

กรมพัฒนาที่ดิน
กระทรวงเกษตรและสหกรณ์

สรุปผลการพัฒนาความรู้ วิชา ความมั่นคงปลอดภัยทางไซเบอร์ กับภัยคุกคามทางดิจิทัล (Cyber Security and Digital Awareness)

“รู้เท่าทัน ป้องกันได้
ปลอดภัยในโลกดิจิทัล”

จัดทำโดย
นายยรรยง ไพรีคำ
นิติกร
กลุ่มวินัย กองการเจ้าหน้าที่
กรมพัฒนาที่ดิน
กันยายน 2569

บรรยายโดย พล.อ.ต.อมร ช่มไชย



1

ความหมายและความสำคัญ



Cyber Security

การป้องกันระบบคอมพิวเตอร์
และข้อมูลจากการถูกเจาะหรือทำลาย



Digital Awareness

การมีความตระหนักรู้และเข้าใจความเสี่ยง
ในโลกออนไลน์ เพื่อรับมือกับกลโกงได้ทัน



ความสำคัญ

ช่วยลดความเสียหายต่อทรัพย์สิน
และข้อมูลส่วนตัว เนื่องจากเราใช้ชีวิต
บนอินเทอร์เน็ตมากขึ้น



โลกออนไลน์
สะดวก แต่ก็มีความเสี่ยง
เราต้องพร้อมรับมือ

2

ภัยคุกคามทางดิจิทัลที่พบบ่อย



Phishing

การส่งลิงก์ปลอมหรืออีเมลหลอกลวง
เพื่อขโมยรหัสผ่าน



Malware

ซอฟต์แวร์อันตรายที่เข้ามาทำลายระบบ
หรือขโมยข้อมูล



Ransomware

มัลแวร์เรียกค่าไถ่โดยการล็อกไฟล์
ในเครื่องคอมพิวเตอร์



อย่าคลิกลิงก์
อย่าเปิดไฟล์แปลกปลอม
ตรวจสอบก่อนเสมอ



3

วิธีป้องกันเบื้องต้น



อัปเดตระบบ

อัปเดตซอฟต์แวร์และแอปพลิเคชัน
ให้เป็นเวอร์ชันล่าสุดเสมอ



รหัสผ่านปลอดภัย

ใช้รหัสผ่านที่เดายาก
และเปลี่ยนบ่อยๆ



ไม่คลิกและแตะ

ตรวจสอบที่อยู่เว็บไซต์หรือผู้ส่ง
ทุกครั้งก่อนกดลิงก์



“เช็กก่อนคลิก
ปลอดภัยกว่า
เสมอ”

4

ด้านบุคลากร (People)

จุดอ่อนและแนวป้องกันที่สำคัญที่สุด



ความผิดพลาดของมนุษย์ (Human Error)
ยังคงเป็นช่องทางหลักที่แฮกเกอร์ใช้โจมตี



Cybersecurity Awareness Training

- อบรมพนักงานอย่างสม่ำเสมอ
- ให้เท่าทันภัยยุคใหม่ (อีเมลหลอกลวง, AI ปลอมเสียง/ภาพ หรือ Deepfake)



Phishing Simulation

- จำลองอีเมลหลอกลวงภายในองค์กร
- ทดสอบความรู้และสร้างความตื่นตัว



Clear IT Policies

- กำหนดแนวทางปฏิบัติที่ชัดเจน เช่น นโยบายการใช้อุปกรณ์ส่วนตัวทำงาน (BYOD) หรือ นโยบายการตั้งรหัสผ่าน



“คนมีสติ
คือเกราะป้องกัน
ที่ดีที่สุด”

5

ด้านระบบและเทคโนโลยี (Process & Technology)



Zero Trust Architecture

ไม่ไว้วางใจใครเลย และต้องตรวจสอบเสมอ
จำกัดสิทธิ์การเข้าถึงข้อมูลเท่าที่จำเป็น



Multi-Factor Authentication (MFA)

บังคับใช้การยืนยันตัวตนหลายชั้น
สำหรับระบบภายในและอีเมลองค์กรทั้งหมด



Patch & Endpoint Management

อัปเดตระบบปฏิบัติการ ซอฟต์แวร์ และแอปพลิเคชัน
ทุกระบบให้เป็นเวอร์ชันล่าสุด



Data Backup

- สำรองข้อมูลสำคัญ 3 ชุด บนสื่อ 2 ชนิด
และแยกเก็บนอกบริษัท (หรือบน Cloud)
อย่างน้อย 1 ชุด



“ป้องกันไว้
ดีกว่าแก้ไข
ภายหลัง”

6

ประโยชน์ที่ได้รับ



ด้านการดำเนินธุรกิจและเสถียรภาพ (Business Continuity)

- ธุรกิจไม่หยุดชะงัก ลดความเสี่ยงจากการถูกโจมตี
- ลดความสูญเสียทางการเงิน
- กู้คืนระบบได้รวดเร็ว



ด้านการปกป้องข้อมูลและทรัพย์สิน (Asset Protection)

- ข้อมูลสำคัญไม่รั่วไหล
- ป้องกันภัยจากกลโกง (Phishing / Social Engineering)



ด้านชื่อเสียงและความเชื่อมั่น (Reputation & Trust)

- สร้างความน่าเชื่อถือให้ลูกค้าและลูกค้า
- รักษาภาพลักษณ์แบรนด์



ด้านกฎหมายและโครงสร้างบุคลากร (Compliance & Culture)

- ปฏิบัติตามกฎหมาย PDPA และ พ.ร.บ. ไซเบอร์ฯ
- สร้างวัฒนธรรมองค์กรที่ปลอดภัย
เปลี่ยนพนักงานเป็น "กำแพงมนุษย์"

“ความปลอดภัยทางไซเบอร์
ไม่ใช่แค่เรื่องของเทคโนโลยี
แต่คือ **“ความรับผิดชอบ”**
ของทุกคน”



ร่วมกันสร้างองค์กร
ให้ปลอดภัยในโลกดิจิทัล

จัดทำโดย
นายบรรยง โพธิ์คำ
นิติกร
กลุ่มวินัย กองการเจ้าหน้าที่
กรมพัฒนาที่ดิน
กันยายน 2569