จริยธรรมและความปลอดภัยในระบบคอมพิวเตอร์และระบบสารสนเทศ

ความหมายของ จริยธรรม (ethics)

- หลักศีลธรรมจรรยาท่กำหนดขึ้นเพื่อใช้เป็นแนวทางปฏิบัติหรือควบคุมการใช้ระบบคอมพิวเตอร์และสารสนเทศ
- หลักของความถูกต้องและความผิดที่บุคคลใช้เป็นแนวทางในการปฏิบัติ
- สรุป เป็นหลักเกณฑ์ที่ประชาชนตกลงร่วมกันเพื่อใช้เป็นแนวทางในการปฏิบัติร่วมกันในสังคม

4 ประเด็นของจริยธรรม (PAPA)

- ความเป็นส่วนตัว information privacy
- ความถูกต้อง information accuracy
- ความเป็นเจ้าของ intellectual property
- การเข้าถึงข้อมูล Data accessibility

information privacy

- สิทธิในการควบคุมข้อมูลของตนเองในการเปิดเผยให้กับผู้อื่น
- การละเมิดความเป็นส่วนตัว
  - เข้าไปอ่าน e-mail , ใช้คอมพิวเตอร์ตรวจจับการทำงานของพนักงาน, รวบรวมข้อมูลส่วนบุคคลสร้างเป็นฐานข้อมูลแล้วเอาไปขาย
  - ทำธุรกิจผ่านเว็บไซต์เพื่อรวบรวมข้อมูลไปขาย เช่น บริษัท doubleclick ,enage
  - ใช้โปรแกรม sniffer วิเคราะห์อัตราการใช้ internet ติดตามผู้ใช้เพื่อทำการส่ง e-mail ขายสินค้า ทำให้เกิด อีเมล์ขยะ (junk mail) ที่ผู้รับไม่ต้องการ เรียกว่า สแปม
- Tool ใช้ในการตรวจจับ spyware ได้แก่ ad-ware , spybot

ความถูกต้อง information accuracy

- ความถูกต้องขึ้นอยู่กับความถูกต้องในการบันทึกข้อมูล
- ต้องมีผู้รับผิดชอบในเรื่องความถูกต้อง
- ต้องมีการตรวจสอบความถูกต้องก่อนการบันทึก
- เช่น ถ้าให้ลูกค้าป้อนข้อมูลเอง ต้องให้สิทธิในการเข้าไปตรวจสอบความถูกต้องด้วยตนเอง
- ข้อมูลต้องมีความทันสมัยอยู่เสมอ

ความเป็นเจ้าของ intellectual property

- กรรมสิทธิในการถือครองทรัพย์สิน โดยทรัพย์สินแบ่งเป็น
  - จับต้องได้ คอมพิวเตอร์ รถยนต์
  - จับต้องไม่ได้แต่บันทึกลงในสื่อต่างๆ ได้ (ทรัพย์สินทางปัญญา) บทเพลง โปรแกรมคอมพิวเตอร์
- ได้รับความคุ้มครองสิทธิภายใต้กฎหมาย
  - ความลับทางการค้า เกี่ยวกับสูตร กรรมวิธีการผลิต รูปแบบสินค้า
  - ลิขสิทธิ์ สิทธิในการกระทำใดๆ เกี่ยวกับ งานเขียน ดนตรี ศิลป คุ้มครองในเรื่องการคัดลอกผลงานหรือทำซ้ำ โดยคุ้มครอง 50 ปีหลังจากได้แสดงผลงานครั้งแรก
  - สิทธิบัตร หนังสือที่คุ้มครองเกี่ยวกับสิ่งประดิษฐ์ หรือ ออกแบบผลิตภัณฑ์ มีอายุ 20 ปี นับตั้งแต่วันที่ขอรับสิทธิ

การละเมิดลิขสิทธิทางซอฟต์แวร์

- สิ่งที่ได้รับการคุ้มครองจากลิขสิทธิ์หรือสิทธิบัตรต้องเป็นเปิดเผยต่อสาธารณะ ให้คนทั่วไปใช้ ซึ่งต่างจากความลับทางการค้า
- โปรแกรมคอมพิวเตอร์ได้รับความคุ้มครองภายใต้ลิขสิทธิ์ (license)
  - Copyright หรือ SW license ซื้อลิขสิทธิ์มาและมีสิทธิใช้
  - Shareware ให้ทดลองใช้ก่อนตัดสินใจซื้อ
  - Free ware ใช้งานได้ฟรี copy ให้ผู้อื่นได้

การเข้าถึงข้อมูล Data accessibility

- กำหนดสิทธิตามระดับผู้ใช้งาน
- ป้องกันการเข้าไปดำเนินการต่างๆ กับข้อมูลของผู้ที่ไม่เกี่ยวข้อง
- ต้องมีการออกแบบระบบรักษาความปลอดภัยในการเข้าถึงข้อมูลของผู้ใช้

กฎหมายเทคโนโลยีสารสนเทศ

- ความก้าวหน้าทางเทคโนโลยีสารสนเทศทำให้เกิดการทำธุรกิจแบบให้บริการโดยไม่จำกัดสถานที่และเวลา คือให้บริการแบบ 24x7x365
- ปี 2546 ประเภทไทยมีกฎหมาย 6 ฉบับ
  - ธุรกรรมทางอิเล็กทรอนิกส์ e-transaction law
  - ลายมือชื่ออิเล็กทรอนิกส์ e-signatures law
  - อาชญากรรมทางคอมพิวเตอร์ computer crime law
  - โอนเงินทางอิเล็กทรอนิกส์ e-funds transfer law
  - พัฒนาโครงสร้างพื้นฐานสารสนเทศ national information infrastructure law

อาชญากรรมคอมพิวเตอร์

(computer crime หรือ cyber crime)

- การกระทำผิดกฎหมายโดยใช้คอมพิวเตอร์เป็นเครื่องมือ
  - การโจรกรรมข้อมูลบริษัท การบิดเบือนข้อมูล การถอดรหัส การก่อกวน เช่น ไวรัส
- แหล่งที่ถูกโจมตีมากที่สุด คือ internet
- อาชญากรคอมพิวเตอร์
  - Hacker คนที่ลักลอบเข้าไปยังเครื่องคอมพิวเตอร์อื่นโดยผ่านเครือข่าย เพื่อทดลองความสามารถ หรือ การอวดอ้าง
  - cracker คือ hacker ที่ทำไปเพื่อผลประโยชน์ในทางธุรกิจ
  - Hacktivist หรือ cyber terroist คือ hacker ที่ทำไปเพื่อผลประโยชน์ทางการเมือง

การใช้คอมพิวเตอร์ในฐานะเป็นเครื่องมือการก่ออาญชกรรม

- การขโมยหมายเลขบัตรเครดิต credit card theft
  - ถูกขโมยผ่านทางอิเล็กทรอนิกส์จะรู้เมื่อได้รับใบแจ้งยอดหนี้
  - การชำระสินค้าด้วยบัตรเครดิตผ่านทาง internet ต้องแน่ใจว่ามีความปลอดภัย โดยสังเกตรูปกุญแจ หรือ ที่ url จะเป็น https://
- การแอบอ้าง identity theft
  - ใช้ข้อมูลส่วนตัวของบุคคลอื่นในการแอบอ้างเป็นบุคคลนั้น เช่น ใช้เปลี่ยนแปลงชื่อเจ้าของ website
- การสแกมทางคอมพิวเตอร์ scam คือใช้คอมพิวเตอร์เป็นเครื่องมือในการหลอกลวงผู้อื่น
  - การส่งข้อความ บอกว่าสามารถใช้บริการได้ราคาถูกแต่ในความเป็นจริงไม่ใช่ ดังนั้นต้องมีการตกลงเป็นลายลักษณ์อักษร
  - การให้เข้าไปใช้บริการเว็บไซต์ได้ฟรี แต่ต้องมีการระบุหมายเลขบัตรเครดิต ซึ่งจะถูกเรียกเก็บเงินในภายหลัง

คอมพิวเตอร์ในฐานะของเป้าหมายอาชญากรรม

- การเข้าถึงและการใช้งานโดยไม่ได้รับอนุญาต
  - การขโมยรหัสส่วนตัว เพื่อก่อให้เกิดความเสียหายแก่บุคคลหรือองค์กร
- การก่อกวนหรือทำลายข้อมูล
  - แทรกแซงการทำงานของ HW และ SW ได้แก่ ไวรัส การปฏิเสธการให้บริการ ข่าวหลอกลวง
- การขโมยข้อมูลและอุปกรณ์คอมพิวเตอร์
  - ใช้กล้องวงจรปิด ใช้กุญแจล็อค ใช้สัญญาณกันขโมย การใช้รหัสผ่านเพื่อควบคุม harddisk

Virus

- ดัดแปลงการทำงานของโปรแกรมอื่น
- ความเสียหาย
  - แสดงข้อความรบกวนหรือทำให้คอมพิวเตอร์ทำงานช้าลง
  - ทำลายการทำงานของระบบคอมพิวเตอร์ เช่น ลบไฟล์ ปิดเครื่อง หรือรบกวนการทำงานของโปรแกรมอื่น เช่น โปรแกรม word

ชนิดของ virus

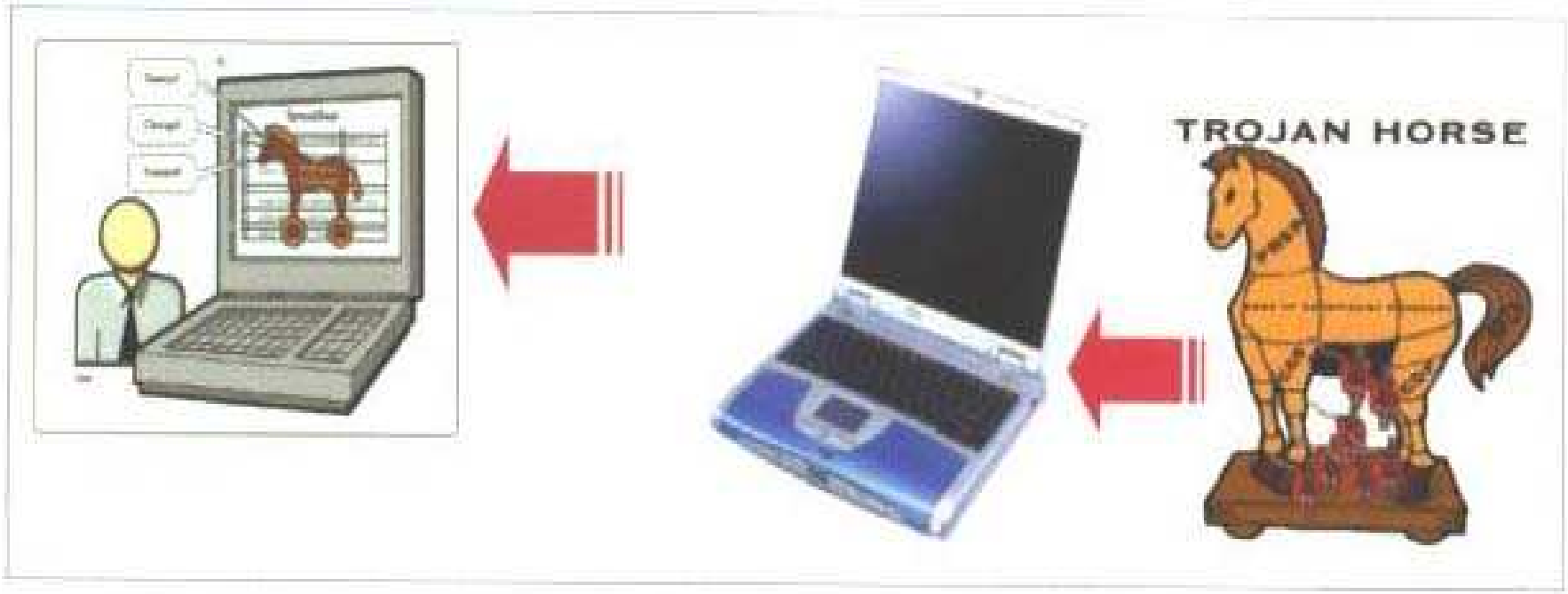
- ทำงานเมื่อเปิดเครื่องหรือเรียกโปรแกรม
  - ทำงานบน boot sector หรือ system virus ฝังตัวที่ boot sector ของดิสก์และหน่วยความจำของเครื่อง ทำงานเมื่อเปิดเครื่อง
  - ติดมากับแฟ้มงานหรือโปรแกรม ฝังตัวอยู่ต่างๆไฟล์ต่างๆ ส่วนใหญ่เป็นไฟล์ .exe และ .com เพราะเรียกใช้บ่อย มักมากับการ download file หรือเปิดไฟล์ที่แนบมากับอีเมล์
  - Macro virus ทำงานบนโปรแกรมที่มีการยอมให้ใช้ภาษา macro เช่น word excel
- ทำงานตามกำหนดเวลาที่ตั้งไว้
  - Logic bomb หรือ time bomb เช่น michelangelo ที่ทำลายข้อมูลทุกวันเกิดของไมเคิลแอนเจลโล

เวริ์ม Worm

- แตกต่างจากไวรัส ตรงที่สามารถแพร่กระจายตัวเองจากคอมพิวเตอร์เครื่องหนึ่งไปยังเครื่องคอมพิวเตอร์อื่นโดยผ่านระบบเครือข่าย
  - ค้นหาที่อยู่ของเครื่องอื่นผ่านทางระบบเครือข่ายแล้วทำการคัดลอกตัวเองส่งไปยังเครื่องอื่น
  - เช่น Nimda W32.blaster ที่ทำการค้นหา e-mail address ในเครื่องที่ติด แล้วทำการส่ง e-mail ที่มีไฟล์แนบเป็น worm ส่งไปให้ตาม e-mail address ที่ได้มา

Trojan Horse

- ไม่มีการแพร่กระจายไปยังเครื่องอื่น จะแฝงตัวมากับโปรแกรมอื่นๆ ที่ส่งมา เช่น



Hoax

- ข่าวหลอกลวง เป็นการส่งข้อความต่อๆ กันเหมือนจดหมายลูกโซ่เพื่อให้เกิดความเข้าใจผิด โดยอาศัยเทคนิคทางจิตวิทยาเพื่อให้เกิดความน่าเชื่อถือ
- เช่น โปรดอย่าใช้มือถือยี่ห้อ..... เครื่องดื่มยี่ห้อ.....เป็นอันตราย

Denial of service

- DoS การทำให้ระบบคอมพิวเตอร์ปฏิเสธการให้บริการ
- ทำการเข้าไปยังระบบคอมพิวเตอร์ที่ไม่ใช้เป้าหมายหลัก เพื่อเปลี่ยนระบบให้กลายเป็นตัวแทน agents หรือ ทาส zombies or slaves และให้ระบบคอมพิวเตอร์ที่เป็น ทาส ทำการส่งการขอใช้บริการจำนวนมากพร้อมๆ กันไปยังระบบคอมพิวเตอร์เป้าหมายเพื่อทำให้ระบบไม่สามารถให้บริการได้ ต้องปิดบริการ
- มักใช้กับเว็บไซต์ที่ให้บริการทางธุรกิจ เช่น ping of death ที่โจมตี amazon.com CNN.com

ข้อสังเกตเกี่ยวกับการได้รับไวรัสคอมพิวเตอร์

- มีข้อความหรือภาพแปลกๆ แสดงบนจอภาพ
- มีเสียงผิดปกติหรือเสียงเพลงเปิดขึ้นเป็นบางเวลา
- หน่วยความจำคอมพิวเตอร์ลดน้อยลงกว่าที่ควรจะเป็น
- โปรแกรมหรือไฟล์หายไป โดยที่ไม่ได้ลบทิ้ง
- มีโปรแกรมแปลกปลอมเข้ามา
- ขนาดของไฟล์ใหญ่ผิดปกติ
- ทำงานของไฟล์หรือโปรแกรมผิดปกติจากเดิม

การป้องกันการเข้าถึงข้อมูลและคอมพิวเตอร์

- การใช้ username และ password
- การใช้วัตถุใดๆ เพื่อการเข้าสู่ระบบ ได้แก่ บัตร กุญแจ
  - การใช้บัตร ATM ควบคู่กับ PIN 4 หลัก(personal identification number)
- การใช้อุปกรณ์ทางชีวภาพ (biometric devices)
  - เสียง ลายนิ้ว ฝ่ามือ ลายเซ็นต์ ม่านตา รูปหน้า โดยแปลงลักษณะบุคคลให้อยู่ในรูปดิจิตัลที่สามารถเปรียบเทียบได้
- ระบบเรียกกลับ callback system
  - ผู้ใช้ระบุชื่อและรหัสผ่านเพื่อขอใช้ระบบปลายทาง ถ้าข้อมูลถูกต้องระบบจะเรียกกลับให้เข้าใช้งานเอง

ข้อควรระวังก่อนเข้าไปใช้งานเครือข่าย

- ป้องกันการถูกขโมยคอมพิวเตอร์ด้วยการล็อก
- ป้องกันการทำลายข้อมูลด้วยการทำสำรอง (backup)

ข้อควรระวังเมื่อเข้าไปใช้งานเครือข่าย

- บัตรเครดิตและการแอบอ้าง
  - ให้เฉพาะบริษัทที่ไว้ใจ เข้าเฉพาะ https:// รหัสผ่านอย่างน้อย 10 ตัว
- ป้องกันข้อมูลส่วนบุคคล
  - ให้เฉพาะที่จำเป็น
- ป้องกันการติดตามเว็บไซต์
  - ใช้โปรแกรม SurfSecret เพื่อป้องกันการติดตามการท่องเว็บไซต์
- หลีกเลี่ยงสแปมเมล
  - ระวังเรื่องการลงทะเบียนเพื่อรับข่าวสาร
- ป้องกันระบบคอมพิวเตอร์และเครือข่าย
  - การใช้ Firewall ที่เป็น HW หรือ SW เพื่อตรวจสอบการเข้าระบบ เช่น McAfee Personal Firewall , Norton Internet Security

ข้อควรระวังเมื่อเข้าไปใช้งานเครือข่าย (ต่อ)

- การป้องกันไวรัสคอมพิวเตอร์ ด้วยเคล็ดลับแบบ EMAIL
  - Exempt from unknown ไม่เปิด e-mail จากคนแปลกหน้า
  - Mind the subject สังเกตหัวจดหมายก่อนเปิดอ่าน
  - Antivirus must be install ติดตั้งโปรแกรมป้องกันไวรัส เช่น norton antivirus , PC-cillin, Dr.solomon
  - Interest on virus news ให้ความสนใจเกี่ยวกับข่าวสารไวรัส
  - Learn to be cautious ให้ระวังให้มาก อย่าเปิดอีเมลล์แบบไม่ยั้งคิด
- ติดตามข่าวสารเกี่ยวกับการป้องกันการก่อกวน ได้ที่ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์แห่งประเทศไทย http://thaicert.nectec.or.th

การสร้างสังคมและรักษาสิ่งแวดล้อม

- ป้องกันไม่ให้เด็กเข้าไปดูเว็บไซต์ที่ไม่เหมาะสม
  - Web filtering software
- วางแผนเพื่อจัดการกับเครื่องคอมพิวเตอร์ที่ไม่ใช้แล้ว
  - บริจาคให้โรงเรียน เอาส่วนประกอบบางส่วนไปขายใหม่ในราคาถูก
- การใช้พลังงาน
  - กำหนดเป็น sleep mode