Cybersecurity Awarness for Everyone

ความปลอดภัยทางไซเบอร์สำหรับทุกคน

สรุปและเรียบเรียงโดย
นางวิมลภัทร์ งามจรัสวาณิชย์
นักสำรวจดินชำนาญการพิเศษ กลุ่มวางแผนการใช้ที่ดิน สำนักงานพัฒนาที่ดินเขต 3
กุมภาพันธ์ 2569

Cybersecurity : เป็นเรื่องใกล้ตัวมาก ต่อให้เราจะทำให้มันแข็งแรงมากแค่ไหน มันก็แข็งแรงได้เท่ากับจุดที่อ่อนแอที่สุดเท่านั้นเอง (จุดที่อ่อนแอที่สุดจะโดนโจมตีก่อน) มนุษย์เป็นสิ่งที่อ่อนแอที่สุด เราจึงต้องสร้างความตระหนักด้าน Cybersecurity ให้รู้เท่าทันกับภัยคุกคามต่างๆ อยู่เสมอ ใครๆ ก็ตกเป็นเหยื่อได้

Social Engineering : ปฏิบัติการทางจิตวิทยาแขนงหนึ่ง ที่ใช้เทคนิคในการชักจูงล่อลวงโดยอาศัยช่องโหว่ จากพฤติกรรมของผู้ใช้ เช่น แก๊ง Call Center

1. ปลอมเป็นหน่วยงานรัฐธนาคารหรือบุคคลที่ดูน่าเชื่อถือเป็นต้นเพื่อหลอกให้ทำธุรกรรม
2. ใช้คำพูดหลอกล่อให้รางวัลหรือข่มขู่เพื่อให้เหยื่อคล้อยตาม
3. ขอข้อมูลลับและข้อมูลส่วนตัว
4. ใช้เบอร์โทรศัพท์ต่างประเทศเบอร์โทรศัพท์ส่วนตัว หรือปลอมเบอร์โทรศัพท์
5. ใช้ Deepfake ปลอมใบหน้า ในการ Video Call

Phishing : เป็นเทคนิคนึงของ Social Engineering เจอบ่อยมี 3 ส่วนคือ

1. Vishing (voice/call) พวก call center โทรมาหลอกลวง
2. E-mail เนื้อหาหว่าน ไม่เฉพาะเจาะจงมีลักษณะชี้ชวน ให้คลิกลิงค์เข้าไปกรอกข้อมูลต่างๆ ศึกษาความสนใจของเหยื่อ
3. Smishing (SMS/Chat) ส่ง SMS ปลอมให้คลิกลิงค์ต่างๆ
   มี web site ช่วยตรวจสอบได้ ชื่อ Virustotal.com ตรวจสอบได้ว่าปลอดภัยไหม

Password : ที่ควรเป็น

1. Password ควรมีความยาว ไม่ควรเอาข้อมูลส่วนตัวมาตั้งเป็น Password หรือการ Log in ผ่านโซเชียลมีเดียต่าง ๆ
2. ไม่ใช้ password เดียวกันในหลายๆ service

3. ใช้ password manager ช่วยตั้ง password ที่มีความยาว ซับซ้อน เก็บในเครื่องเราอย่างปลอดภัย มีการเข้ารหัส
4. ใช้ Multi-Factor Authentication พวก OTP

Malware : คือ Sofeware อันตราย ส่งผลต่อระบบต่างๆ ที่ควบคุมโดยคอมพิวเตอร์ มักมากับ Software เถื่อน

Online Privacy : ความเป็นส่วนตัวของข้อมูล การใช้โทรศัพท์มือถือ การใช้ app ต่างๆ ที่เก็บข้อมูลของเรา เราใช้ฟรี แต่เขาเอาข้อมูลของเราไปใช้ประโยชน์ให้เกิดมูลค่าเป็นรายได้เข้าองค์กรของเขา “Data is the new oil”

Social Media Security : ควรใช้อย่างระมัดระวัง บัญชีปลอมมีเยอะ

Mobile Security : ติดตั้ง App ผ่าน App Store หรือ Play Store เท่านั้น การชาร์ตไฟควรชาร์ตไฟผ่านอแดปเตอร์เท่านั้น

Working Remotely : พยายามไม่เชื่อมต่อกับ Wifi สาธารณะ เพราะอาจมีแฮกเกอร์ใช้งานอยู่ด้วย ถ้าจำเป็นต้องใช้ไม่ควรใส่ข้อมูลส่วนตัว หรือข้อมูลลับต่างๆ ใช้ผ่านโทรศัพท์ของเราเองปลอดภัยกว่า

Got Hacked! : ต้องทำอย่างไร

คุณต้องเตรียมพร้อมด้วยการ Backup ข้อมูลของคุณอย่างสม่ำเสมอ ถ้ารู้สึกไม่ชอบมาพากล รีบ Disconnect สายเชื่อมต่อต่างๆ หรือออกจาก Hotspot ที่กำลังเชื่อมต่ออยู่ ล้างเครื่องเพื่อกำจัดโปรแกรมและข้อมูลไม่พึงประสงค์ แล้วจึงกู้ข้อมูลจาก Backup ที่ปลอดภัย username และ Password ที่เคยใช้งานอยู่ที่เครื่องที่มีอาการผิดปกติอาจมีความเสี่ยง ให้หาเครื่องที่มั่นใจว่าปลอดภัยทำการเปลี่ยน password ของ account ดังกล่าวอย่าลืมเปลี่ยน account Share Password แบบเดียวกันด้วยเพราะเราเตือนคุณแล้วว่าอย่า reuse password จับตา statement หรือ activity lock ที่มีโอกาสเกิดขึ้นเราไม่รู้ว่าแฮกเกอร์จะเอาไปทำอะไรบ้าง ถ้าเป็นเครื่องขององค์กรให้แจ้ง it support โดยด่วน ถ้าเป็นเครื่องของคุณเองทางเลือกที่ดีที่สุดคือติดตั้งใหม่และทำให้ Security ของระบบดีขึ้นทุกวิธีที่ทำได้

สรุป

- เลือกใช้ Network 4G หรือ 5g ส่งข้อมูลผ่าน HTTPS/SSL ปิด WiFi หรือ Bluetooth เมื่อไม่ใช้งาน
- อุปกรณ์ ตั้งค่า Lock อุปกรณ์ อัพเดท OS อย่างสม่ำเสมอ ไม่ทำการ Jailbreak/Root อุปกรณ์ เก็บเครื่องอย่างปลอดภัยไม่ให้ผู้อื่นเข้าถึง
- Application ต้อง Update อย่างสม่ำเสมอ ไม่ติดตั้งซอฟต์แวร์จากแหล่งที่ไม่น่าเชื่อถือไม่ติดตั้งซอฟต์แวร์เถื่อน
- password ตั้งค่ารหัสผ่านที่แข็งแรงใช้ Password Manager เปิดใช้งาน MFA (2FA) ไม่ reuse รหัสผ่าน

- Data แยกแยะ Secret/Confidential/Public Data ตรวจสอบข้อมูลก่อนที่จะเชื่อแหล่งข้อมูลนั้นๆ คิดก่อนที่จะแชร์ข้อมูล
- เทคนิค Social engineering ตระหนักถึงความเสี่ยงที่อาจเกิดขึ้น