

Cybersecurity & AI Awareness:

การใช้ AI อย่างปลอดภัยในองค์กร

ระยะเวลา 1 วัน

วัตถุประสงค์

- ลดความเสี่ยงด้านการรั่วไหลของข้อมูลจาก Human Error
- พนักงานสามารถใช้ AI ได้อย่างมั่นใจและปลอดภัย
- สร้างวัฒนธรรมด้าน AI Security Awareness ภายในองค์กร

รายละเอียดหลักสูตร

Session 1 | 09:00 – 10:30

Cybersecurity & AI Awareness Fundamentals

สร้างความเข้าใจพื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์ และปรับมุมมอง (Mindset) ให้ตระหนักว่า AI เป็นทั้งเครื่องมือเพิ่มประสิทธิภาพและแหล่งความเสี่ยงหากใช้งานไม่ถูกต้อง

เนื้อหา

- ภาพรวม Cyber Threat Landscape ในยุค AI
- Generative AI ส่งผลต่อรูปแบบภัยไซเบอร์อย่างไร
- ตัวอย่างเหตุการณ์จริงที่เกิดขึ้นในองค์กร
 - การรั่วไหลของข้อมูล (Data Leakage) จากการใช้ AI
 - การหลอกลวงแบบ AI-generated Phishing / Scam
- ประเภทข้อมูลที่ไม่ควรนำไปใช้กับ AI Tools
 - ข้อมูลส่วนบุคคล
 - ข้อมูลลูกค้า
 - ข้อมูลภายในองค์กรและข้อมูลลับ

Key Message: “AI ช่วยงานได้ แต่ถ้าไม่เข้าใจความเสี่ยง จะกลายเป็นช่องโหว่ด้านความมั่นคงปลอดภัยทันที”

Session 2 | 10:45 – 12:00

Secure Use of AI Tools & Best Practices

ให้ผู้เรียนสามารถใช้ AI Tools ได้อย่างปลอดภัย และเหมาะสมกับการทำงานประจำวันในองค์กร

เนื้อหา

- ความเสี่ยงจากการใช้งาน AI
 - Prompt Injection (อธิบายเชิงแนวคิด ไม่เชิงเทคนิค)
 - Shadow AI และความเสี่ยงจากการใช้งาน AI นอกการควบคุมองค์กร
- Best Practices สำหรับผู้ใช้งาน
 - การจัดการรหัสผ่าน (Password Hygiene)
 - การใช้ Multi-Factor Authentication (MFA)
 - การจัดการบัญชีผู้ใช้งาน AI Tools
- Prompt Hygiene
 - ตัวอย่าง Prompt ที่ปลอดภัย
 - ตัวอย่าง Prompt ที่มีความเสี่ยง

Mini Demo / Discussion

- วิเคราะห์ตัวอย่าง Prompt ที่ใช้จริงในงานประจำ
- ปรับ Prompt ให้ปลอดภัยและเหมาะสมกับองค์กร

Session 3 | 13:00 – 14:30**Data Privacy & Compliance for AI Usage**

สร้างความเข้าใจการใช้ AI ให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยไม่ต้องมีพื้นฐานด้านกฎหมาย

เนื้อหา

- ภาพรวม PDPA / GDPR ที่เกี่ยวข้องกับการใช้ AI (เฉพาะสาระสำคัญ)
- ความแตกต่างระหว่าง Personal Data และ Sensitive Data
- ความรับผิดชอบขององค์กรและพนักงาน เมื่อข้อมูลรั่วไหลผ่าน AI
- Use Case ที่พบบ่อยในองค์กร
 - การใช้ AI สรุปสัญญา
 - การใช้ AI วิเคราะห์หรือสรุป Email ลูกค้า
 - การแปลเอกสารด้วย AI

Group Discussion

- วิเคราะห์สถานการณ์ตัวอย่าง
- ถกประเด็นว่า “กรณีนี้เข้าข่ายละเมิด PDPA หรือไม่”

Session 4 | 14:45 – 16:00**Hands-on Simulation & Practical Workshop**

เปลี่ยนความรู้เป็นพฤติกรรมการใช้งาน AI ที่ถูกต้องและปลอดภัยในชีวิตการทำงานจริง

กิจกรรม**1. Phishing Simulation**

- ตัวอย่าง Email และ Chat Scam ที่สร้างโดย AI
- เทคนิคการสังเกต Phishing และ Social Engineering ยุคใหม่

2. AI Prompt Safety Workshop

- ปรับ Prompt จากรูปแบบที่มีความเสี่ยง ให้เป็น Prompt ที่ปลอดภัย
- Template Prompt สำหรับการใช้งานในองค์กร
- Checklist สำหรับการใช้ AI ในงานประจำ

Wrap-up

- AI Safe Use Checklist สำหรับผู้ใช้งาน
- บทบาทของพนักงานในการลดความเสี่ยงด้าน Cybersecurity และ AI Risk

หลักสูตรนี้เหมาะกับ

- พนักงานทั่วไป / หัวหน้างาน / ผู้จัดการ / หน่วยงานสนับสนุน