Cybersecurity Awareness

ปัจจุบันการโจมตีทางเครือข่ายไซเบอร์มีความรุนแรงและครอบคลุมไปเกือบทุกผ่านส่วน โดยจากข้อมูลพบว่าโดยเฉลี่ยแล้วประชาชนคนอเมริกันมากกว่า 73% ได้ประสบพบกับภัยคุกคามทางไซเบอร์และนำมาซึ่งความสูญเสียในหลายๆระดับ โดยรูปแบบการโจมตีทางไซเบอร์ในปัจจุบันมีอยู่มากมายดังแสดงในรูปข้างล่าง อาทิเช่น ransomware, work และ virus เป็นต้น

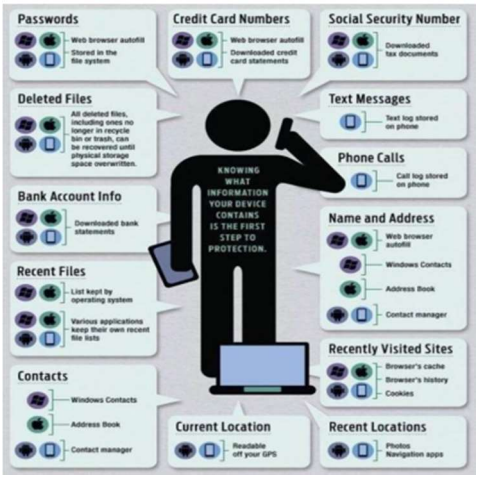
ความเสียหายจากการโจมตีทางไซเบอร์

รูปแบบของภัยคุกคามทางไซเบอร์

ในที่นี้เราจะพูดถึงแนวทางการโจมตีและแนวปฏิบัติที่ดีในการที่จะป้องกันหรือลดความเสี่ยงที่จะถูกโจมตีทางไซเบอร์โดยมีหัวข้อต่างๆดังต่อไปนี้

1. You are a target **ทำไมอุปกรณ์อิเล็กทรอนิกส์/สื่อสารของเราถึงเป็นเป้าหมาย**
    - โทรศัพท์มือถือแบบ smart phone สามารถใช้ทำธุรกรรมทางการเงินได้มากมาย
    - ใช้ระบุตัวตนของผู้ใช้
    - ผู้ไม่ประสงค์ดีที่ได้โทรศัพท์ของเราไปสามารถปลอมเป็นตัวเราเพื่อทำกิจกรรม/ธุรกรรมที่ทุจริตได้

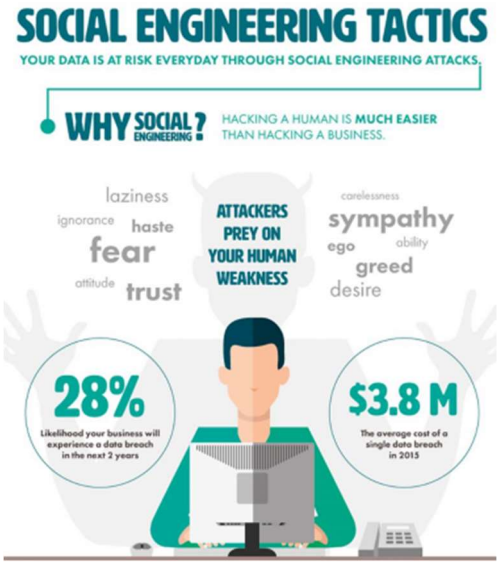
- แนวปฏิบัติ:ควรมีการเข้ารหัสโทรศัพท์มือถือไว้พร้อมทั้ง 2FA



ตัวอย่างข้อมูลที่อยู่ในโทรศัพท์มือถือของเรา

- เลขบัตรเครดิต
- Username/password
- เลขบัตรประชาชน

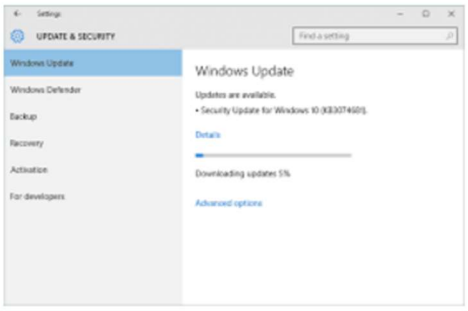
2. Social Engineering/Phishing scam การโจมตีโดยการหลอกลวง



การโจมตีด้วยวิธี Social Engineering

- อาศัยความเชื่อใจ/กลัว/โลภ ในการขอรหัสผ่าน หรือ บังคับให้เอาไฟล์สำคัญออกไปเผยแพร่
- ส่งอีเมลหรือข่าวสารปลอมให้ผู้รับหลงเชื่อและกด download ไฟล์ที่แนบมาด้วย
- แนวปฏิบัติ:ไม่กด download ไฟล์หรือกด link ที่ได้รับจากคนที่ไม่รู้จักหรือไม่แน่ใจว่าคนที่รู้จักส่งมาจริงหรือไม่

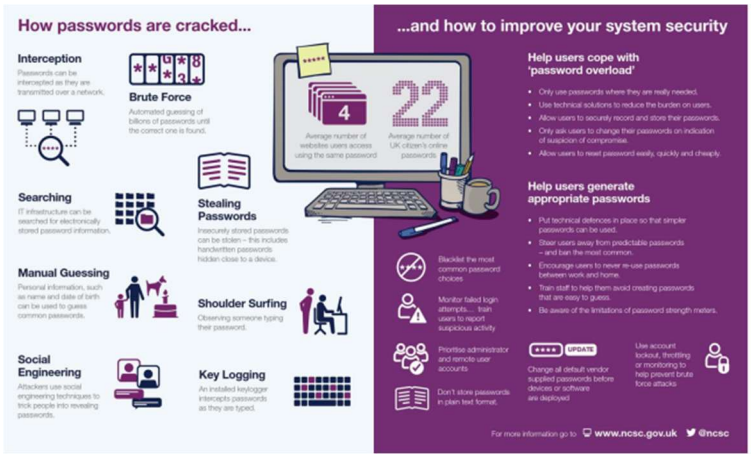
3. System security



แนวปฏิบัติ

1. หมั่น update Windows' patch
2. ติดตั้งและ update Antivirus software

4. Basic Identification การระบุตัวตน



1. การระบุตัวตนด้วยสิ่งที่เรารู้password, PIN
2. การระบุตัวตนด้วยสิ่งที่เรามี: fingerprint, face, eyes
3. แนวปฏิบัติ:ติดตั้ง 2fa เพื่อใช้สิ่งที่เรารู้และสิ่งที่เรามีในการระบุตัวตน

Google's own data proves two-factor is the best defense against most account hacks

5. วิธีการ Shopping online ให้ปลอดภัย

1. ใช้บัตรเครดิต ไม่ใช้เดบิต
2. ไม่บันทึกข้อมูลบัตรเครดิตบน browser
3. ซื้อจากร้านที่น่าเชื่อถือ (ดูจาก credit, user rating)
4. ไม่ click link ใน email ที่ดูแปลกๆ
5. ตั้ง password ในการเข้าโทรศัพท์มือถือ
6. Update ระบบ application software บ่อยๆ
7. ติดตั้ง Antivirus
8. อย่าหลงเชื่อข้อเสนอที่เกินจริง