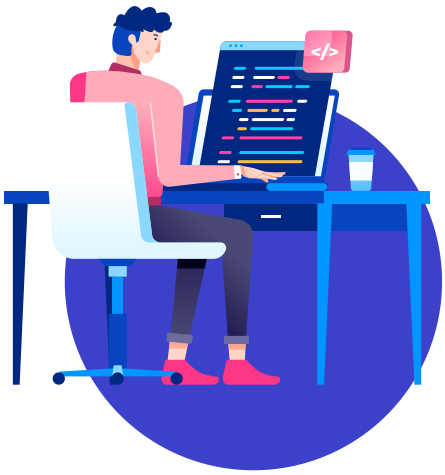
km.mof.go.th

7 วิธี รับมือภัยไซเบอร์

7 Strategies for Preventing Cybersecurity Attacks



CYBER SECURITY

คือ กระบวนการและมาตรการที่ใช้ในการปกป้องข้อมูล, ระบบคอมพิวเตอร์, และเครือข่ายจาก การถูกโจมตี, เข้าถึงโดยไม่ได้รับอนุญาต, หรือการทำลาย ความปลอดภัยทางไซเบอร์ครอบคลุมหลายด้าน

การป้องกันข้อมูล (Data Protection)
ปกป้องข้อมูลส่วนบุคคลและข้อมูลสำคัญขององค์กรจากการถูกขโมยหรือรั่วไหล

การรักษาความปลอดภัยของระบบ (System Security)
ปกป้องข้อมูลส่วนบุคคลและข้อมูลสำคัญขององค์กรจากการถูกขโมยหรือรั่วไหล

การจัดการความเสี่ยง (Risk Management)
ประเมินและจัดการความเสี่ยงที่อาจเกิดขึ้นจากภัยคุกคามทางไซเบอร์

การควบคุมการเข้าถึง (Access Control)
กำหนดว่าใครสามารถเข้าถึงข้อมูลหรือระบบใดได้บ้าง

7 วิธี รับมือภัยไซเบอร์

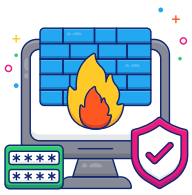
1 อัปเดต Software อย่างสม่ำเสมอ
โปรแกรมอาจมีช่องโหว่หรือถูกค้นพบช่องโหว่โดยผู้ผลิตและพัฒนา จึงมีการอัปเดตโปรแกรมออกมา ทำให้โปรแกรมสามารถปิดช่องโหว่ดังกล่าวได้

2 ใช้งานโปรแกรม Antivirus
ที่ได้รับการอัปเดตอย่างสม่ำเสมอ เพราะเวอร์ชันเดิมอาจไม่รู้จักกับ Malware ใหม่ ๆ

3 สร้างรหัสผ่านที่คาดเดาได้ยาก
ไม่ใช้ซ้ำกันทุกบัญชี ความยาวไม่น้อยกว่า 8 ตัวอักษร และทำให้ซับซ้อนด้วยเลขหรืออักขระพิเศษ

4 เปลี่ยนรหัสผ่านเริ่มต้น
เมื่อรับรหัสผ่านเริ่มต้นมา ซึ่งเราควรเปลี่ยนรหัสผ่านนั้นโดยใช้วิธีการสร้างรหัสผ่านที่คาดเดาได้ยาก

5 ใช้งานการยืนยันตัวตนแบบหลายปัจจัย (MULTI-FACTOR AUTHENTICATION)
ควรเปิดใช้งานการยืนยันตัวตนหลากหลายวิธี เช่น ใช้รหัสผ่านร่วมกับ OTP (One Time Password) โดยการรับรหัสทางโทรศัพท์ (SMS)



6 ติดตั้ง FIREWALL ในอุปกรณ์
สร้างกำแพงกั้นไม่ให้โปรแกรมหรือซอฟต์แวร์ที่ไม่ได้รับอนุญาตเข้ามาหรือทำงานในอุปกรณ์ของเรา

7 คิดก่อนเปิด (BE SUSPICIOUS OF UNEXPECTED EMAILS)
เมื่อได้รับ Email ควรคิดก่อนเปิดลิงก์ (Link) ที่ส่งมาด้วย เพราะอาจทำให้เราดาวน์โหลด Malware เข้ามาในเครื่องโดยไม่รู้ตัว ซึ่งรวมถึงข้อความสั้นทางโทรศัพท์ และข้อความจากโปรแกรมแชทด้วย

ที่มา : https://www.etda.or.th/th/Useful-Resource/Knowledge-Sharing/Articles/Cybersecurity-101.aspx?feed=cb66f430-5546-4dd8-b279-3827e88d154b