รายวิชา การประยุกต์ใช้เทคโนโลยีดิจิทัลในอาชีพ
(Application of Digital Literacy for Career)

การใช้ดิจิทัลเพื่อความมั่นคงปลอดภัย

สร้างเกราะป้องกันไซเบอร์ สู่การเป็นมืออาชีพด้านธุรกิจดิจิทัล

ผู้สอน: ครูอุดมลักษณ์ สุวรรณัง

สำหรับนักศึกษาระดับ ปวส.
สาขาเทคโนโลยีธุรกิจดิจิทัล

ทำไมผู้เชี่ยวชาญธุรกิจดิจิทัลต้องมี ‘เกราะป้องกัน’?

Cybersecurity (ความมั่นคงปลอดภัยทางไซเบอร์) คืออะไร?

1. อุปกรณ์เครือข่าย (Network Devices)
2. โครงสร้างพื้นฐานทางสารสนเทศ (IT Infrastructure)
3. ระบบหรือโปรแกรม (Systems & Applications)

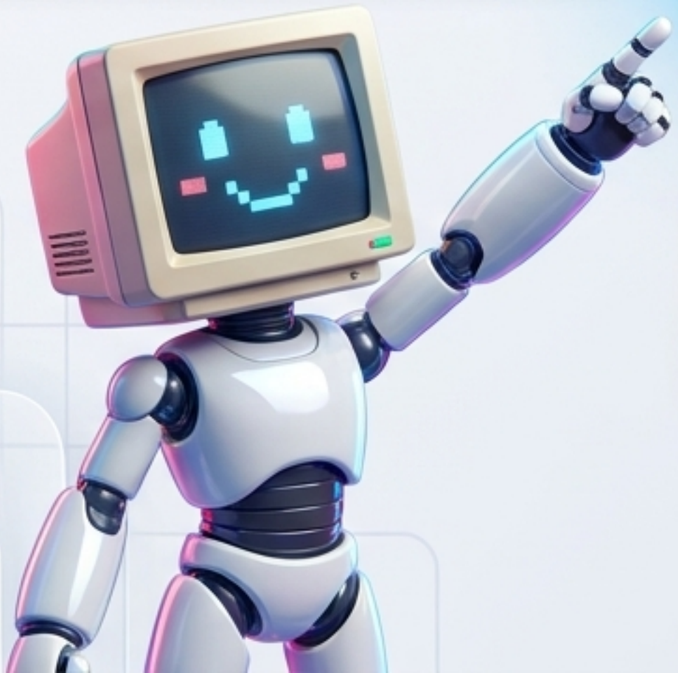
การนำเครื่องมือ เทคโนโลยี และกระบวนการมาออกแบบเพื่อ “ป้องกันและรับมือ” การโจมตีทางไซเบอร์

เป้าหมายหลัก: ป้องกันความเสียหายจากการถูกเข้าถึงโดย “บุคคลที่สามที่ไม่ได้รับอนุญาต”

หัวใจสำคัญของความมั่นคงปลอดภัย (The CIA Triad)

C : Confidentiality (ความลับ)
ข้อมูลเข้าถึงได้เฉพาะผู้ที่มีสิทธิ์เท่านั้น

ตัวอย่าง: “ข้อมูลเงินเดือน” เป็นความลับสูงสุด เข้าถึงได้เฉพาะผู้จัดการ HR



I : Integrity (ความถูกต้อง)
ข้อมูลต้องสมบูรณ์ ไม่ถูกดัดแปลงแก้ไขโดยไม่ได้รับอนุญาต

A : Availability (ความพร้อมใช้งาน)
ระบบและข้อมูลต้องพร้อมให้บริการแก่ผู้มีสิทธิ์ใช้งานได้ตลอดเวลาเมื่อต้องการ

รู้จักศัตรู: รูปแบบภัยคุกคามทางไซเบอร์ (The Threat Landscape)

ภัยคุกคามทางโปรแกรม (Malware / Virus)

- โปรแกรมไม่พึงประสงค์ที่มุ่งทำลายระบบคอมพิวเตอร์ ข้อมูล หรือเครือข่าย
- **เป้าหมาย:** โจมตี "ช่องโหว่ของระบบปฏิบัติการและซอฟต์แวร์"
- **การป้องกัน:** อัปเดตระบบ, ติดตั้ง Antivirus, ตั้งค่า Firewall

ภัยคุกคามทางจิตวิทยา (Social Engineering)

- การหลอกลวงหรือชักจูงให้เหยื่อเปิดเผยข้อมูลสำคัญด้วยความสมัครใจหรือรู้เท่าไม่ถึงการณ์
- **เป้าหมาย:** โจมตี "ความตื่นตระหนกหรือความไม่รู้ของมนุษย์"
- **การป้องกัน:** มีสติ, ตรวจสอบ URL, ไม่คลิกลิงก์แปลกปลอม

เจาะลึก: ภัยร้ายที่โจมตี "คน" (Social Engineering & Phishing)

Context

อาชญากรไซเบอร์สร้าง "เว็บไซต์เลียนแบบ"
เว็บไซต์ที่โด่งดังหรือธนาคาร
เพื่อหลอกให้ผู้ใช้กรอกรหัสผ่าน

Actionable Checklist

3 จุดสังเกตก่อนคลิก

1. **ตรวจสอบ URL เสมอ:** ตัวสะกดผิดปกติหรือไม่? (เช่น bnkk.com แทน bank.com)
2. **อย่าหลงเชื่อข้อความเร่งด่วน:** ระวังอีเมลหรือ SMS ที่ขู่ให้ปิดบัญชีหรือแจ้งว่าได้รางวัลใหญ่
3. **แหล่งที่มา:** ไม่คลิกลิงก์ที่ส่งมาจากคนแปลกหน้าหรือแหล่งที่ไม่น่าเชื่อถือ

"ระบบความปลอดภัยที่แข็งแกร่งที่สุด จะพังทลายลงหากผู้ใช้งานเป็นผู้ยื่นกุญแจให้แฮกเกอร์เสียเอง"

Digital Security: การปกป้องตัวตนและสินทรัพย์ดิจิทัล

การป้องกันตัวตนออนไลน์ ข้อมูลส่วนบุคคล และเทคโนโลยีจากอาชญากรไซเบอร์

Fingerprint Scanning
(การสแกนลายนิ้วมือ)

Facial Recognition
(การจดจำใบหน้า)

Eye Scanning
(การสแกนม่านตา)

Voice Identification
(การยืนยันตัวตนด้วยเสียง)

Data Protection
(การเข้ารหัสและปกป้องข้อมูล)

เครื่องมือยกระดับความปลอดภัย: Multi-Factor Authentication (MFA)

การยืนยันตัวตนแบบหลายปัจจัย เพื่อรับรองความปลอดภัยของผู้ใช้งาน

Step 1 / สิ่งที่รู้

Password / PIN

รหัสผ่านขั้นแรก (สิ่งที่ผู้ใช้จดจำ)

Step 2 / สิ่งที่มี

OTP & Token (ระบบ EngageLab)

รหัสแบบใช้ครั้งเดียว ผ่านช่องทาง:

- SMS Marketing / AppPush Event
- WebPush / WhatsApp Business API / Email

Step 3 / สิ่งที่เป็น

Biometrics

การอืนยันทางชีวภาพ (ใบหน้า, ลายนิ้วมือ)
ยืนยันขั้นสุดท้าย

ยืนยันทันที
ปลอดภัย 100%

ความมั่นคงปลอดภัยบนระบบคลาวด์ (Cloud Security)

อ้างอิงประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2562

1. นโยบายการจัดการบุคลากร

พัฒนาพนักงานให้มีความรู้และตระหนักถึงความปลอดภัยของข้อมูลบนคลาวด์

2. การจัดการสินทรัพย์และการเปลี่ยนแปลง

ควบคุมการเข้าถึง และติดตามดูแลการใช้บริการ Cloud Service อย่างใกล้ชิด

3. มาตรการทางกายภาพ

มีมาตรการรักษาความปลอดภัยของสินทรัพย์และอุปกรณ์ที่ใช้เชื่อมต่อ

ระบบคลาวด์สำหรับองค์กร
เช่น Google Drive, OneDrive, Dropbox

กฎหมายและมาตรฐานที่คนทำงานดิจิทัล "ต้องรู้"

พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
ปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ ให้พร้อมรับมือภัยคุกคาม

พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560
ควบคุมและเอาผิดผู้ที่ใช้คอมพิวเตอร์ในทางมิชอบ หรือสร้างความเสียหาย

PDPA (พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล)
ปกป้องความเป็นส่วนตัวของข้อมูลประชาชน ป้องกันการละเมิด

มาตรฐาน ISO 27001
ระบบบริหารจัดการความปลอดภัยของข้อมูลระดับสากล

เจาะลึก PDPA: บุคคลที่เกี่ยวข้องในระบบข้อมูล (The Data Ecosystem)

เจ้าของข้อมูลส่วนบุคคล (Data Subject)

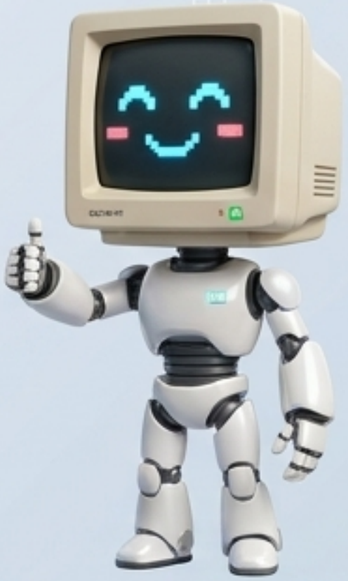
บุคคลทั่วไปที่เป็นเจ้าของข้อมูล
มีสิทธิรับรู้และควบคุมข้อมูลของตนเอง

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

องค์กร หรือบริษัท ที่มีอำนาจตัดสินใจ
ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล

ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

ผู้ที่ประมวลผลข้อมูลตามคำสั่ง
หรือในนามของผู้ควบคุมข้อมูล
(เช่น ผู้ให้บริการ Cloud, Agency)



*นอกจากนี้ยังมี DPO
(Data Protection Officer)
หรือ เจ้าหน้าที่คุ้มครองข้อมูล

PDPA: สิทธิของประชาชน และ บทลงโทษขั้นเด็ดขาด

8 สิทธิสำคัญ

1. ได้รับแจ้ง
2. เพิกถอนความยินยอม
3. แก้ไขให้ถูกต้อง
4. ลบข้อมูล
5. โอนย้ายข้อมูล
6. เข้าถึงข้อมูล
7. ห้ามประมวลผล
8. คัดค้านการประมวลผล

บทลงโทษ / The Penalties

[Criminal / อาญา]:
จำคุกไม่เกิน 1 ปี หรือ
ปรับสูงสุดไม่เกิน 1 ล้านบาท
(หรือทั้งจำทั้งปรับ)

[Civil / แพ่ง]:
จ่ายค่าสินไหมทดแทน
ไม่เกิน 2 เท่า ของค่าเสียหายจริง

[Administrative / ปกครอง]:
ปรับสูงสุดไม่เกิน 5 ล้านบาท

Digital Literacy in Action (ทักษะดิจิทัลที่องค์กรต้องการ)

DLit101 - Hardware & Software

- ติดตั้งและปรับรุ่นระบบปฏิบัติการ / โปรแกรมได้อย่างถูกต้องและปลอดภัย
- วิเคราะห์และตรวจสอบอาการผิดปกติของคอมพิวเตอร์เบื้องต้น

DLit103 - Cybersecurity Awareness

- ใช้งานอินเทอร์เน็ตอย่างปลอดภัย เลือกใช้ระบบรหัสลับ (Encryption) ที่เหมาะสม
- การกำหนดค่าไฟร์วอลล์ (Personal Firewall) และอัปเดต Antivirus สม่ำเสมอ
- ตระหนักถึงลิขสิทธิ์ ไม่ใช้งานเนื้อหาละเมิดกฎหมาย

บทสรุป: เช็คลิสต์เกราะป้องกัน สำหรับมืออาชีพด้านธุรกิจดิจิทัล

Quadrant 1: Mindset & Core

นำหลักการ CIA Triad (ความลับ/ถูกต้อง/พร้อมใช้) มาใช้ออกแบบระบบและสิทธิ์การเข้าถึงในองค์กร

Quadrant 2: Defense Mechanism

เข้าใจความต่างของ Malware และ Social Engineering เพื่ออบรมพนักงานและตั้งค่า Firewall ได้ตรงจุด

Quadrant 3: Identity & Access

บังคับใช้ MFA (SMS, Biometrics) กับทุกบัญชีสำคัญของบริษัท เพื่อปิดประตูการถูกแฮ็กรหัสผ่าน

SMS

Quadrant 4: Legal Compliance

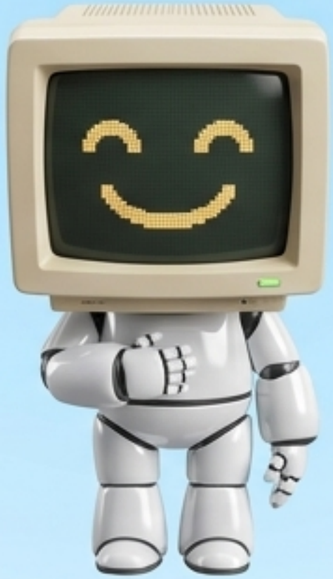
วางระบบจัดเก็บข้อมูลลูกค้าบน Cloud โดยยึดหลัก PDPA เพื่อหลีกเลี่ยงโทษปรับสูงสุด 5 ล้านบาท

PDPA

"เพราะความมั่นคงปลอดภัย คือรากฐานของธุรกิจดิจิทัลที่ยั่งยืน"

Q&A

คำถามและข้อเสนอแนะ (Q&A)



แหล่งเรียนรู้เพิ่มเติม: หลักสูตร DLit จากสำนักงาน ก.พ. / ThaiMOOC
รายวิชา การประยุกต์ใช้เทคโนโลยีดิจิทัลในอาชีพ | ครูอุดมลักษณ์ สุวรรณัง