Personal Benefits)

- รอดพ้นจากการตกเป็นเหยื่อมิจฉาชีพ: ช่วยให้เรามี "ภูมิคุ้มกัน" รู้ทันกลโกง ไม่หลงกลคลิกลิงก์ปลอม (Phishing) ไม่โอนเงินให้แก๊งคอลเซ็นเตอร์ (Social Engineering) และไม่ถูกหลอกให้ดาวน์โหลดแอปดูดเงิน

- ปกป้องข้อมูลและทรัพย์สินส่วนตัว: รู้วิธีตั้งรหัสผ่านที่ปลอดภัย และใช้การยืนยันตัวตน 2 ชั้น (2FA) ทำให้บัญชีโซเชียลมีเดีย (Facebook, Line) และแอปพลิเคชันธนาคาร (Mobile Banking) ปลอดภัยจากการถูกแฮก

- เพิ่มทักษะความสามารถ (Digital Literacy): เป็นการอัปเกรดทักษะดิจิทัลของตัวเอง ซึ่งเป็นสมรรถนะหลักที่สำนักงาน ก.พ. ใช้ประเมินความพร้อมและสร้างความก้าวหน้าในอาชีพราชการยุคปัจจุบัน

2. ประโยชน์ต่อหน่วยงานและองค์กรภาครัฐ (Organizational Benefits)

- รักษาความลับและข้อมูลของราชการ: ป้องกันไม่ให้ข้อมูลลับ เอกสารราชการ หรือฐานข้อมูลสำคัญของหน่วยงานรั่วไหลออกไปภายนอก หรือตกไปอยู่ในมือของผู้ไม่ประสงค์ดี

- ระบบงานทำงานได้อย่างต่อเนื่อง (Business Continuity): ลดความเสี่ยงที่ระบบคอมพิวเตอร์ของหน่วยงานจะโดน "มัลแวร์เรียกค่าไถ่" (Ransomware) ล็อกไฟล์ หรือโดนยิงระบบจนล่ม ทำให้หน่วยงานสามารถเปิดให้บริการและทำงานได้อย่างไม่หยุดชะงัก

- ลดการสูญเสียทรัพยากรและงบประมาณ: การกู้คืนระบบที่ถูกแฮกหรือโดนทำลาย ข้อมูลสูญหาย มีค่าใช้จ่ายที่สูงมาก ทั้งค่าจ้างผู้เชี่ยวชาญ และเวลาที่เสียไป การมี Cyber Awareness จึงช่วยป้องกันความเสียหายตั้งแต่ต้นน้ำ ซึ่งประหยัดกว่าการตามแก้ไขภายหลัง

3. ประโยชน์ต่อประชาชนและประเทศชาติ (National & Public Benefits)

- สร้างความเชื่อมั่นให้กับประชาชน: เมื่อระบบของรัฐมีความปลอดภัย ประชาชนก็มั่นใจที่จะเข้ามาใช้บริการดิจิทัลของรัฐ (เช่น แอปทางรัฐ, ระบบพร้อมเพย์, ระบบยื่นภาษีออนไลน์) โดยไม่ต้องระแวงว่าข้อมูลส่วนตัวจะถูกขโมย

- ปฏิบัติถูกต้องตามกฎหมาย (Compliance): ช่วยให้หน่วยงานและเจ้าหน้าที่รัฐไม่ละเมิด พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) และ พ.ร.บ. ไซเบอร์ฯ ลดความเสี่ยงที่จะถูกฟ้องร้องหรือลงโทษทางกฎหมายจากการทำข้อมูลประชาชนรั่วไหล

- เสริมสร้างความมั่นคงระดับประเทศ: ในภาพรวม หากข้าราชการทุกคนมี Awareness ที่ดี จะเปรียบเสมือน "กำแพงมนุษย์" ที่ช่วยปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (CII) จากการโจมตีทางไซเบอร์ข้ามชาติได้