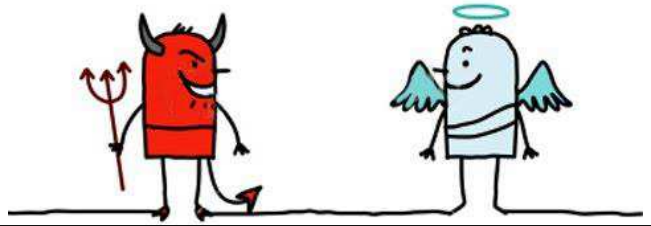
จริยธรรมและการรักษาความปลอดภัยในระบบคอมพิวเตอร์ (COMPUTER ETHICS AND COMPUTER SECURITY)

โดย ร.ศ. พรรณิภา ไพบูลย์นิมิตร
ปรับปรุงโดย อ.ดร.รัศมีทิพย์ วิตา

จริยธรรมในการใช้คอมพิวเตอร์ Computer Ethics

จริยธรรม (Ethics)

- จริยธรรม คือหลักเกณฑ์ที่มีการตกลงร่วมกัน เพื่อเป็นแนวทางปฏิบัติในสังคม
- เป็นที่ยอมรับระหว่างสมาชิกของสังคม
- ใช้เพื่อจำแนกแยกแยะว่าสิ่งไหนถูกและสิ่งไหนผิด



Ethics in Computer System

- ระบบคอมพิวเตอร์ มีส่วนเกี่ยวข้องกับชีวิตมนุษย์ในหลายแง่มุม เช่น
  - ระบบธนาคาร
  - ระบบทางการแพทย์
  - ระบบฐานข้อมูลประชากร
  - ข้อมูลส่วนตัว (เช่น เลขประจำตัวประชาชน วันเดือนปีเกิด ฯลฯ)
  - ข้อมูลความคิดเห็นในสังคมออนไลน์ต่างๆ
- การใช้งานและการเข้าถึงข้อมูลต่างๆ สามารถเกิดผลดี/เสียโดยตรงกับเจ้าของข้อมูล
- จำเป็นต้องมีหลักจริยธรรมในการใช้งานระบบคอมพิวเตอร์

4 Issues in Information Ethics*

- ความเป็นส่วนตัว (Information Privacy)
  - ระดับของการเปิดเผยข้อมูลส่วนบุคคล และการยืนยันตัวตน
- ความถูกต้องของข้อมูล (Information Accuracy)
  - ตรวจสอบที่มาที่ไปของข้อมูล และแหล่งอ้างอิงได้
- ความเป็นเจ้าของ (Information Property)
  - การครอบครอง หรือเผยแพร่ข้อมูล/เนื้อหาที่มีลิขสิทธิ
- การเข้าถึงข้อมูล (Information Accessibility)
  - จำกัดสิทธิ ในการเข้าถึงเนื้อหาในระดับที่ต่างกัน

*Richard O. Mason, **Four Ethical Issues of the Information Age,** *MIS Quarterly* , Vol. 10, No. 1 (Mar., 1986), pp. 5-12

Consequences of Ethical Issues

- การขายข้อมูลเพื่อใช้ในการโฆษณา สร้างความรำคาญให้เจ้าของข้อมูล
- การปลอมตัวโดยใช้ข้อมูลส่วนตัวผู้อื่นในการยืนยันตัวตน
  - การทำธุรกรรมทางการเงิน
  - การแอบอ้างสิทธิ
- การกระจายของข้อมูลที่เป็นเท็จหรือบิดเบือน ข่าวลือต่างๆ
- การถูกละเมิดลิขสิทธิ (โปรแกรม เพลง รูปภาพ หรือผลงานอื่นๆ)
- ไวรัส หรือเวิร์ม
- เกิดความเสียหายในชีวิตและทรัพย์สิน เช่น ล่อลวง หรือข่มขู่จากข้อมูลที่ขโมยได้

PAPA: 4 Ethical Issues

- Information **P**rivacy
- Information **A**ccuracy
- Information **P**roperty
- Information **A**ccessibility

ความเป็นส่วนตัว (Information Privacy)

- ลักษณะของข้อมูลที่เป็นส่วนตัว
  - ประวัติครอบครัว
  - ประวัติการรักษาพยาบาล
  - ข้อมูลที่ใช้ยืนยันตัวตน (หมายเลขบัตรประจำตัวประชาชน วันเดือนปีเกิด)
  - ที่อยู่ (การเช็คอินในสังคมออนไลน์)
  - ชื่อแอคเคาท์ และพาสเวิร์ดสำหรับเว็บต่างๆ

ตัวอย่าง:
เพื่อนลืมล็อกเอ๊าท์เฟสบุคในเครื่องที่แลบ นศ ใช้งานต่อจากเพื่อนจะทำอย่างไร

- การละเมิดความเป็นส่วนตัว
  - จากระบบอัตโนมัติ เช่น โปรแกรมประเภท Trojan หรือ Spyware
  - จากการตั้งค่าการเปิดเผยข้อมูลส่วนตัวใน Social Network

ความถูกต้องของข้อมูล (Information Accuracy)

- การตรวจสอบข้อมูลส่วนตัวในการกรอกข้อมูลในระบบต่าง เช่น
  - ข้อมูลการศึกษา
  - การทำธุรกรรมธนาคาร
  - ระเบียนการรักษาพยาบาล

ตัวอย่าง:
กรอกเลขประจำตัวผิด/ไม่กรอก = ไม่สามารถตรวจสอบและให้คะแนนได้ ☹

- การตรวจสอบข้อมูลที่มีการเผยแพร่
  - ความหน้าเชื่อถือของแหล่งที่มา
  - หลักฐานอ้างอิง
  - วิเคราะห์ด้วยหลักการและเหตุผล

ตัวอย่าง:
ข้อมูลเตือนภัย แชร์แล้วได้เงินบริจาค ให้ตรวจสอบให้ดีก่อน อย่าอ้างว่า "ก็ไม่รู้สินะ เค้าแชร์มาอีกที"

ความเป็นเจ้าของ (Information Property)

- **ลิขสิทธิ์** เป็นทรัพย์สินทางปัญญาประเภทหนึ่งที่ **กฎหมายให้ความคุ้มครอง** โดยให้เจ้าของลิขสิทธิ์เป็นผู้มีสิทธิแต่ผู้เดียว (Exclusive rights) ที่จะกระทำการใด ๆ เกี่ยวกับงานสร้างสรรค์ที่ได้ทำขึ้น
  - ลิขสิทธิ์นี้มีอยู่ตลอดอายุของผู้สร้างสรรค์ และมีอยู่ต่อไปอีกเป็นเวลา 50 ปี นับแต่ผู้สร้างสรรค์ถึงแก่ความตาย

ที่มา: ความหมายของลิขสิทธิ http://dict.longdo.com/search/copyright

ความเป็นเจ้าของ (Information Property)

ตัวอย่างข้อมูลที่มีลิขสิทธิ์

- วรรณกรรม (โปรแกรมคอมพิวเตอร์)
- นาฏกรรม
- ศิลปกรรม
- ดนตรีกรรม
- โสตทัศนวัสดุ
- ภาพยนตร์
- สิ่งบันทึกเสียง
- งานแพร่ภาพแพร่เสียง

ตัวอย่างข้อมูลที่ไม่มีลิขสิทธิ์

- ข่าวประจำวัน และข้อเท็จจริงต่างๆ
- รัฐธรรมนูญ และ กฎหมาย
- ระเบียบ ข้อบังคับ ประกาศ คำสั่ง กระทรวง
- คำพิพากษา คำสั่ง คำวินิจฉัย และรายงานของทางราชการ
- คำแปลและการรวบรวมสิ่งต่างๆตามข้อ 1 ถึง 4 ที่หน่วยงานของรัฐจัดทำขึ้น

ความเป็นเจ้าของ (Information Property)

- การละเมิดลิขสิทธิ ตามพรบ.ลิขสิทธิ์ ปี พ.ศ.2537
  - ขาย มีไว้เพื่อขาย เสนอขาย ให้เช่า เสนอให้เช่า ให้เช่าซื้อ หรือเสนอให้เช่าซื้อ
  - เผยแพร่ต่อสาธารณชน
  - แจกจ่ายในลักษณะที่อาจก่อให้เกิดความเสียหายแก่เจ้าของลิขสิทธิ์
  - นำหรือสั่งเข้ามาในราชอาณาจักร
- บทลงโทษ
  - เผยแพร่โดยมิได้รับการยินยอม
    - ปรับ 20,000-200,000
  - เผยแพร่เพื่อการค้า
    - จำคุก 0.8-2 ปี ปรับ 100,000-800,000 หรือทั้งจำทั้งปรับ

ตัวอย่าง:
ข้อมูล/รูปภาพในอินเตอร์เน็ต มีเจ้าของ การคัดลอกหรือนำมาใช้งานโดยไม่ได้รับอนุญาต มีความผิดตามกฎหมาย

ที่มา:http://th.wikipedia.org/wiki/กฎหมายลิขสิทธิ์ไทย

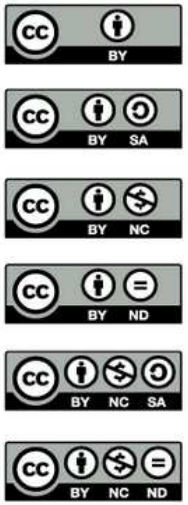
Free use license -Creative Commons (CC)

- เงื่อนไขในการให้อนุญาตของครีเอทีฟคอมมอนส์มีอยู่ 4 เงื่อนไข คือ
  - อ้างอิงแหล่งที่มา (BY) หมายถึงการนำไปใช้จะต้องอ้างอิงกลับมาถึงผู้เขียน
  - ให้อนุญาตต่อไปแบบเดียวกัน (SA) คือยินยอมให้มีการดัดแปลงงานได้โดยต้องมอบความยินยอมต่อไปด้วย
  - ห้ามนำไปใช้เพื่อการค้า (NC)
  - ห้ามดัดแปลง (ND) คือต้องใช้งานต้นฉบับเท่านั้นโดยไม่มีการดัดแปลงใดๆ ทั้งสิ้น

ที่มา http://th.wikipedia.org/wiki/ครีเอทีฟคอมมอนส์

Free use license -Creative Commons (CC)

- สัญญาอนุญาตครีเอทีฟคอมมอนส์แบ่งได้เป็น 6 ชนิดใหญ่ดังนี้
  - อ้างอิงแหล่งที่มา (CC-BY)
  - อ้างอิงแหล่งที่มา ให้อนุญาตต่อไปแบบเดียวกัน (CC-BY-SA)
  - อ้างอิงแหล่งที่มา ห้ามดัดแปลง (CC-BY-ND)
  - อ้างอิงแหล่งที่มา ห้ามนำไปใช้เพื่อการค้า (CC-BY-NC)
  - อ้างอิงแหล่งที่มา ห้ามนำไปใช้เพื่อการค้า และให้อนุญาตต่อไปแบบเดียวกัน (CC-BY-NC-SA)
  - อ้างอิงแหล่งที่มา ห้ามนำไปใช้เพื่อการค้า และห้ามดัดแปลง (CC-BY-NC-ND)



การเข้าถึงข้อมูล (Information Accessibility)

- สิทธิการเข้าถึงข้อมูลของผู้อื่น เช่นการมอนิเตอร์อีเมลในองค์กร สามารถทำได้ โดยต้องมีรายละเอียดที่ชัดเจนดังนี้
  - กำหนดผู้ที่มีสิทธิดำเนินการ *(เช่น กำหนดให้แอดมินทำได้เท่านั้น)*
  - ระดับของการดำเนินการ *(เช่น ตรวจสอบหัวเรื่อง ห้ามดูเนื้อหา)*
  - การนำข้อมูลออกไปใช้งาน *(เช่น ต้องเข้ารหัสก่อน หรือห้ามนำออกจากห้อง)*
  - ระเบียบขั้นตอนในการใช้ข้อมูล *(เช่น ต้องมีคำสั่ง ถึงจะดำเนินการได้)*

การเข้าถึงข้อมูล (Information Accessibility)

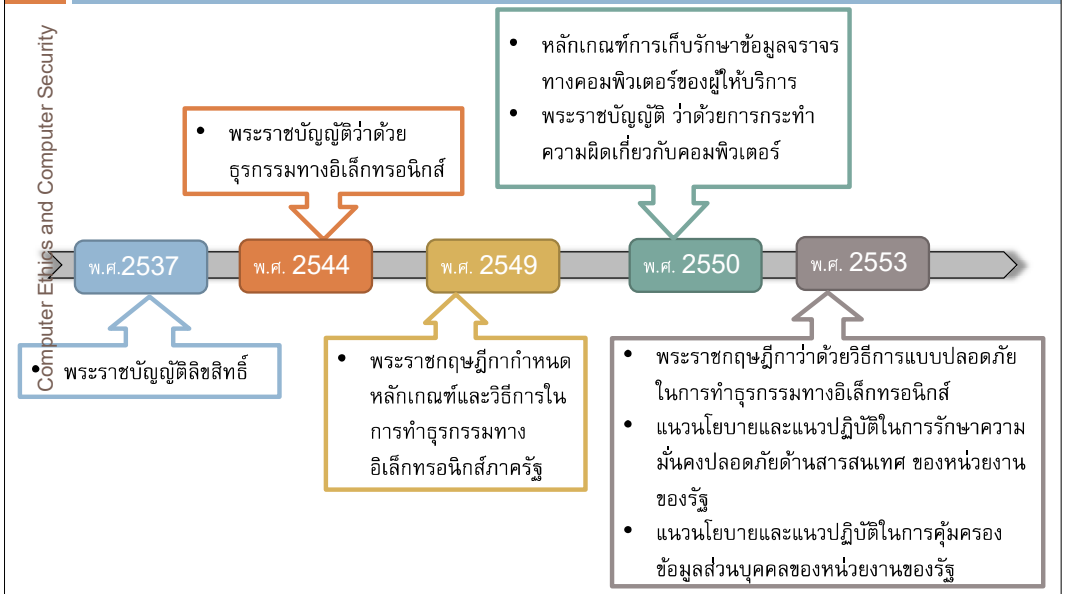
- ตัวอย่างการอนุญาตให้ผู้อื่นมีสิทธิใช้ข้อมูลส่วนตัว
  - การเซ็น Consent สำหรับการทำธุรกรรมออนไลน์
  - การกด Accept ใน Term&Condition ในการลงโปรแกรมต่างๆ

ตัวอย่าง:
เป็นแอดมิน สามารถเข้าถึงข้อมูลของทุกคนในระบบได้ แต่ต้องมีแนวทางปฏิบัติ หรือการบันทึกการทำงานที่สามารถตรวจสอบได้ เพื่อไม่ให้ละเมิดข้อมูลส่วนบุคคล

Information Law and Commandment

- Information Law in Thailand
- 10 Commandments for Ethical Computing

Information Law in Thailand



พ.ร.บ.คอมพิวเตอร์ ปี 2550 มาตรา 14

- ระบุไว้ว่า “ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(๑) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือ ข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

(๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(๓) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(๔) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(๕) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (๑) (๒) (๓) หรือ (๔)

พ.ร.บ.คอมพิวเตอร์ ปี 2550 มาตรา 14

- ระบุไว้ว่า “ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกิ

สรุป

การโพสภาพตัดต่อ ข้อมูลเท็จ ภาพอนาจาร ที่ทำให้เกิดความเสียหาย ต่อบุคคลและความมั่นคงของชาติ มีความผิด

“จำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน100,000 บาท”

ผิดทั้งคนโพส และคนแชร์!!

ตาม (๑) (๒) (๓) หรือ (๔)

บัญญัติ 10 ประการในการใช้คอมพิวเตอร์*(1)

- ต้องไม่ใช้คอมพิวเตอร์**ทำร้าย หรือละเมิดผู้อื่น**
- ต้องไม่**รบกวนการทำงาน**ของผู้อื่น
- ต้องไม่สอดแนม แก้ไข หรือ**เปิดดูแฟ้มข้อมูล**ของผู้อื่น
- ต้องไม่ใช้คอมพิวเตอร์เพื่อการ**โจรกรรมข้อมูล**ข่าวสาร
- ต้องไม่ใช้คอมพิวเตอร์**สร้างหลักฐานที่เป็นเท็จ**

*Ramon C. Barquin, **In Pursuit of a 'Ten Commandments' for Computer Ethics,** Computer Ethics Institute, May 7, 1992, *Washington Consulting Group and Computer Ethics Institute*

บัญญัติ 10 ประการในการใช้คอมพิวเตอร์*(2)

- ต้องไม่**คัดลอกโปรแกรม**ของผู้อื่นที่มีลิขสิทธิ์
- ต้องไม่**ละเมิดการใช้ทรัพยากรคอมพิวเตอร์**โดยที่ตนเองไม่มีสิทธิ์
- ต้องไม่**นำเอาผลงานของผู้อื่น**มาเป็นของตน
- ต้องคำนึงถึง**สิ่งที่จะเกิดขึ้นกับสังคม**ที่เกิดจากการกระทำของท่าน
- ต้องใช้คอมพิวเตอร์โดย**เคารพกฎระเบียบ**กติกาและมีมารยาท

*Ramon C. Barquin, **In Pursuit of a 'Ten Commandments' for Computer Ethics,** Computer Ethics Institute, May 7, 1992, *Washington Consulting Group and Computer Ethics Institute*

การรักษาความปลอดภัยในระบบคอมพิวเตอร์

Computer Security

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: มุ่งทำความเสียหายให้กับข้อมูล ระบบคอมพิวเตอร์และเน็ตเวิร์กโดยตรง
- Computer Crimes: ใช้เทคโนโลยีคอมพิวเตอร์และเน็ตเวิร์กเพื่อเป็นเครื่องมือในการทำความเสียหาย หรืออาชญากรรมต่อเนื่อง

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

ประเภทภัยคุกคามในระบบคอมพิวเตอร์ (2) (Threats Classification)

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

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

Computer Attacks

- 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 หรือเครื่องคอมพิวเตอร์ช้า ทำงานไม่ได้

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

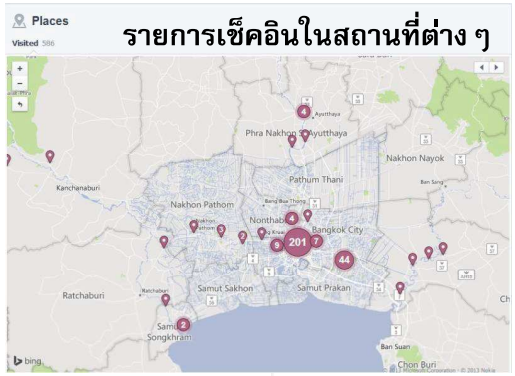
Computer Crimes

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

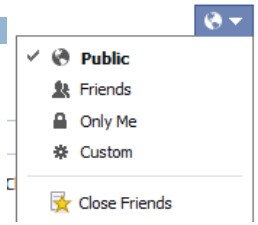
Cyber Stalking and Harassment

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

ตัวอย่างการแชร์ Location ของตนเองใน Facebook



รายการเช็คอินในสถานที่ต่าง ๆ



รูปแบบความเป็นส่วนตัวของการโพสข้อความ

การเปิด Location Service ใน Chat

Fraud in Internet Banking

1. หลอกให้ติดตั้งโปรแกรมในเครื่องคอมพิวเตอร์หรือมือถือ
2. ทำการสร้างเว็บไซต์ปลอมของธนาคารเพื่อให้ล๊อกอินและขโมยพาสเวิร์ด
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

- ข้อความหรือบทความที่แชร์ต่อ ๆกันมา
- ส่วนใหญ่เป็นข่าวลือ หาแหล่งอ้างอิงยืนยันไม่ได้
- ต้องมีสติในการพิจารณา

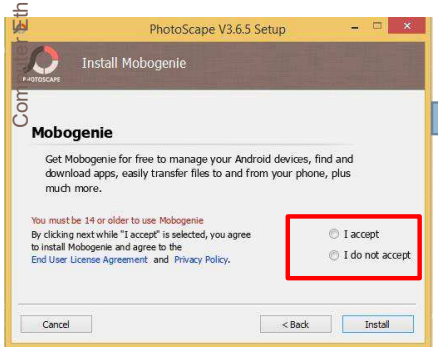
สีที่ท้ายหลอดยาสีฟัน มีชื่อเรียกว่า Eye mark มีไว้เพื่อให้เครื่องหนีบตัดหลอด"มองเห็น"ตำแหน่งที่จะตัด
สีจะแตกต่างกันไปแล้วแต่ยี่ห้อและความสวยงาม
ไม่เกี่ยวกับว่าทำจากสารเคมีหรือวัตถุดิบธรรมชาติแต่อย่างใด

How to stay safe online

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

How to stay safe online (2)

- ขั้นตอนการลงโปรแกรม มักจะมีโฆษณาแฝง ก่อนลงโปรแกรม ให้แน่ใจว่าอ่านรายละเอียดก่อนกด Next

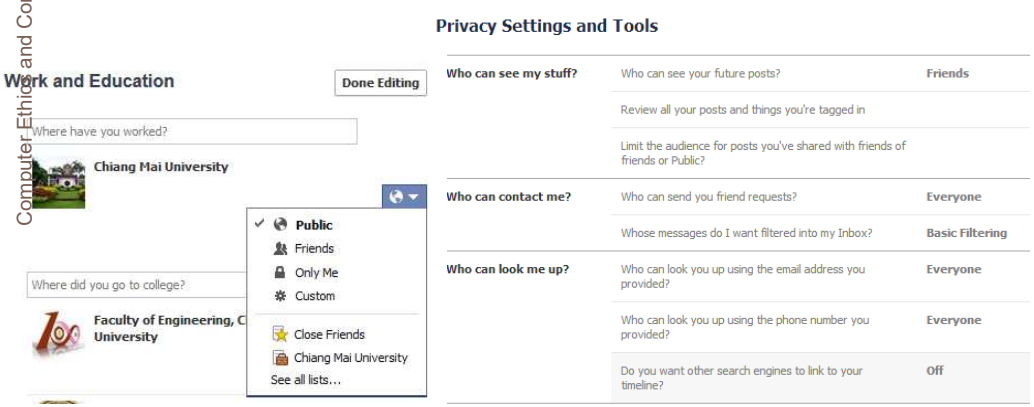


How to stay safe online (3)

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

How to stay safe online (4)

- ตัวอย่างการตั้งค่าความเป็นส่วนตัวของ Facebook



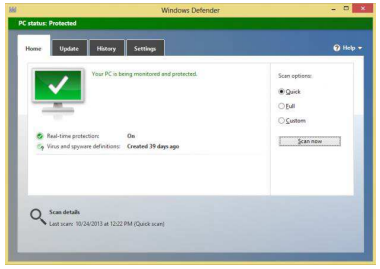
How to stay safe online (6)

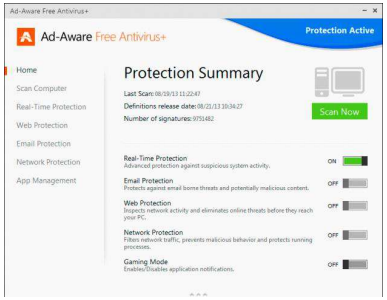
- Top Free Antivirus (2013)
  - Avast Free Antivirus
  - Panda Cloud Antivirus Free
  - ZoneAlarm Free Antivirus +Firewall
  - Avira Free Antivirus
  - Bitdefender Antivirus Free Edition

ที่มา: http://www.techradar.com/news/software/applications/best-free-antivirus-9-reviewed-and-rated-1057786

How to stay safe online (7)

- Top Antispyware (2013)
  - Macafee Virus Scan and Anti Spyware (not free)
  - Navarre Webroot Spy Sweeper (not free)
  - Lavasoft's Ad-Aware SE, Personal Edition
  - Microsoft Windows Defender
  - Spybot Search & Destroy





ที่มา :http://netforbeginners.about.com/od/lockdownyourpc/a/antispyware.htm

Q&A