10-024-109 ความฉลาดทางดิจิทัล (Digital Intelligence)

# หน่วยที่ 4: การจัดการความปลอดภัยในโลกดิจิทัล

สัปดาห์ที่ 5-6 | ผู้สอน: อาจารย์คณะวิทยาการจัดการ

เมื่อชีวิตประจำวันของเราผูกติดอยู่กับอุปกรณ์ดิจิทัลและบริการออนไลน์มากขึ้น ความเข้าใจเรื่องภัยคุกคามทางไซเบอร์และวิธีป้องกันตนเองจึงเป็นทักษะที่จำเป็นสำหรับพลเมืองดิจิทัลทุกคน เอกสารนี้สรุปภัยคุกคามที่พบบ่อยและแนวทางปฏิบัติเพื่อรักษาความปลอดภัยในโลกดิจิทัล

## 4.1 ภัยคุกคามทางไซเบอร์ที่พบบ่อย

ทำความรู้จักมัลแวร์ (Malware) ไวรัสคอมพิวเตอร์ การหลอกลวงแบบฟิชชิง (Phishing) และแรนซัมแวร์ (Ransomware) ที่เข้ารหัสไฟล์เพื่อเรียกค่าไถ่ พร้อมตัวอย่างรูปแบบการหลอกลวงที่พบในชีวิตจริง เช่น อีเมลปลอม ลิงก์ปลอม และข้อความ SMS หลอกลวง ตัวอย่างที่พบบ่อยในไทยคือ SMS แอบอ้างเป็นธนาคารหรือบริษัทขนส่งหลอกให้กดลิงก์กรอกข้อมูลบัตรเครดิต หรืออีเมลปลอมจากฝ่ายไอทีองค์กรหลอกให้ติดตั้งโปรแกรมที่แท้จริงเป็นมัลแวร์ ผลกระทบอาจรุนแรงถึงขั้นสูญเสียเงินในบัญชีหรือข้อมูลส่วนตัวรั่วไหล วิธีป้องกันเบื้องต้นคือตรวจสอบชื่อผู้ส่งและโดเมนเว็บไซต์ก่อนคลิกทุกครั้ง และไม่เปิดไฟล์แนบจากผู้ส่งที่ไม่รู้จัก

## 4.2 รหัสผ่านและการยืนยันตัวตนหลายขั้นตอน

หลักการตั้งรหัสผ่านที่คาดเดายาก การใช้โปรแกรมจัดการรหัสผ่าน (Password Manager) และความสำคัญของการยืนยันตัวตนแบบหลายขั้นตอน (Multi-Factor Authentication: MFA) เพื่อเพิ่มชั้นความปลอดภัยให้บัญชีออนไลน์ รหัสผ่านที่ปลอดภัยควรมีความยาวอย่างน้อย 12 ตัวอักษร ผสมตัวพิมพ์ใหญ่-เล็ก ตัวเลข และสัญลักษณ์ และไม่ใช้รหัสเดียวกันซ้ำในหลายบริการ เพื่อลดผลกระทบหากรหัสผ่านรั่วไหลจากเว็บใดเว็บหนึ่ง (credential stuffing) การเปิดใช้ MFA เช่น รับ OTP ทาง SMS หรือแอป Authenticator จะช่วยป้องกันบัญชีได้แม้รหัสผ่านรั่วไหลไปแล้วก็ตาม

## 4.3 การปกป้องข้อมูลส่วนบุคคล

แนวทางตั้งค่าความเป็นส่วนตัวบนโซเชียลมีเดีย การจำกัดสิทธิ์การเข้าถึงข้อมูลของแอปพลิเคชัน และข้อควรระวังในการเปิดเผยข้อมูลส่วนตัวบนพื้นที่สาธารณะออนไลน์ ควรตรวจสอบและปิดสิทธิ์เข้าถึงตำแหน่งที่ตั้งหรือสมุดรายชื่อของแอปที่ไม่จำเป็นต้องใช้ ตั้งค่าโพสต์ในโซเชียลมีเดียให้เห็นเฉพาะเพื่อน และระมัดระวังการแชร์ข้อมูลอ่อนไหว เช่น เลขบัตรประชาชน ที่อยู่ หรือภาพถ่ายบัตรนักศึกษา ซึ่งอาจถูกนำไปแอบอ้างทำธุรกรรมหรือสร้างบัญชีปลอมในชื่อเรา

## 4.4 แนวทางปฏิบัติเพื่อความปลอดภัยในชีวิตดิจิทัล

ข้อปฏิบัติพื้นฐานที่ทุกคนทำได้ทันที เช่น การอัปเดตซอฟต์แวร์ให้ทันสมัย การสำรองข้อมูลสำคัญ การตรวจสอบลิงก์ก่อนคลิก และการตั้งค่าความปลอดภัยบน Wi-Fi และอุปกรณ์ส่วนตัว เช่น ตั้งค่าสำรองข้อมูลอัตโนมัติขึ้นระบบคลาวด์อย่างน้อยสัปดาห์ละครั้ง หลีกเลี่ยงการทำธุรกรรมทางการเงินผ่าน Wi-Fi สาธารณะที่ไม่มีรหัสผ่าน และเปิดใช้การอัปเดตซอฟต์แวร์อัตโนมัติเพื่อปิดช่องโหว่ความปลอดภัยที่ผู้ผลิตค้นพบและแก้ไขอยู่เสมอ

# งานมอบหมายประจำหน่วยที่ 4

งานเดียว

## บันทึกสะท้อนความเสี่ยงดิจิทัลของฉัน

สำรวจพฤติกรรมการใช้งานดิจิทัลของตนเอง (การตั้งรหัสผ่าน การตั้งค่าความเป็นส่วนตัว ประสบการณ์ภัยไซเบอร์ที่เคยเจอหรือเคยได้ยินจากคนใกล้ตัว) แล้ววิเคราะห์ช่องโหว่ พร้อมเสนอแนวทางปรับปรุง โดยอ้างอิงแนวคิดจากหน่วยที่ 4 อย่างน้อย 2 หัวข้อย่อย

**รูปแบบส่ง**

เอกสาร 1-2 หน้า (400-600 คำ)

**กำหนดส่ง**

สัปดาห์ที่ 7

**องค์ประกอบที่ต้องมี**

- พฤติกรรม/สถานการณ์ที่สำรวจ
- ช่องโหว่ความเสี่ยงที่พบ พร้อมอ้างอิงทฤษฎี
- แนวทางปรับปรุงที่นำไปใช้จริงได้
- ข้อคิดสะท้อน (reflection)

**เกณฑ์การให้คะแนน (เต็ม 100)**

| | |
|---|---|
| ความครบถ้วนของเนื้อหา | 30 |
| การเชื่อมโยงทฤษฎี | 30 |
| ความลึกของการสะท้อนคิด | 20 |
| การสื่อสาร/รูปแบบการเขียน | 20 |

งานกลุ่ม

## แผนรณรงค์ความปลอดภัยดิจิทัล

กลุ่ม 4-5 คน สำรวจความตระหนักด้านความปลอดภัยดิจิทัลของคนรอบตัวอย่างน้อย 10 คน ด้วยแบบสอบถามสั้น ๆ วิเคราะห์ปัญหาที่พบบ่อยที่สุด แล้วออกแบบแผนรณรงค์ (โปสเตอร์ คลิปสั้น หรือกิจกรรม) เพื่อแก้ปัญหานั้น

**รูปแบบส่ง**

สไลด์ 8-12 หน้า + นำเสนอ 8-10 นาที/กลุ่ม

**กำหนดส่ง**

สัปดาห์ที่ 7

**องค์ประกอบที่ต้องมี**

- ผลสำรวจพร้อมสรุปตัวเลข
- ปัญหาหลักที่เลือกแก้ พร้อมเหตุผล
- แผนรณรงค์ที่เป็นรูปธรรม พร้อมตัวอย่างสื่อ
- บทบาทของสมาชิกแต่ละคน

**เกณฑ์การให้คะแนน (เต็ม 100)**

| | |
|---|---|
| คุณภาพข้อมูลสำรวจ | 25 |
| ความคิดสร้างสรรค์ของแผนรณรงค์ | 25 |
| ความเป็นไปได้ในการนำไปใช้จริง | 25 |
| การนำเสนอและการมีส่วนร่วมของสมาชิก | 25 |