ความปลอดภัยยุคดิจิตอล

หลักสูตรความเข้าใจดิจิทัล (Digital Literacy)

ความปลอดภัยยุคดิจิตอล

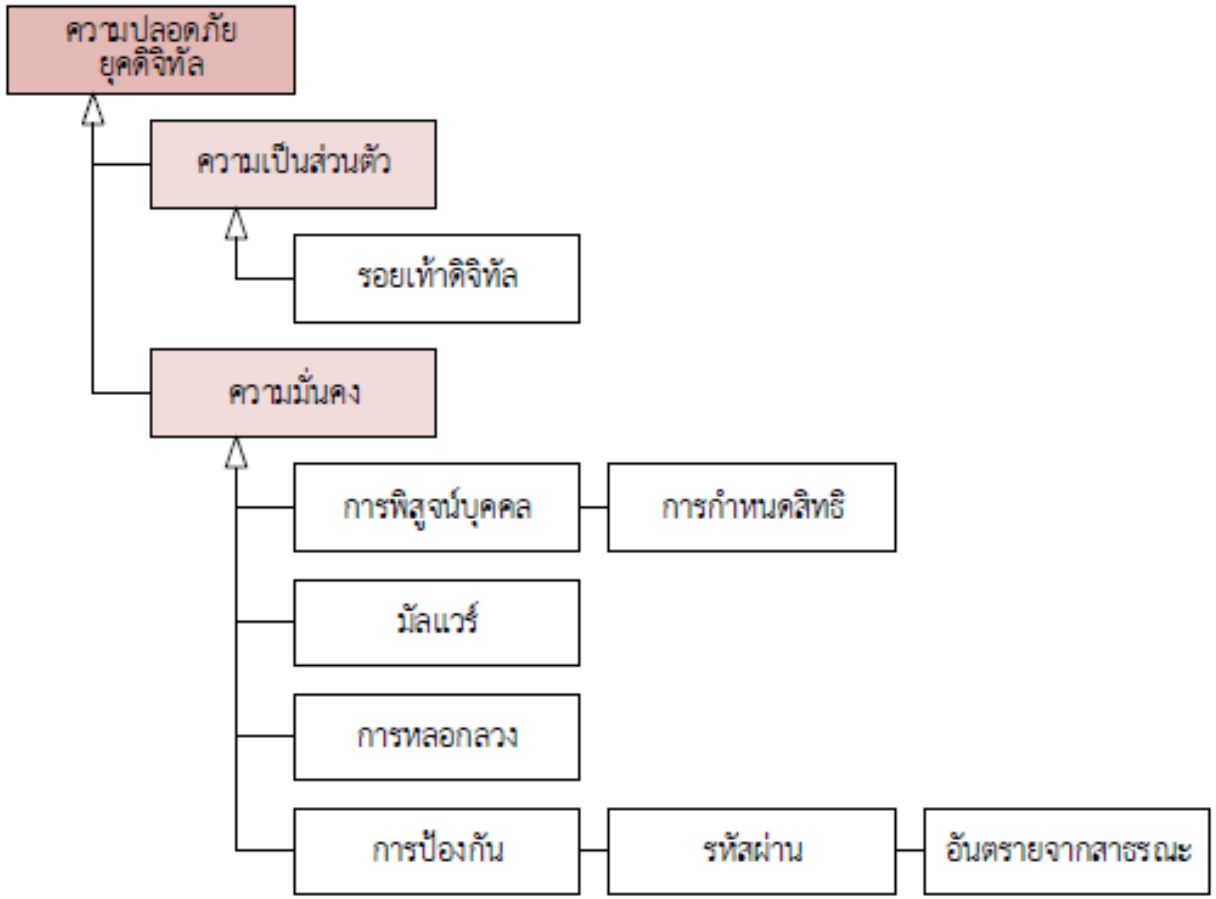
ผู้ศึกษาจำเป็นต้องเข้าใจความมั่นคง ความเป็นส่วนตัว และการทิ้งรอยเท้าดิจิทัล ในการใช้อุปกรณ์อิเล็กทรอนิกส์ในยุตดิจิทัล รวมถึงภัยในรูปแบบต่าง ๆ ทั้งในแง่วิธีการที่ได้รับการคุกคาม ผลกระทบที่เกิดขึ้น การป้องกัน การลดความเสี่ยง ต่อภัยเหล่านั้น

จุดประสงค์หลัก

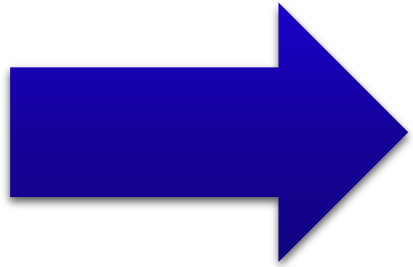
- เข้าใจความมั่นคง (Security) ความเป็นส่วนตัว (privacy) และการทิ้งรอยเท้าดิจิทัล (Digital Footprint) ไว้ในโลกออนไลน์
- เข้าใจวิธีการ และ ผลกระทบ ของภัยในรูปแบบต่าง ๆ
- เข้าใจการปฏิบัติเพื่อป้องกันและลดความเสี่ยงต่อภัยคุกคาม

ความปลอดภัยยุคดิจิตอล

โครงสร้างหัวเรื่องหลัก



ความปลอดภัยยุคดิจิตอล



Security

Privacy

จำเป็นต้องใช้งานให้เป็น

ความปลอดภัยยุคดิจิตอล

รอยเท้าดิจิทัล หรือ Digital Footprint

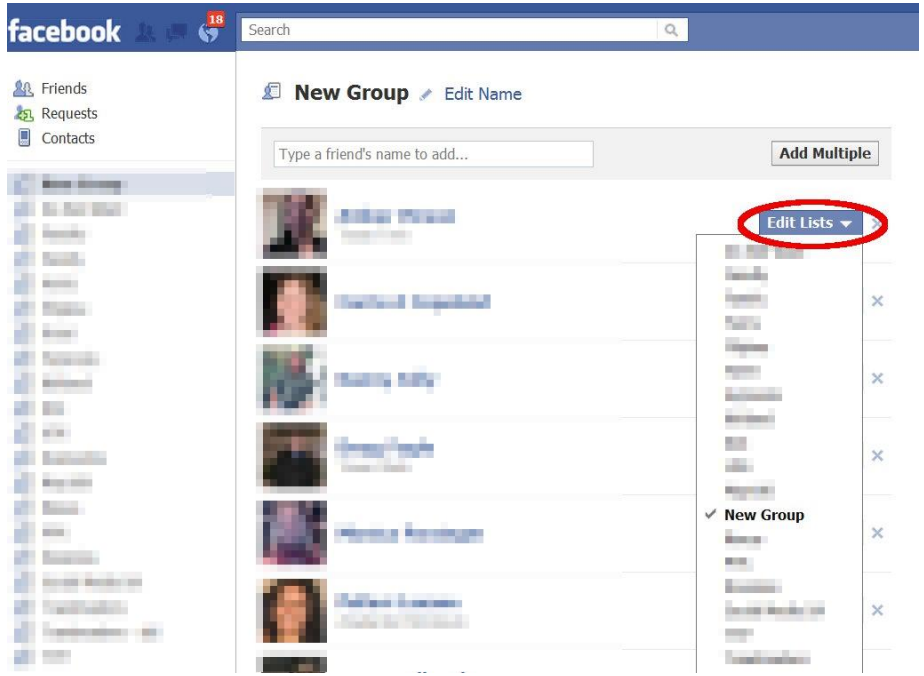
คือข้อเขียน รูปภาพ สิ่งต่าง ๆ ที่เราเขียนหรือลงไว้ใน Social Media ทั้งหลาย ไม่ว่าจะเป็น Facebook, Twitter, Instagram, Social Cam หรือช่องทางไหนก็ตาม

https://www.facebook.com/wannamdotcom/posts/695510607158112

ความปลอดภัยยุคดิจิตอล

อะไรบ้างที่เป็นข้อมูลพื้นฐานของ Digital Footprint

- ภาพหรือข้อมูลส่วนตัว เช่น หมายเลขโทรศัพท์ ที่อยู่ หมายเลขบัตรประชาชน
- การดำเนินชีวิต และ การเป็นอยู่ของเรา
- ภาพกับเพื่อน กลุ่มต่าง ๆ
- ความสัมพันธ์กับคนต่าง ๆ ยกตัวอย่างเช่น เพื่อนใน Facebook (เพื่อนร่วมงาน เจ้านาย)



ความปลอดภัยยุคดิจิตอล

หลายเหตุผลที่กระทำก่อให้เกิด Digital Footprint

- ไม่เห็นเป็นอะไร Facebook , Instagram เป็นพื้นที่ส่วนตัว
- ไม่ใช่คนดัง ไม่ใช่ดารา ไม่มีใครสนใจหรอก
- แค่อยากระบายอะไรบ้าง

ความปลอดภัยยุคดิจิตอล

อันตรายของการทิ้ง Digital Footprint

- ทดสอบค้นหาชื่อตัวเอง
- ข้อมูลมีโอกาสโดนทำสำเนาไปนับไม่ถ้วน
- อยู่ในมือผู้ไม่หวังดี
- เสียภาพพจน์ และ ภาพลักษณ์ โดยไม่อาจแก้ไขได้

ดังนั้นคิดให้ดีก่อนที่จะ Post

ความปลอดภัยยุคดิจิตอล

การพิสูจน์ตัวตน

การพิสูจน์ตัวบุคคลโดยใช้ 2 ปัจจัย
(Two-Factor Authentication)

คือการใช้ปัจจัยที่สอง ร่วมกับการล็อกอินด้วยรหัสผ่านตามปกติ ซึ่งหลังจากการล็อกอินด้วยรหัสผ่านแล้ว ระบบจะถามรหัสยืนยันจากอุปกรณ์อื่น เช่น โทรศัพท์มือถือ หรือ Token เพื่อความปลอดภัยมากขึ้น อาทิ Google 2 Factor Authentication เป็นต้น

Source :https://docs.google.com/presentation/d/10EfOYjGaatwvQ9No5Ag9CwxEfj0aNdIjLp4qe1kJM-k/htmlpresent?hl=en

ความปลอดภัยยุคดิจิตอล

การพิสูจน์ตัวตน

การพิสูจน์ตัวบุคคล โดยใช้หลายปัจจัย (Multi-Factor Authentication)

กลไกของการพิสูจน์ตัวตน (Authentication mechanisms) สามารถแบ่งออกได้เป็น 3 คุณลักษณะคือ

1. สิ่งที่คุณมี (Possession factor) เช่น กุญแจหรือเครดิตการ์ด เป็นต้น
2. สิ่งที่คุณรู้ (Knowledge factor) เช่น รหัสผ่าน (passwords) หรือการใช้พิน (PINs) เป็นต้น
3. สิ่งที่คุณเป็น (Biometric factor) เช่น ลายนิ้วมือ รูปแบบเรตินา (retinal patterns) หรือใช้รูปแบบเสียง (voice patterns) เป็นต้น

Source :https://carryrmu.wordpress.com/authentication-%E0%B8%84%E0%B8%B7%E0%B8%AD/

ความปลอดภัยยุคดิจิตอล

Multi-Factor Authentication

ความปลอดภัยยุคดิจิตอล

การกำหนดสิทธิ์ (Authorization)

หลักการสิทธิน้อยที่สุด Principle of Least Privilege สามารถใช้ปรับปรุงความปลอดภัยของระบบคอมพิวเตอร์ นี่เป็นเรื่องพื้นฐานแต่สำคัญมากที่มักถูกมองข้าม หลักการนี้ คือ ผู้ใช้ จะต้องมีระดับต่ำที่สุดของสิทธิตามความต้องการเพื่อ กระทำงานตามที่มอบหมาย

ความปลอดภัยยุคดิจิตอล

การเข้ารหัสข้อมูล

HTTPS ย่อมาจาก Hypertext Transfer Protocol Secure หรือ Hypertext Transfer Protocol Over SSL(Secure Socket Layer) เป็นการทำงานเหมือนกับ HTTP ธรรมดาแต่ทำอยู่บน SSL เพื่อให้เกิดความปลอดภัยในการส่งข้อมูลมากยิ่งขึ้น มีรูปแบบดังนี้

- การใช้งาน URL จะเข้าต้นด้วย https:// ตามด้วยชื่อของเว็ปไซต์
- ทำงานที่พอร์ต(port) 443 (มาตรฐาน)
- ส่งข้อมูลเป็นแบบ Cipher text คือ มีการเข้ารหัสข้อมูลในระหว่างการส่ง (Encryption) สามารถถูกดักจับได้ แต่อ่านข้อมูลนั้นไม่รู้เรื่อง
- มีการทำ Authentication เพื่อตรวจสอบยืนยันระบุตัวตน

ความปลอดภัยยุคดิจิตอล

การเข้ารหัสข้อมูล

WPA2 คือเทคโนโลยีการรักษาความปลอดภัยที่ปกป้องเครือข่าย Wi-Fi ของคุณโดยการเข้ารหัสการจราจรบนเครือข่าย นอกจากนี้ ยังทำให้ผู้ใช้ที่ไม่ได้รับอนุญาตเข้าถึงเครือข่ายได้ยากขึ้น

ความปลอดภัยยุคดิจิตอล

มัลแวร์ (malware – malicious software)

คือโปรแกรมที่ถูกสร้างขึ้นมาเพื่อประสงค์ร้ายต่อเครื่องคอมพิวเตอร์ และเพื่อมาล้วงข้อมูลสำคัญไปจากผู้ใช้งานคอมพิวเตอร์

http://www.xn--12cg1cxchd0a2gzc1c5d5a.net/malware/

มัลแวร์ (malware – malicious software)

Malware มีกี่ชนิด

มัลแวร์มีอยู่หลายชนิดด้วยกัน ซึ่งสามารถแบ่งออกเป็น 6 ชนิดด้วยกันคือ

1. ไวรัส (Virus) เป็นโปรแกรมที่ติดต่อจากไฟล์หนึ่งไปสู่อีกไฟล์หนึ่งได้ และสามารถส่งผ่านไฟล์ด้วยการแนบไวรัสไปกับไฟล์ที่เราส่งไปยังเครื่องคอมพิวเตอร์อีกเครื่องหนึ่งได้ โดยไวรัสจะทำการทำลายทั้งฮาร์แวร์และซอฟแวร์ในเครื่องพร้อมกับไฟล์ที่ไวรัสแฝงตัวเองเพื่อแพร่กระจายไปสู่เครื่องอื่นๆด้วย

2. เวิร์ม (Worm) สามารถที่จะแพร่ขยายตัวเองโดยที่ไม่ต้องมีโปรแกรมอื่นในการแพร่กระจายก็ได้เช่นกัน เป้าหมายของเวิร์มจะจ้องทำลายระบบเครือข่าย และขยายการแพร่กระจายไปยังคอมพิวเตอร์ตัวอื่นๆ โดยการส่งอีเมล์หรือช่องโหว่ของระบบปฏิบัติการณ์

3. โทรจัน (Trojan Horse) เป้าหมายของมัลแวร์ตัวนี้จะค่อยจ้องทำลายระบบและเปิดช่องโหว่ให้กับผู้ไม่หวังดีเข้ามาทำลายระบบและควบคุมจากระยะไกล และไม่แพร่กระจายไปยังไฟล์อื่น ๆ

4. สปายแวร์ (Spyware) จะไม่แพร่กระจายไปยังไฟล์อื่น ๆเหมือนกับโทรจัน โดยเป้าหมายของสปายแวร์นั้นจ้องที่จะรบกวนและละเมิดความเป็นส่วนตัวของผู้ใช้.

5. Hybrid Malware/Blended Threats เป็นมัลแวร์ที่อันตรายมากเพราะรวมความสามารถของ ไวรัส เวิร์ม โทรจัน สปายแวร์ ไว้ด้วยกัน

6. Phishing เป็นมัลแวร์ที่จ้องจะขโมยข้อมูลทางการเงินเช่น บัตรเครดิตหรือพวก Online bank account

http://www.xn--12cg1cxchd0a2gzc1c5d5a.net/malware/

การหลอกลวง (Scam)

เล่ห์อุบาย แผนการร้าย คำนี้หากอยู่ในวงการออนไลน์ จะใช้เรียกพฤติกรรม ที่มีเจตนาหลอกลวง ให้เสียทรัพย์ ให้เสียข้อมูล ตัวอย่างการหลอกลวงทางอินเทอร์เน็ต เช่น Email Scams Phishing Scam เป็นต้น

https://sites.google.com/site/karskaemscam02/home/ka-rs-kaem-scam

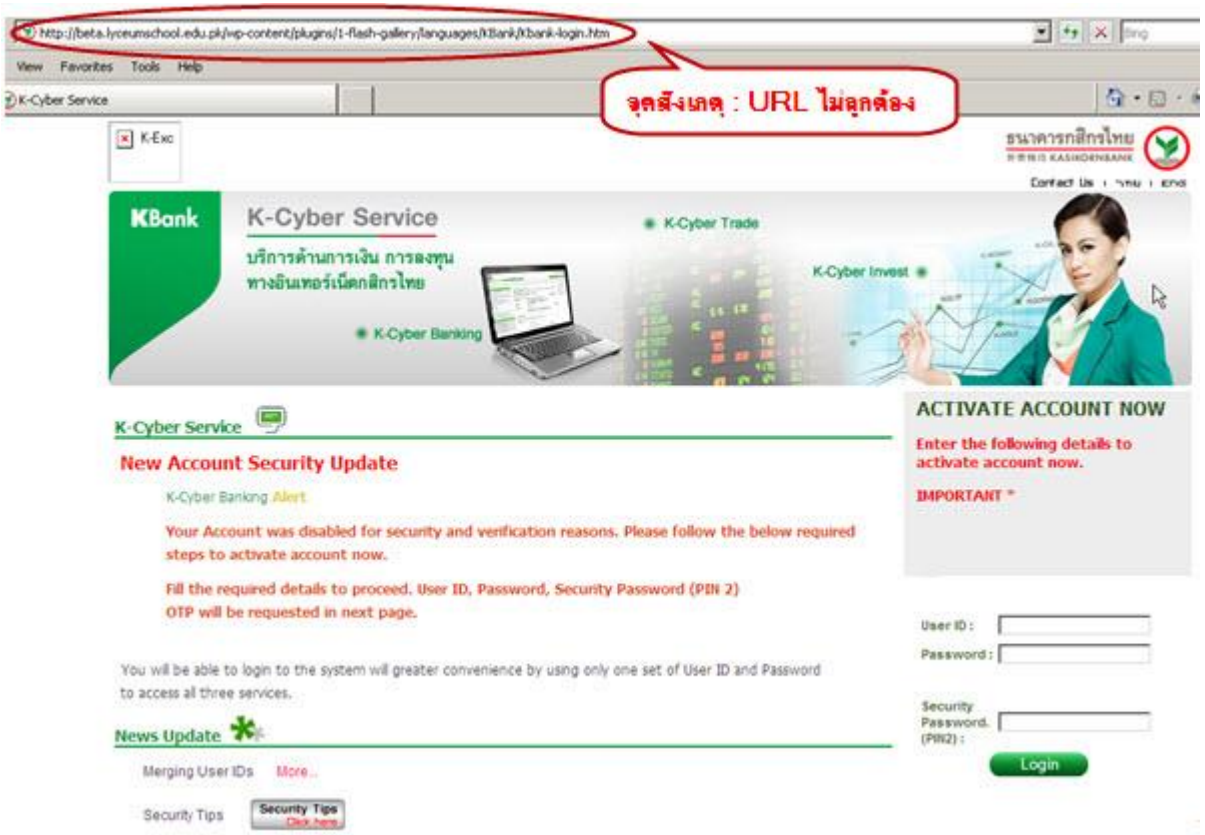
การโจมตีแบบวิศวกรรมสังคม (Social Engineering)

Phishing คือคำที่ใช้เรียกเทคนิคการหลอกลวงโดยใช้อีเมลหรือหน้าเว็บไซต์ปลอมเพื่อให้ได้มาซึ่งข้อมูล เช่น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลส่วนบุคคลอื่น ๆ เพื่อนำข้อมูลที่ได้ไปใช้ในการเข้าถึงระบบโดยไม่ได้รับอนุญาต หรือสร้างความเสียหายในด้านอื่น ๆ เช่น ด้านการเงิน เป็นต้น ในบทความนี้จะเน้นในเรื่องของ Phishing ที่มีจุดมุ่งหมายเพื่อหลอกลวงทางการเงิน เนื่องจากจะทำให้ผู้อ่านมองเห็นผลกระทบได้ง่าย

https://www.thaicert.or.th/papers/general/2012/pa2012ge007.html

ความปลอดภัยยุคดิจิตอล

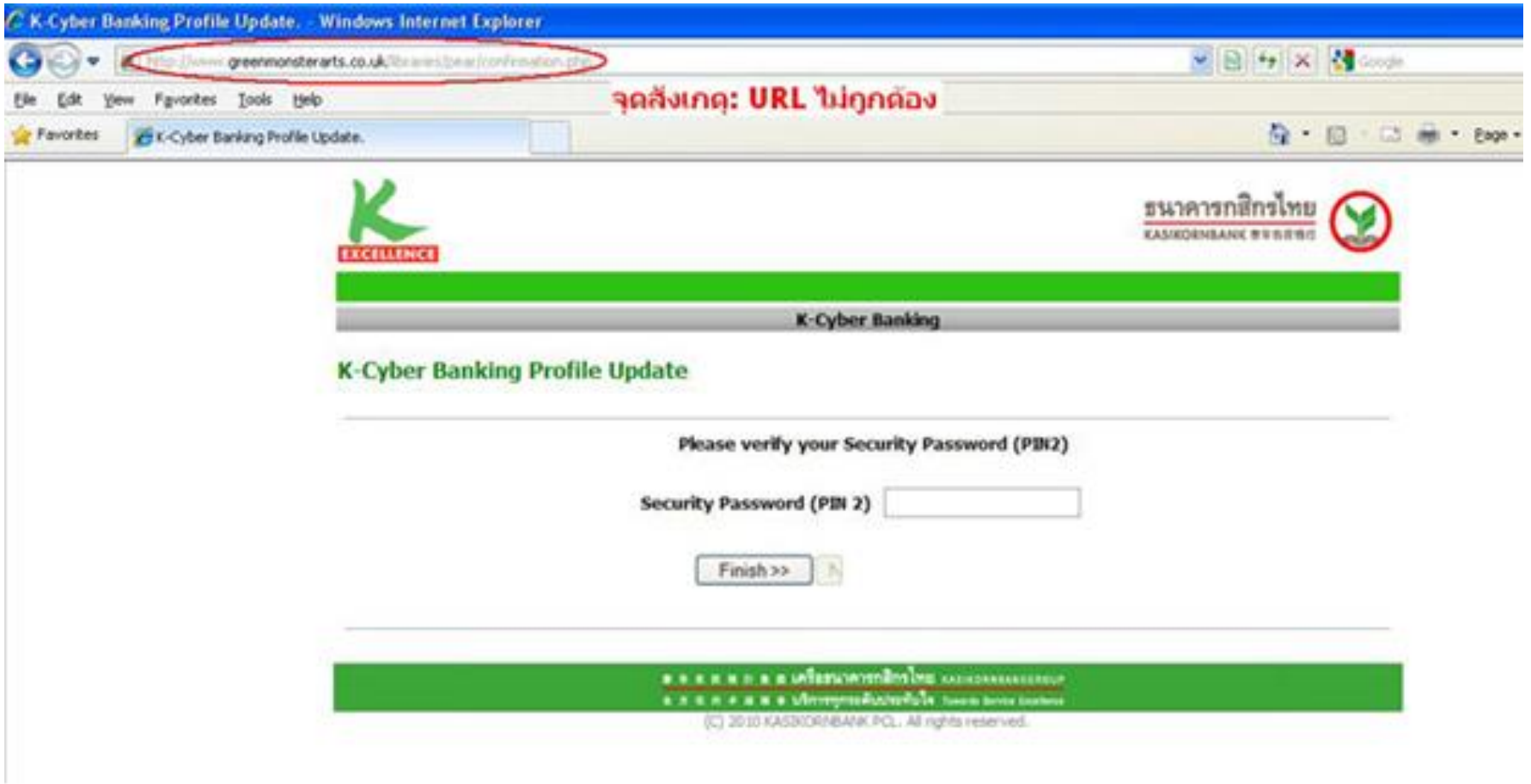
ตัวอย่าง การ Phishing



http://nongblogs-nn.blogspot.com/2012_05_01_archive.html

ความปลอดภัยยุคดิจิตอล

ตัวอย่าง การ Phishing



http://nongblogs-nn.blogspot.com/2012_05_01_archive.html

ความปลอดภัยยุคดิจิตอล

Mobile Security and Privacy

ความเป็นส่วนตัวและความปลอดภัยบนมือถือ ซึ่งในยุคปัจจุบันเราใช้อุปกรณ์ประเภทเคลื่อนที่ได้ จัดเก็บข้อมูลสำคัญมากขึ้น อาทิเช่น รายชื่อผู้ติดต่อ รูปถ่าย ภาพเคลื่อน รวมทั้งเอกสารสำคัญเรื่องงานไว้บน อุปกรณ์ประเภทเคลื่อนที่มากขึ้น

ความปลอดภัยยุคดิจิตอล

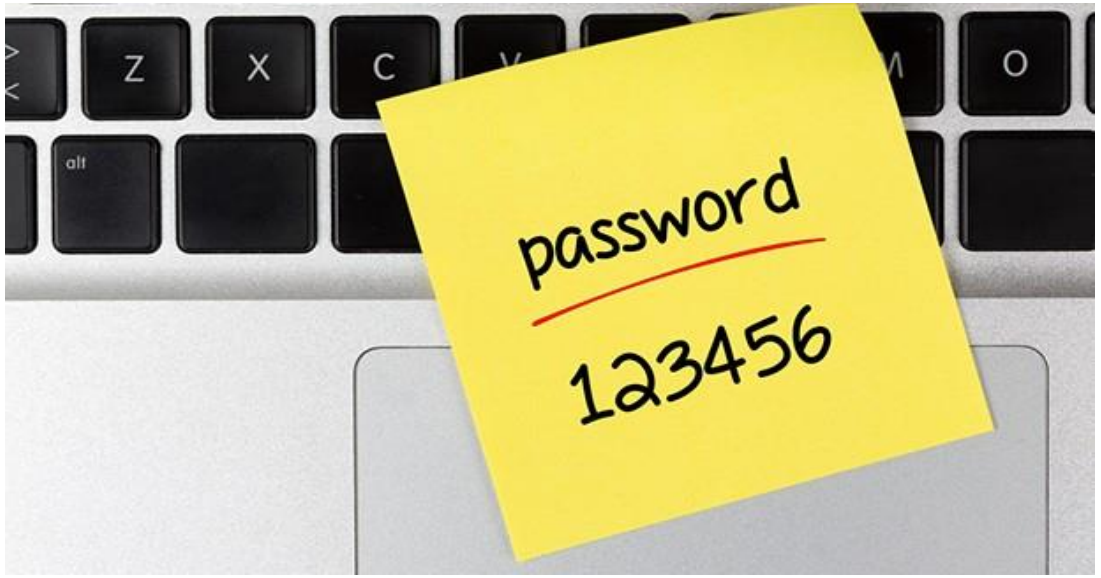
Mobile Security and Privacy

- การเก็บข้อมูลสำคัญ
- เกิดอะไรขึ้นถ้าโทรศัพท์เคลื่อนที่หาย
- การส่งตำแหน่งที่อยู่ของอุปกรณ์ไปยังเครื่องแม่ข่ายตลอดเวลา
- การสำรองข้อมูลบนมือถือ
- เอกสารงานสำคัญบนโทรศัพท์เคลื่อนที่

ความปลอดภัยยุคดิจิตอล

รหัสผ่านที่ไม่ควรตั้ง

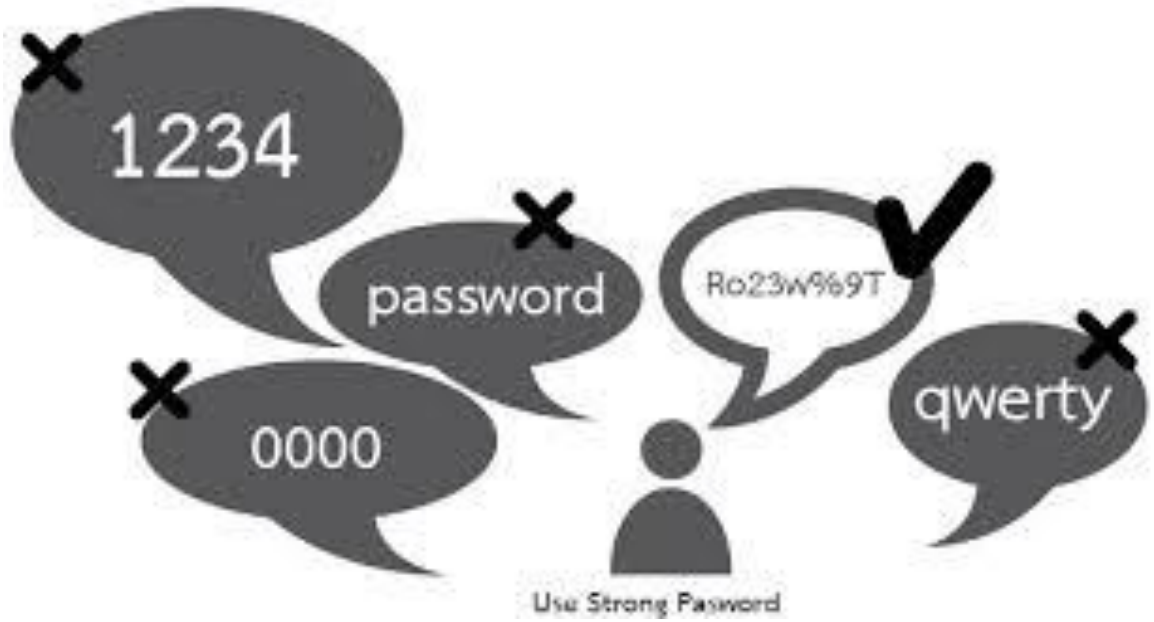
- ใช้รหัสเดียวกันหมด รู้รหัสเดียวสามารถเข้าถึงได้หมด
- ไม่มีการเปลี่ยนรหัสผ่า
- คาดเดาง่ายเช่น 1234567
- ประกอบด้วยข้อมูลบุคคล เช่น วันเกิด เบอร์โทร
- ใช้คำมีความหมาย เช่น ชื่อเล่น love happy
- ใช้ตัวพิมพ์ทั้งหมด ไม่มีตัวเลขหรือตัวอักษรผสม



ความปลอดภัยยุคดิจิตอล

รหัสผ่านที่ดี

- ใช้รหัสผ่านที่ยาว (อย่างน้อย 7 ตัว)
- ใช้ตัวอักษรตัวพิมพ์ใหญ่และตัวพิมพ์เล็ก ตัวเลข รวมทั้งสัญลักษณ์ต่างๆ ประกอบกัน
- ใช้สัญลักษณ์อย่างน้อยหนึ่งตัวในตำแหน่งที่ 2 – 6
- ใช้ตัวอักษรที่แตกต่างกันอย่างน้อย 4 ตัว (อย่าใช้ตัวอักษรซ้ำกัน) ใช้ตัวเลขและตัวอักษรแบบสุ่ม



ความปลอดภัยยุคดิจิตอล

เวลาที่ใช้ในการถอดรหัสผ่าน

5 นาที	เดือนครึ่ง	229 ปี
		
รหัสผ่านมีความยาว 6 ตัว มีตัวอักษรเล็กอย่างเดียว เช่น darren	รหัสผ่านมีความยาว 7 ตัว มีตัวอักษรเล็กใหญ่และตัวเลข เช่น Land3rz	รหัสผ่านมีความยาว 8 ตัว มีตัวอักษรเล็กใหญ่และตัวเลข และอัขระพิเศษ เช่น B33r&Mug

หมายเหตุ: เวลาในการถอดรหัสอยู่ที่ 1,000,000 ชุดต่อวินาที

mindterra

ความปลอดภัยยุคดิจิตอล

พฤติกรรมเสี่ยง เมื่อใช้อุปกรณ์ในที่สาธารณะ

- เชื่อมกับไวไฟที่ไม่ได้เข้ารหัส
- ไม่ระวังว่ามีผู้อื่นแอบฟังบทสนทนาอยู่
- ไม่ระวังผู้อื่นแอบหน้าจอ
- ไม่ระวังรอบตัว

ความปลอดภัยยุคดิจิตอล

การหลอกลวงออนไลน์ (Fraud)

การหลอกลวงในการซื้อขายสินค้าออนไลน์ วงจรของกลโกงที่มิจฉาชีพร้านขายสินค้าปลอมมักจะใช้เพื่อหาเหยื่อนั้นมี 6 ขั้นตอน ได้แก่

- มิจฉาชีพจะติดต่อหาเหยื่อที่กำลังต้องการสินค้า
- สร้างความเชื่อถือด้วยภาพสินค้า และหลักฐานปลอมเพื่อระบุตัวตน
- หว่านล้อมให้เหยื่อยอมโอนเงินค่าสินค้า หากเหยื่อรู้สึกว่าราคาถูกจนผิดปกติ หรือ รู้สึกไม่ไว้วางใจ มิจฉาชีพก็จะพยายามพูดโกหกเพื่อตอบข้อสงสัยของเหยื่อ
- ส่งสินค้าปลอมให้เหยื่อ หรือในกรณีที่แย่ที่สุด คือไม่ส่งสินค้าใดๆ ให้เลย
- ปิดช่องทางการสื่อสาร และหลบหนี ลบข้อมูลทุกอย่างทิ้ง
- เปลี่ยนชื่อ หลักฐาน เริ่มวงจรหลอกลวงใหม่

https://report.thaihotline.org/knowledge/online_safety/279

ความปลอดภัยยุคดิจิตอล

การหลอกลวงออนไลน์ (Fraud)

การหลอกลวงขอหมายเลขบัตรเครดิต เพื่อนำไปลักลอบใช้ทุกวันนี้ด้วยโลกอินเทอร์เน็ตที่เข้ามาในบ้านเรา และมีเครือข่ายที่ครอบคลุมมากขึ้นเรื่อยๆ ทำให้คนยุคใหม่ที่เคยซื้อของต่างๆได้ง่ายขึ้นผ่านระบบออนไลน์ โดยไม่ต้องออกไปข้างนอกให้เสียเวลา เพียงแค่สั่งซื้อสินค้าที่เราสนใจและจ่ายผ่านทางบัตรเครดิต เท่านี้เราก็จะได้สินค้าส่งตรงถึงบ้าน แต่โลกออนไลน์ก็เต็มไปด้วยการหลอกลวงเพื่อเอาเงินของเรา จึงต้องระวังอย่างมากเมื่อ ใช้บัตรเครดิตซื้อของออนไลน์ ในปัจจุบัน

ความปลอดภัยยุคดิจิตอล

การหลอกลวงออนไลน์ (Fraud)

5 ข้อควรระวังเมื่อ ใช้บัตรเครดิตซื้อของออนไลน์

- อย่าให้หมายเลขบัตรผ่านทางอีเมลล์
- ตรวจสอบความน่าเชื่อถือของร้านค้าเสมอ
- แน่ใจว่าเว็บไซต์ต่างๆปลอดภัยสำหรับคุณ
- เช็คยอดหนี้ในบัตรเครดิตอย่างละเอียด
- ไม่มีการส่งลิงค์หรือส่งข้อมูลสำคัญทางอีเมลล์

https://moneyhub.in.th/article/credit-card-online-shopping/

ความปลอดภัยยุคดิจิตอล

การหลอกลวงออนไลน์ (Fraud)

การป้องกันไม่ให้ตกเป็นเหยื่อการหลอกลวงออนไลน์

- ตั้งรหัสผ่านที่ยากต่อการคาดเดา
- สังเกตุความเปลี่ยนแปลง เช่น มีโปรแกรมแปลกปลอมหรือไม่
- หมั่นปรับปรุงระบบปฏิบัติการและโปรแกรมต่าง ๆ
- ลงซอฟต์แวร์เท่าที่จำเป็น
- หลีกเลี่ยงเวบไซค์เสี่ยง
- ระวังการใช้งานเมื่ออยู่ในที่สาธารณะ
- ไม่เปิดเผยข้อมูลส่วนตัว
- ปฏิบัติตามกฎหมายเกียงกับการใช้งานอินเตอร์เน็ต

ความปลอดภัยยุคดิจิตอล

อันตรายจากการใช้ Wifi สาธารณะ

ความไม่ปลอดภัยที่เป็นไปได้ เมื่อคุณเข้าใช้

ฟรี wifi network, การ hack

wireless มีรูปแบบใหนบ้าง และวิธีการป้องกันตนเอง เพื่อป้องกันจากการถูก hack บนเครือข่าย ฟรี wifi network

ความปลอดภัยยุคดิจิตอล

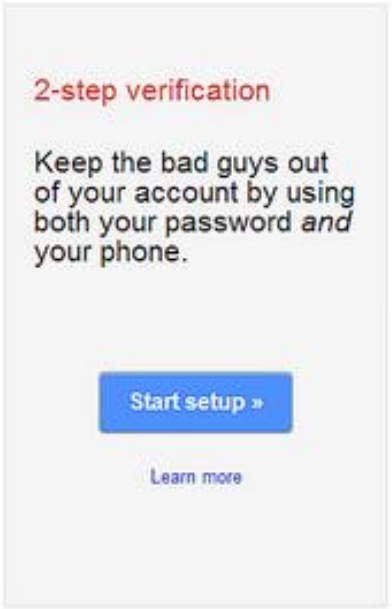
อันตรายจากการใช้ Wifi สาธารณะ

รูปแบบ การ hack บนเครือข่าย Wireless

- **Sniffing** เป็นการใช้โปรแกรมในการดักจับ packets ที่ผ่านไปมาบนเครือข่ายไวเลสที่ไม่มีความปลอดภัย (ฟรี wifi network)
- **Sidejacking** เป็นเทคนิคในการดักจับ cookie sessions เพื่อ login เข้าใช้ account facebook ของคุณ เป็นต้น โดยไม่ต้องใช้ username หรือ รหัสผ่าน
- **Evil Twin/Honeypot** เทคนิคในการสร้าง access point ปลอมขึ้นมา เพื่อหลอกให้คุณเข้าใช้ โดยตั้งชื่อ access point ให้เหมือนกับเครือข่ายไวเลส ที่คุณใช้อยู่ประจำ หลังจากนั้น จะใช้ โปรแกรม hack password หรือ โปรแกรมดักจับข้อมูล เพื่อเก็บข้อมูลการใช้งานอินเตอร์เน็ต

Workshop 1

- เพิ่มความปลอดภัยด้วย two step authentication บน Facebook, Gmail..



Workshop 2

- **ชัวร์ก่อนแชร์: กับดักโซเชียล**

“พ่อในเครื่องแบบ ตบต่อยลูกสาวแท้ ๆ ประชดแฟนสาวที่ตีจาก หวังให้กลับมา”

เมื่อเห็นหัวข้อข่าวแบบนี้ ย่อมกระทบจิตใจชาวโซเชียลยิ่งนัก ชื่อเว็บไซต์ต้นทางเป็นเว็บข่าวดังน่าเชื่อถือ และยิ่งในลิงก์ก็มีการแสดงภาพบางส่วนจากหน้าเว็บ เห็นเป็นภาพนายตำรวจกับภาพเด็กที่เต็มด้วยรอยแผลฟกช้ำ ยิ่งทำให้คนที่ได้อ่านต้องรีบกด “แชร์” ต่อให้เพื่อนทันที เพราะเรื่องนี้รุนแรงมาก “โหดร้ายทารุณ ต้องลงโทษคนผิดให้ได้ !!!!” บางคนอาจจะเติมความเห็นเข้าไปเพิ่มด้วย

เดี๋ยวนะครับ... ยังไม่ได้กดเข้าไปอ่าน ก็แชร์กันแล้วเหรอ ?

จะมีสักกี่คนที่เกิดความสงสัยว่า “ข่าวนั้นจริงหรือไม่ ?” “ชัวร์เหรอ ?”