การรักษาความปลอดภัยในระบบคอมพิวเตอร์ Computer Security

ปรับปรุงโดย อ.ดร.นพรัตน์ วนิชชานันท์

ประเภทของแฮกเกอร์ (Hacker Type)(1)

- Script Kiddies
  - เป็นกลุ่มคนที่ไม่จำเป็นต้องมีความรู้เกี่ยวกับการแฮกมาก
  - ใช้สคริปส์หรือโปรแกรมสำเร็จรูป หรือแฮกตามวิธีที่มีการแชร์ในอินเตอร์เน็ต
  - แฮกพาสเวิร์ด หรือปลอมแปลงการแสดงผลข้อมูลในหน้าเว็บ
- Hackers
  - White Hat/Ethical Hacker
    - เป็นผู้เชี่ยวชาญในการเจาะระบบ เพื่อหาช่องโหว่ในระบบ ใช้ในการป้องกัน (Penetration Test, Vulnerability Assessment)
    - ทำงานในบริษัทที่ปรึกษาด้านความมั่นคงปลอดภัย หรือบริษัทผู้ผลิตซอฟต์แวร์

ประเภทของแฮกเกอร์ (Hacker Type) (2)

- Black Hat/Cracker
  - มีความสามารถสูง จุดมุ่งหมายการแฮก เพื่อทำให้ระบบปั่นป่วน หรือต้องการควบคุม เพื่อก่ออาชญากรรมอื่นๆ
  - เช่นการลักลอบเข้าระบบควบคุมสาธารณูปโภคต่างๆ หรือ คนเขียนโปรแกรมเพื่อแครกรหัสผ่าน
- Grey Hat
  - กลุ่มแฮกเกอร์ที่ทำงานสองด้าน คือมีการลักลอบเจาะระบบ เพื่อความสนุกสนาน แต่ก็ทำการเตือนให้ผู้ดูแลระบบเพื่อให้ป้องกันระบบเช่นกัน

ประเภทของแฮกเกอร์ (Hacker Type) (3)

- Hacktivist/cyber terrorist
  - กลุ่มนี้เรียกได้ว่าเป็นอาชญากรทางคอมพิวเตอร์ มีจุดประสงค์ในการก่อให้เกิดความเสียหายในวงกว้าง หรือต้องการผลประโยชน์ทางการเมือง
  - ทำความเสียหายประเภท Denial of Service หรือเปลี่ยนหน้าเว็บไซต์ (Defacing) องค์กรต่างๆ

ประเภทภัยคุกคามในระบบคอมพิวเตอร์ (1) (Threats Classification)

- Computer Attack:
  มุ่งทำความเสียหายให้กับ ข้อมูล ระบบคอมพิวเตอร์และเน็ตเวิร์กโดยตรง
- Computer Crimes:
  ใช้เทคโนโลยีคอมพิวเตอร์และเน็ตเวิร์กเพื่อเป็นเครื่องมือในการทำความเสียหาย หรืออาชญากรรมต่อเนื่อง

ที่มา http://en.wikipedia.org/wiki/Computer_crime

ประเภทภัยคุกคามในระบบคอมพิวเตอร์ (2) (Threats Classification)

- Computer Attack ได้ แก่
  - คอมพิวเตอร์ไวรัส และเวิร์ม (Virus and worm)
  - การโจมตีเพื่อไม่ให้ทำงานปกติได้ (Denial of Service)
  - โปรแกรมประเภทมัลแวร์ (Malware)

ที่มา http://en.wikipedia.org/wiki/Computer_crime

ประเภทภัยคุกคามในระบบคอมพิวเตอร์ (3) (Threats Classification)

- Computer Crimes :
  - การสะกดรอยจากการใช้อินเตอร์เน็ต (Cyber stalking)
  - การปลอมตัว หรือทำรายการปลอม (Fraud and Identity theft)
  - การล่อลวง หลอกลวง (Phishing, Scams, Hoax)

ที่มา http://en.wikipedia.org/wiki/Computer_crime

ตัวอย่างภัยคุกคามในระบบคอมพิวเตอร์ - Computer Attack

- Virus
- Worm
- Malware
- Denial of Service

Computer Attacks

- โปรแกรมอัตโนมัติที่มุ่งหวังทำให้เกิดความเสียหายในระบบคอมพิวเตอร์และเน็ตเวิร์ก
  - ประเภทเพิ่มจำนวนตัวได้เองโดยอัตโนมัติ ได้แก่ Virus และ Worm
  - ประเภทไม่เพิ่มจำนวนเอง ได้แก่ Malware/Trojan และ Denial of Service

Virus

- ทำความเสียหายให้กับโปรแกรม หรือไฟล์ที่อยู่ในเครื่อง
- สามารถแพร่ได้ผ่านสื่อ เช่น แนบไปกับอีเมลล์ หรือ usb drive
- สามารถป้องกันโดยการติดตั้งโปรแกรมประเภท Antivirus

Worm

- เพิ่มจำนวนตัวเองได้อัตโนมัติ
- เน้นการโจมตีเน็ตเวิร์ก หรือคอมพิวเตอร์ด้วยข้อมูลมหาศาล ทำให้ไม่สามารถใช้งานได้
- ทำให้อินเตอร์เน็ตช้า หรือเครื่องคอมพิวเตอร์ช้าทำงานไม่ได้

Malware/Trojan

- ไม่เพิ่มจำนวน แต่เป็นการซ่อนตัวอยู่ในระบบ
- โจมตีตามคำสั่งที่ระบุ เช่น เก็บข้อมูลการพิมพ์ของผู้ใช้ เพื่อขโมยพาสเวิร์ด
- มักติดมากับโปรแกรมประเภท Keygen หรือ Crack

Denial of Service

- Denial of Service (DOS) and Distributed Denial of Service (DDOS)
  - เป็นการโจมตีโดยอาศัยเครื่องปกติในการร้องขอการใช้งานจำนวนมหาศาลจนเกินความสามารถในการให้บริการ และทำให้เซิร์ฟเวอร์ไม่สามารถทำงานได้
  - อาจติดมาจากโปรแกรมประเภท Worm หรือ Trojan

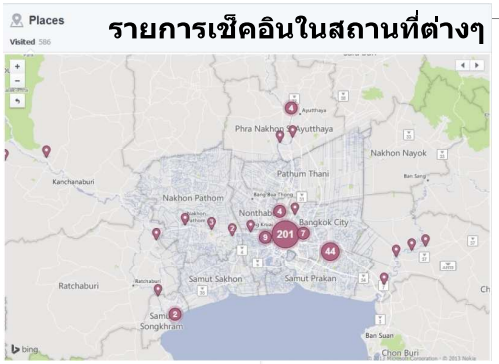
ตัวอย่างภัยคุกคามในระบบคอมพิวเตอร์ - Computer Crime

- Cyber stalking
- Fraud and Identity theft
- Phishing, Scams, Hoax

Cyber Stalking and Harassment

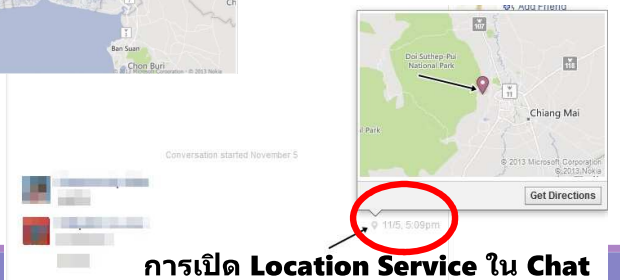
- คอยติดตามพฤติกรรมการใช้อินเตอร์เน็ตของเหยื่อ (โดยเฉพาะจาก Social Network)
  - ไม่ควรเช็คอินที่บ้าน หรือตั้งสถานะว่าอยู่บ้านคนเดียว หรือให้ข้อมูลส่วนตัวมากเกินไป
  - ไม่ควรเปิด Location Service ในโปรแกรมแชต
  - ไม่ควรตั้งค่าการแชร์เป็นแบบ Public

ตัวอย่างการแชร์ Location ของตนเองใน Facebook



รายการเช็คอินในสถานที่ต่างๆ

รูปแบบความเป็นส่วนตัวของการโพสข้อความ



การเปิด **Location Service** ใน **Chat**

ภัยในการทำธุรกรรมออนไลน์

1. หลอกให้ติดตั้งโปรแกรมในเครื่องคอมพิวเตอร์หรือมือถือ
2. ทำการสร้างเว็บไซต์ปลอมของธนาคารเพื่อให้ ล๊อกอินและขโมยพาสเวิร์ด
3. ทำการล๊อกโทรศัพท์เพื่อตรวจจับ SMS ที่เป็น OTP
4. ทำการโอนเงินโดยที่เจ้าของบัญชีไม่รู้ตัว

http://www.1213.or.th/th/finfrauds/OnlineFraud/Pages/OnlineFraud.aspx

การใช้งานธนาคารออนไลน์ทั่วไป

- ไม่ควรใช้รหัสผ่าน (password) ที่ง่ายต่อการคาดเดา เช่น 123456 หรือ วัน/เดือน/ปีเกิด
- ก่อนเข้าใช้ธนาคารออนไลน์ จะต้องมั่นใจหรือตรวจสอบให้แน่ใจว่าเป็นอุปกรณ์ที่ใช้นั้นไม่มีมัลแวร์ (Malware) แฝงอยู่
- ติดตั้งโปรแกรมป้องกันไวรัสที่ถูกกฎหมาย พร้อมตรวจสอบและอัพเดตโปรแกรมอยู่เสมอ
- ไม่ติดตั้ง หรือดาวน์โหลดโปรแกรมแปลก ๆ หรือโปรแกรมที่ไม่ถูกกฎหมาย เพราะอาจเป็นช่องทางให้มัลแวร์ เข้ามาในคอมพิวเตอร์ สมาร์ทโฟน หรือแท็บเล็ตได้
- ไม่ใช้ลิงก์เชื่อมโยงที่มากับอีเมลหรือในเว็บไซต์ต่าง ๆ เพื่อเข้าสู่ระบบธนาคารออนไลน์ แต่ควรพิมพ์ URL ด้วยตัวเอง
- ไม่ทำธุรกรรมการเงินผ่านอินเทอร์เน็ตสาธารณะ แต่หากจำเป็น ให้เปลี่ยนรหัสผ่านหลังจากใช้งานทันที

http://www.1213.or.th/th/finfrauds/OnlineFraud/Pages/OnlineFraud.aspx

การใช้งานธนาคารออนไลน์ทั่วไป (ต่อ)

- ตรวจสอบรายการเคลื่อนไหวในบัญชี และการเข้าใช้ระบบธนาคารออนไลน์อยู่เสมอ ว่าเป็นรายการที่ได้ทำไว้หรือไม่
- ควร "ออกจากระบบ" (logout) ทุกครั้งเมื่อไม่ใช้งาน
- จำกัดวงเงินในการทำธุรกรรมผ่านธนาคารออนไลน์ เพื่อลดความเสี่ยงในกรณีถูกมิจฉาชีพขโมยรหัสผ่าน
- ธนาคารไม่มีนโยบายส่ง SMS หรือ email เพื่อให้ดาวน์โหลด ติดตั้งโปรแกรม หรือเข้าสู่ระบบธนาคารออนไลน์
- หากคลิกลิงก์ต้องสงสัย ให้รีบติดต่อเจ้าหน้าที่ธนาคารหรือฝ่ายบริการลูกค้าของธนาคารทันทีและขอคำปรึกษาเกี่ยวกับการใช้งานที่ปลอดภัย
- ติดตามข่าวสารกลโกงธนาคารออนไลน์เป็นประจำ เพื่อรู้เท่าทันเล่ห์เหลี่ยมกลโกง

http://www.1213.or.th/th/finfrauds/OnlineFraud/Pages/OnlineFraud.aspx

Hoax

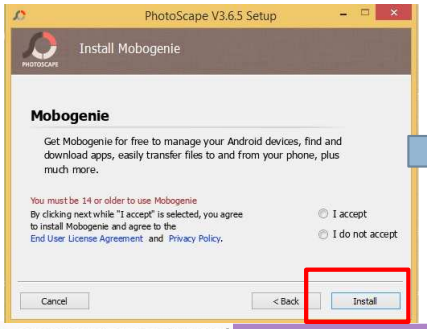
- ข้อความหรือบทความที่แชร์ต่อๆ กันมา
- ส่วนใหญ่เป็นข่าวลือ หาแหล่งอ้างอิงยืนยันไม่ได้
- ต้องมีสติในการพิจารณา

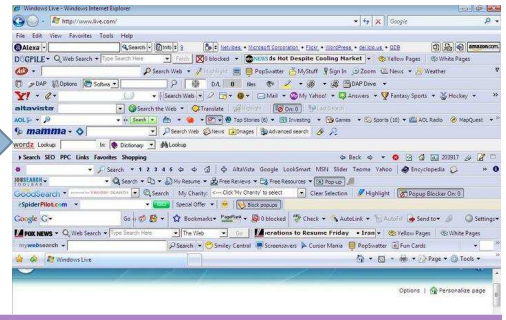
วิธีท่องเวปอย่างปลอดภัย (1)

1. อ่าน และคิดก่อนคลิกลิ้งค์ใดๆ
2. ไม่ใช้โปรแกรมแครก หรือโปรแกรมที่ผู้ผลิตไม่น่าเชื่อถือ
3. ตั้งค่าการเปิดเผยข้อมูลส่วนตัวใน Social online ให้เหมาะสม
4. ติดตั้งโปรแกรมรักษาความปลอดภัยในเครื่อง
5. เปลี่ยนพาสเวิร์ดแอคเค้าท์ส่วนตัวเป็นประจำ
6. ไม่เลือกพาสเวิร์ดที่เดาได้ง่าย
7. ล๊อกเอาท์ทุกครั้งในการใช้งานเครื่องคอมพิวเตอร์สาธารณะ
8. ติดตั้งพาสเวิร์ดสำหรับล๊อกหน้าจอคอมพิวเตอร์/โทรศัพท์/แทบเล็ต

วิธีท่องเวปอย่างปลอดภัย (2)

- ขั้นตอนการลงโปรแกรม มักจะมีโฆษณาแฝงก่อนลงโปรแกรม ให้แน่ใจว่าอ่านรายละเอียดก่อนกด Next



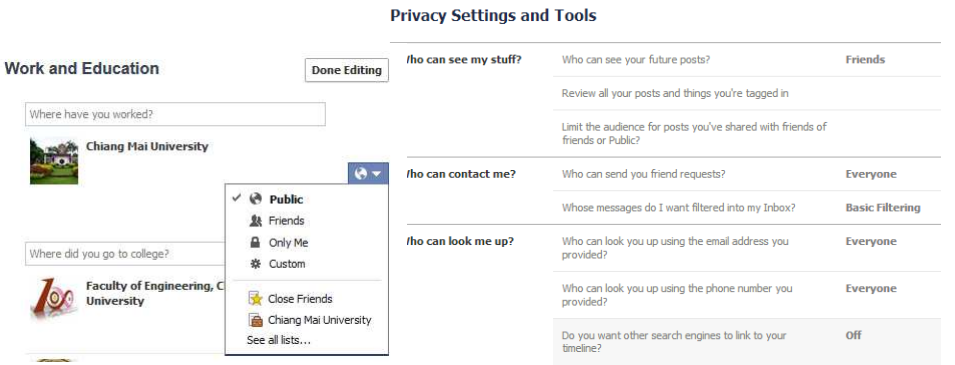


วิธีท่องเวปอย่างปลอดภัย (3)

- ตรวจสอบลิงค์ต่างๆ ให้ดีก่อนคลิก
- คิดทุกครั้งก่อนกรอกข้อมูลส่วนตัว
  - หมายเลขบัตรประจำตัวประชาชน
  - วันเดือนปีเกิด
  - เบอร์โทรศัพท์
  - ที่อยู่

วิธีท่องเวปอย่างปลอดภัย (4)

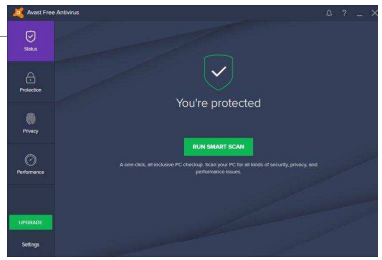
- ตัวอย่างการตั้งค่าความเป็นส่วนตัวของ Facebook



วิธีท่องเวปอย่างปลอดภัย (5)

Top Free Antivirus (2017)

- Avast Free Antivirus
- AVG Antivirus Free
- Bitdefender Antivirus Free Edition
- ZoneAlarm Free Antivirus
- Avira Free Antivirus

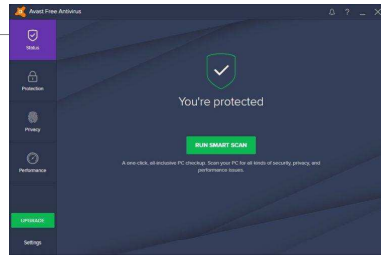


ที่มา: http://www.pcmag.com/article2/0,2817,2388652,00.asp

วิธีท่องเวปอย่างปลอดภัย (6)

Top Free Antivirus (2017)

- Avast Free Antivirus
- AVG Antivirus Free
- Bitdefender Antivirus Free Edition
- ZoneAlarm Free Antivirus
- Avira Free Antivirus

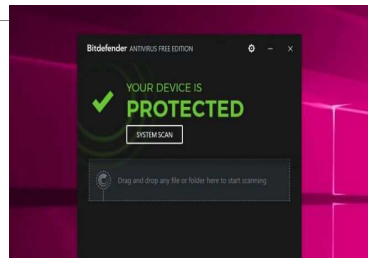


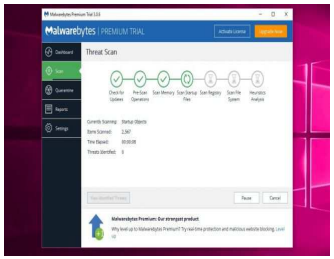
ที่มา: http://www.pcmag.com/article2/0,2817,2388652,00.asp

วิธีท่องเวปอย่างปลอดภัย (7)

Top Free Anti-malware (2017)

- BitDefender Antivirus Free Edition
- AVG AntiVirus Free
- MalwareBytes Anti-Malware
- SpyBot Search & Destroy
- Emsisoft Emergency Kit





ที่มา :http://www.techradar.com/news/software/applications/best-free-anti-spyware-and-anti-malware-software-1321656