มหาวิทยาลัยราชภัฏนครปฐม
Nakhon Pathom Rajabhat University

ความปลอดภัยในคอมพิวเตอร์ส่วนบุคคล และสมาร์ตโฟน

เนื้อหา

1. การยืนยันตัวตนและการเข้าถึง
2. สุขอนามัยของระบบและซอฟต์แวร์
3. การตระหนักรู้เรื่องวิศวกรรมสังคม
4. การปกป้องข้อมูลและการเชื่อมต่อ
5. การจัดการอุปกรณ์พกพาเฉพาะทาง

การยืนยันตัวตนและการเข้าถึง

กระบวนการระบุและพิสูจน์ตัวตน (IA)

- **การระบุตัวตน (Identification):** คือขั้นตอนแรกที่ระบบจดจำผู้ใช้ผ่านชื่อผู้ใช้ (User ID/Username).
- **การพิสูจน์ตัวตน (Authentication):** คือการยืนยันว่าผู้ที่ขอเข้าใช้งานคือตัวจริง

ปัจจัยการพิสูจน์ตัวตน (Authentication)

สิ่งที่คุณรู้

Knowledge: รหัสผ่าน,

PIN, Passphrase

สิ่งที่คุณมี

Possession: โทเค็น, OTP,

สมาร์ทการ์ด

สิ่งที่คุณเป็น

Biometrics: ลายนิ้วมือ,

ใบหน้า, ม่านตา

สิ่งที่คุณผลิต

Traits: ลายเซ็น, เสียง,

รูปแบบการพิมพ์

การเสริมสร้างความปลอดภัยให้แข็งแกร่ง

- **Multifactor Authentication (MFA):** การใช้ 2 ปัจจัยขึ้นไปร่วมกัน (เช่น รหัสผ่าน + ลายนิ้วมือ) จะช่วยลดความเสี่ยงจากการถูกขโมยรหัสผ่านได้มาก.
- **คุณภาพของรหัสผ่าน:** รหัสที่ดีควรมีความยาว (แนะนำ 10 ตัวอักษรขึ้นไป), มีความซับซ้อน (ผสมตัวเลขและอักขระพิเศษ), และไม่ควรใช้ข้อมูลส่วนตัวที่เดาง่าย.
- **ข้อควรระวังในสมาร์ตโฟน:** หลีกเลี่ยงการใช้ PIN 4 หลักเพียงอย่างเดียวเพราะเสี่ยงต่อการถูกเจาะแบบ Brute-force ควรใช้รหัสผ่าน Alphanumeric หรือไบโอเมตริกซ์แทน

หลักการป้องกัน

สิทธิ์ขั้นต่ำ (Least Privilege)

ให้สิทธิ์เข้าถึงเท่าที่ "จำเป็น" ต่อการใช้งาน

เท่านั้น เพื่อจำกัดความเสียหาย

ล็อกหน้าจออัตโนมัติ

ตั้งค่า Inactive screen lock เพื่อป้องกัน

การเข้าถึงเมื่อไม่ได้อยู่หน้าจอ

สุขอนามัยของระบบและซอฟต์แวร์

สุขอนามัยของระบบและซอฟต์แวร์ (System and Software Hygiene) คือการรักษาสภาพแวดล้อมดิจิทัลให้ปลอดภัยสม่ำเสมอ

สุขอนามัยของระบบและซอฟต์แวร์

- การอัปเดตอย่างสม่ำเสมอ: ให้ตั้งค่าอัปเดตอัตโนมัติทั้งระบบปฏิบัติการ (OS) และแอปพลิเคชัน เพื่อปิดช่องโหว่ที่ผู้โจมตีมักใช้งาน
- การใช้ซอฟต์แวร์ป้องกันมัลแวร์: ติดตั้งแอนตี้ไวรัสที่มีระบบสแกนแบบ Real-time เพื่อดักจับมัลแวร์หรือสปายแวร์ก่อนจะเริ่มทำงานในเครื่อง
- การลดพื้นที่การโจมตี (Hardening): ให้ลบซอฟต์แวร์ที่ไม่จำเป็นและปิดบริการ (Services) ที่ไม่ได้ใช้งาน เพื่อลดช่องทางที่แฮกเกอร์จะใช้บุกรุก

สุขอนามัยของระบบและซอฟต์แวร์

- การเลือกใช้แอปพลิเคชันที่ปลอดภัย: ไม่ควรทำ Jailbreak (iOS) หรือ Root (Android) เครื่อง และต้องดาวน์โหลดแอปจากแหล่งที่น่าเชื่อถือ (Official Stores) เท่านั้น เพื่อเลี่ยงแอปที่จงใจแฝงรหัสอันตราย
- การตรวจสอบความผิดปกติ: หมั่นสแกนระบบแบบละเอียด (Full Scan) เป็นระยะ และสังเกตพฤติกรรมที่ผิดปกติของเครื่อง เช่น เครื่องทำงานช้าลงอย่างเห็นได้ชัดหรือมีหน้าต่างป๊อปอัปแปลกๆ

การตระหนักรู้เรื่องวิศวกรรมสังคม

การตระหนักรู้เรื่องวิศวกรรมสังคม (Social Engineering) เป็นส่วนสำคัญที่สุดในการป้องกันข้อมูล เพราะแฮกเกอร์มักมุ่งเป้าไปที่ "คน" ซึ่งเป็นจุดที่อ่อนแอที่สุด โดยใช้จิตวิทยาเรื่องความเชื่อใจ ความใจดี หรือความกลัวมาหลอกล่อ

การตระหนักรู้เรื่องวิศวกรรมสังคม

- การหลอกลวงผ่านข้อความ: ทั้ง Phishing (อีเมล), Smishing (SMS) และ Vishing (โทรศัพท์) ซึ่งมักปลอมตัวเป็นธนาคารหรือบุคคลที่น่าเชื่อถือเพื่อขอรหัสผ่านหรือข้อมูลส่วนตัว
- Baiting: การหลอกล่อด้วยสิ่งของ เช่น การวาง USB หรือสื่อบันทึกข้อมูลที่ติดมัลแวร์ทิ้งไว้ในที่สาธารณะเพื่อให้เหยื่อเก็บไปใช้งานกับเครื่องคอมพิวเตอร์ของตน
- การแอบดูและสะกดรอย: เช่น Shoulder Surfing (การแอบมองข้ามไหล่ขณะพิมพ์รหัสหรือ PIN) หรือ Tailgating (การแอบเดินตามหลังผู้มีสิทธิ์เข้าไปในพื้นที่หวงห้าม)
- Pretexting: การสร้างสถานการณ์สมมติที่ดูสมจริงเพื่อหลอกให้เหยื่อเผยข้อมูลลับออกมา

การตระหนักรู้เรื่องวิศวกรรมสังคม: วิธีป้องกันตัว

- มีความสงสัยอยู่เสมอ: สงสัยข้อความที่ดูเร่งด่วนผิดปกติ หรือใช้อำนาจกดดันให้เราทำตามทันที.
- อย่าคลิกหรือเปิดโดยไม่ตรวจสอบ: หลีกเลี่ยงการคลิกลิงก์หรือเปิดไฟล์แนบจากแหล่งที่ไม่รู้จักหรือไม่แน่ใจ.
- ไม่บอกข้อมูลลับ: ไม่บอกรหัสผ่าน PIN หรือข้อมูลส่วนตัวให้ใครทราบทางโทรศัพท์หรือช่องทางแชทเด็ดขาด.
- ทำลายเอกสารสำคัญ: ข้อมูลในถังขยะอาจถูกขโมยได้ (Dumpster Diving) จึงควรทำลายเอกสารที่มีข้อมูลส่วนบุคคลด้วยการย่อยก่อนทิ้ง

การปกป้องข้อมูลและการเชื่อมต่อ

การปกป้องข้อมูลและการเชื่อมต่อเป็นรากฐานสำคัญของการรักษาความปลอดภัยในอุปกรณ์ส่วนบุคคล

การปกป้องข้อมูลและการเชื่อมต่อ

การปกป้องข้อมูล (Data Protection)

- การสำรองข้อมูล (Backup): ควรสำรองข้อมูลสำคัญอย่างสม่ำเสมอ ทั้งบนระบบคลาวด์หรืออุปกรณ์เก็บข้อมูลภายนอก (Hard drive/USB) เพื่อป้องกันข้อมูลสูญหายจากมัลแวร์เรียกค่าไถ่หรืออุปกรณ์พัง.
- การเข้ารหัสข้อมูล (Encryption): เปิดใช้งานการเข้ารหัสข้อมูลในเครื่อง (Disk Encryption) เพื่อให้ข้อมูลไม่สามารถถูกอ่านได้หากไม่มีกุญแจถอดรหัส. สมาร์ตโฟนสมัยใหม่มักมีการเข้ารหัสแบบ AES มาให้ในตัวซึ่งควรเปิดใช้งานไว้.
- การลบข้อมูลระยะไกล (Remote Wipe): ตั้งค่าให้อุปกรณ์สามารถสั่งลบข้อมูลทั้งหมดได้จากระยะไกลในกรณีที่เครื่องถูกขโมยหรือสูญหาย

การปกป้องข้อมูลและการเชื่อมต่อ

การเชื่อมต่อที่ปลอดภัย (Secure Connectivity)

- Wi-Fi: หลีกเลี่ยงการใช้ Wi-Fi สาธารณะโดยไม่จำเป็น และควรใช้มาตรฐานความปลอดภัย WPA2 หรือ WPA3 แทนที่ WEP ซึ่งล้าสมัยและถูกเจาะได้ง่าย. นอกจากนี้ควรเปลี่ยนชื่อ SSID ไม่ให้ระบุถึงชื่อเจ้าของหรือองค์กรเพื่อไม่ให้เป็นเป้าหมาย.
- Bluetooth: ปิด Bluetooth ทุกครั้งเมื่อไม่ใช้งาน และตั้งค่าโหมด "ไม่ให้ค้นพบ" (Non-discoverable) เพื่อป้องกันผู้ไม่หวังดีแอบเชื่อมต่อหรือส่งมัลแวร์ผ่านการ Pairing.
- VPN (Virtual Private Network): ใช้ VPN เพื่อสร้าง "อุโมงค์" ที่มีการเข้ารหัสข้อมูลเมื่อต้องเชื่อมต่อผ่านเครือข่ายที่ไม่น่าเชื่อถือ ช่วยรักษาความลับและความถูกต้องของข้อมูลขณะรับส่ง

การจัดการอุปกรณ์พกพาเฉพาะทาง

การจัดการอุปกรณ์พกพาเฉพาะทาง (Specialized Mobile Device Management) มีความสำคัญอย่างยิ่งเนื่องจากอุปกรณ์เหล่านี้มักมีการจัดเก็บข้อมูลส่วนตัวและข้อมูลองค์กรปะปนกัน

การจัดการอุปกรณ์พกพาเฉพาะทาง

การใช้ระบบบริหารจัดการส่วนกลาง (MDM/UEM)

องค์กรและผู้ใช้งานควรใช้เครื่องมือ Mobile Device Management (MDM) หรือ Unified Endpoint Management (UEM) เพื่อควบคุมนโยบายความปลอดภัยจากระยะไกล ซึ่งช่วยในการ:

- กำหนดนโยบาย (Policy Management): บังคับใช้การตั้งค่าความปลอดภัยที่เหมือนกันในทุกอุปกรณ์
- การลงทะเบียนและจัดเก็บคลัง: ติดตามรายชื่ออุปกรณ์และเจ้าของเพื่อป้องกันอุปกรณ์ที่ไม่ได้รับอนุญาตเข้าถึงระบบ
- การจัดการซอฟต์แวร์: ควบคุมการติดตั้ง อัปเดต หรือบล็อกแอปพลิเคชันที่เป็นอันตราย

การจัดการอุปกรณ์พกพาเฉพาะทาง

การแยกส่วนข้อมูล (Containerization)

เทคนิคนี้ใช้เพื่อแบ่งแยกข้อมูลส่วนตัวออกจากข้อมูลงาน อย่างเด็ดขาด ซึ่งช่วยให้ฝ่าย IT สามารถควบคุมหรือลบข้อมูลของบริษัทได้โดยไม่กระทบต่อข้อมูลส่วนตัวของพนักงาน

การควบคุมจากระยะไกล (Remote Operations)

- การลบข้อมูลระยะไกล (Remote Wipe): เป็นนโยบายที่สำคัญที่สุด โดยต้องตั้งค่าให้อุปกรณ์สามารถสั่งลบข้อมูลทั้งหมดหรือเลือกลบเฉพาะข้อมูลองค์กรได้ทันทีเมื่อเครื่องสูญหายหรือถูกโขมย
- การล็อกระยะไกล (Remote Lock): สั่งล็อกเครื่องทันทีเพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

การจัดการอุปกรณ์พกพาเฉพาะทาง

มาตรการความปลอดภัยพื้นฐานที่เข้มงวด

- ห้าม Jailbreak หรือ Root: การข้ามระบบป้องกันของ OS จะทำให้กลไกการแยกแอป (Application Isolation) พังลง และเพิ่มความเสี่ยงจากมัลแวร์อย่างมหาศาล
- การเข้ารหัสข้อมูล (Encryption): บังคับใช้การเข้ารหัสทั้งตัวเครื่องและ SD Card (เช่น AES 256-bit) ซึ่งมักต้องใช้ร่วมกับการตั้งรหัสผ่านหรือ PIN
- ดาวน์โหลดจากแหล่งทางการเท่านั้น: จำกัดให้ติดตั้งแอปจาก Official Stores เท่านั้น เพื่อลดความเสี่ยงจากการติดตั้งแอปที่แฝงมัลแวร์ (Sideloading)

วิธีการในการใช้คอมพิวเตอร์อย่างปลอดภัย

1. รู้จักเครื่องคอมพิวเตอร์ส่วนบุคคลของตนเอง
2. การจัดการตรวจสอบปัญหาของฮาร์ดิสก์
3. การจัดเรียงฮาร์ดิสก์อย่างสม่ำเสมอ (Disk Defragmentation)
4. การวางแผนและการจัดการในการเก็บข้อมูลหรือไฟล์อย่างเป็นระบบ
5. การสำรองข้อมูลไว้ที่อุปกรณ์สำรอง (Backup Data)
6. การวางแผนในการติดตั้งหรือถอดถอนโปรแกรมคอมพิวเตอร์ รวมถึงการลบไฟล์ หรือการไปเล่นกับไฟล์ต่าง ๆ ในคอมพิวเตอร์
7. การป้องกันไวรัสคอมพิวเตอร์ มัลแวร์ และสปายแวร์
8. การรักษาคอมพิวเตอร์ให้สะอาด หรือไม่นำอาหารมารับประทานใกล้ ๆ กับคอมพิวเตอร์
9. การใส่รหัสป้องกันการเข้าเครื่องคอมพิวเตอร์อย่างชาญฉลาด
10. การเปิด-ปิดเครื่องอย่างถูกวิธี

(สมบูรณ์ สุขชัย, 2555)


Q
&
A