จริยธรรมและความปลอดภัย ของระบบสารสนเทศ

การขยายขีดความสามารถของ Transaction Web

- พ.ร.บ.ว่าด้วยธุรกรรมอิเล็กทรอนิกส์ พ.ศ.2544 (ธุรกรรมอิเล็กทรอนิกส์ + ลายมือชื่อ digital signature)

การขยายขีดความสามารถของ Transaction Web

- ความเชื่อมั่น ความวางใจ (Trust & Confidence)
  - ระบบความปลอดภัย (ระหว่างทางจะมีใครมาดึงข้อมูล?)
  - เทคโนโลยีด้านการเข้ารหัส
  - การคุ้มครองข้อมูลส่วนบุคคล

ประเด็นจริยธรรมและกฎหมาย

1) ความเป็นส่วนตัว (privacy)

การเก็บรวบรวม การเก็บรักษา และการเผยแพร่ข้อมูล/สารสนเทศเกี่ยวกับปัจเจกบุคคล

ประเด็นจริยธรรมและกฎหมาย

- การใช้อุปกรณ์อิเล็กทรอนิกส์ในการตรวจจับ หรือเฝ้าดูพนักงาน หรือการเก็บข้อมูลของลูกค้า ณ จุดขาย
- ข้อมูล/สารสนเทศใดบ้างที่สามารถเปิดเผยแก่ผู้อื่น
- การใช้ข้อมูลเกี่ยวกับลูกค้าในการให้บริการ ด้านการตลาดเพิ่มเติม
- Junk e-mail

แนวทางการป้องกัน

- ควรเก็บข้อมูลเพื่อใช้ในการดำเนินงานเพื่อบรรลุวัตถุประสงค์ทางธุรกิจ (ถูกต้องตามก.ม.)
- ปัจเจกบุคคลต้องให้ความยินยอม
- บุคคลที่สามไม่ควรได้รับอนุญาต

แนวทางการป้องกัน

- ตัวอย่างความเป็นส่วนตัว เช่น การส่งข้อสอบทางอีเมล์ การแจ้งผลการสอบที่แสดงเฉพาะชื่อหรือเลขรหัสเท่านั้น

ประเด็นจริยธรรมและกฎหมาย

2) ความถูกต้อง (accuracy)

ความถูกต้องของการเก็บและวิธีการปฏิบัติกับข้อมูล/สารสนเทศ

ประเด็นจริยธรรมและกฎหมาย

- ใครเป็นผู้รับผิดชอบต่อความถูกต้องของข้อมูลที่จัดเก็บ

  (ตัวอย่างเช่น สาธิต ม.เกษตรฯ ให้ผู้ปกครองบันทึกข้อมูลเอง)

- จะมั่นใจได้อย่างไรว่าข้อมูลมีความถูกต้อง

แนวทางการป้องกัน

- ข้อมูลควรได้รับการตรวจสอบก่อนนำเข้าฐานข้อมูล
- ข้อมูลต้องมีการปรับปรุงให้ทันสมัย
- แฟ้มข้อมูลควรทำให้บุคคลเข้าถึงและตรวจสอบความถูกต้องได้
- ตัวอย่างเช่น คะแนนที่ป้อนจะต้องไม่ถูกเปลี่ยนแปลง

ประเด็นจริยธรรมและกฎหมาย (ต่อ)

3) ความเป็นเจ้าของ (property)

กรรมสิทธิ์ในการถือครอง

- ใครเป็นเจ้าของข้อมูล/สารสนเทศ

- มาตรการในการจัดการผู้ละเมิด

- เจ้าของควรได้รับการตอบแทนอย่างไร

ความเป็นเจ้าของ (ต่อ)

ลิขสิทธิ์ (copyright) เช่น งานเขียน งานศิลปะ (50 ปี)

สิทธิบัตร (patent) เช่น สิ่งประดิษฐ์ การออกแบบต่างๆ (20 ปี)

Copyright ซื้อลิขสิทธิ์

Shareware ทดลองใช้ก่อนซื้อ

Freeware ใช้ คัดลอก share

ประเด็นจริยธรรมและกฎหมาย (ต่อ)

4) การเข้าถึงข้อมูล (data accessibility)

สิทธิในการเข้าถึงข้อมูล/สารสนเทศ

- ใครควรได้รับอนุญาต

- การขออนุญาตจะต้องเสียค่าใช้จ่ายเท่าไร

แนวทางป้องกัน

- กำหนดระบบรักษาความปลอดภัย

อาชญากรรมคอมพิวเตอร์
(Computer crime or Cybercrime)

การกระทำที่ผิดกฎหมายโดยการใช้คอมพิวเตอร์หรือการทำลายระบบคอมพิวเตอร์

1. การเข้าถึงและการใช้คอมพิวเตอร์ที่ผิดกฎหมาย
   - Hacker คือบุคคลที่ใช้ความรู้ความสามารถในทางที่ไม่ถูกต้อง / ผิดกฎหมาย

อาชญากรรมคอมพิวเตอร์

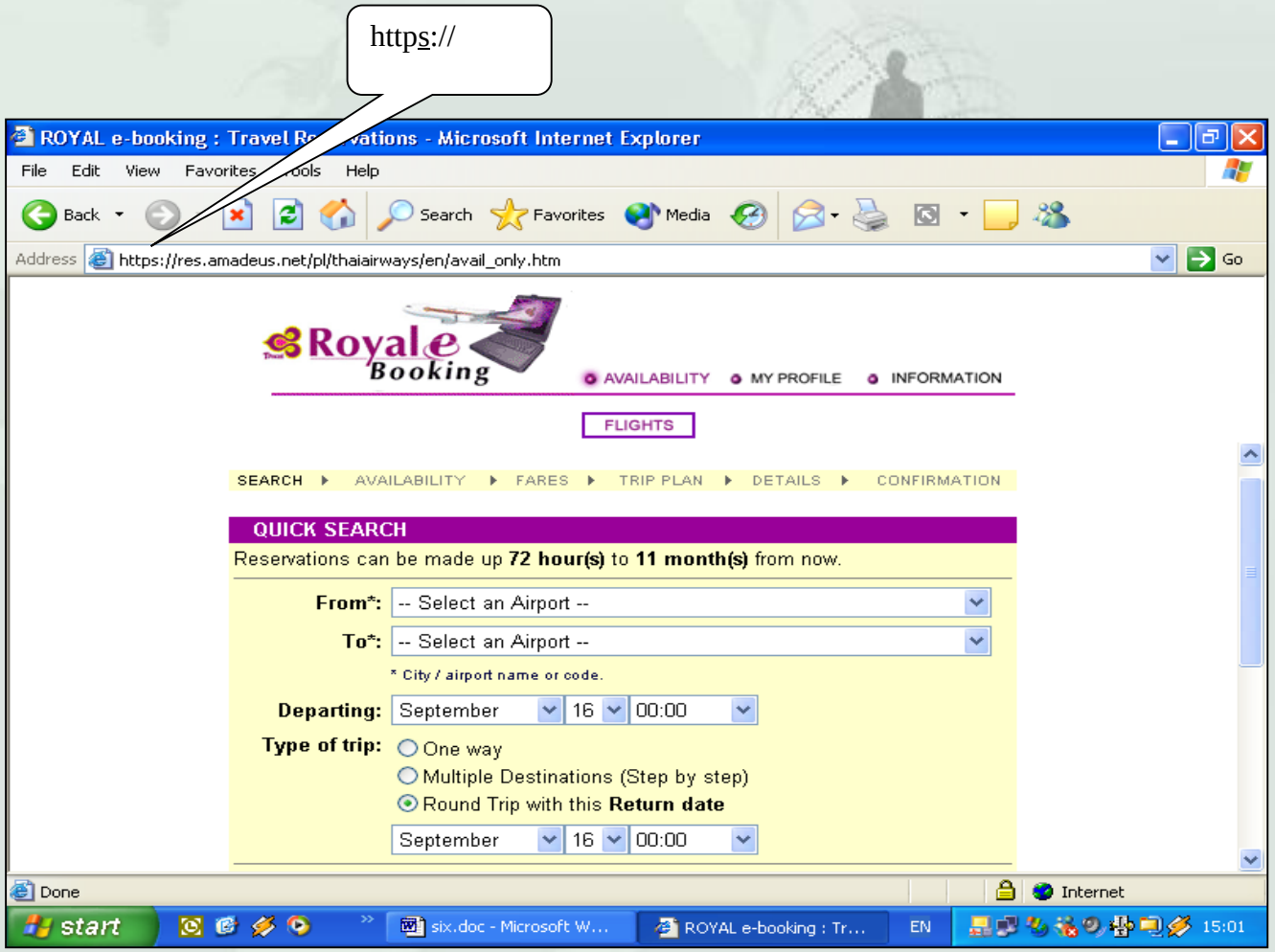
(Computer crime or Cybercrime)

- Cracker คือบุคคลที่ลักลอบเข้าไปยังคอมพิวเตอร์ของผู้อื่น เพื่อวัตถุประสงค์ในเชิงธุรกิจ
- Hacktivist or cyber terrorist ได้แก่ บุคคลที่ใช้อินเทอร์เน็ตในการส่งข้อความเพื่อประโยชน์ทางการเมือง)

การใช้คอมพิวเตอร์ในฐานะเป็นเครื่องมือในการก่ออาชญากรรม

- การขโมยเลขบัตรเครดิต : เมื่อซื้อสินค้าและชำระเงินด้วยบัตรเครดิตผ่านทางอินเทอร์เน็ต จะต้องแน่ใจว่ามีระบบรักษาความปลอดภัย ที่อยู่เว็บไซต์หรือ URL จะระบุ https://

ตัวอย่างเว็บไซต์ที่มีระบบรักษาความปลอดภัย



© 2004 by Prentice Hall

การใช้คอมพิวเตอร์ในฐานะเป็นเครื่องมือในการก่ออาชญากรรม

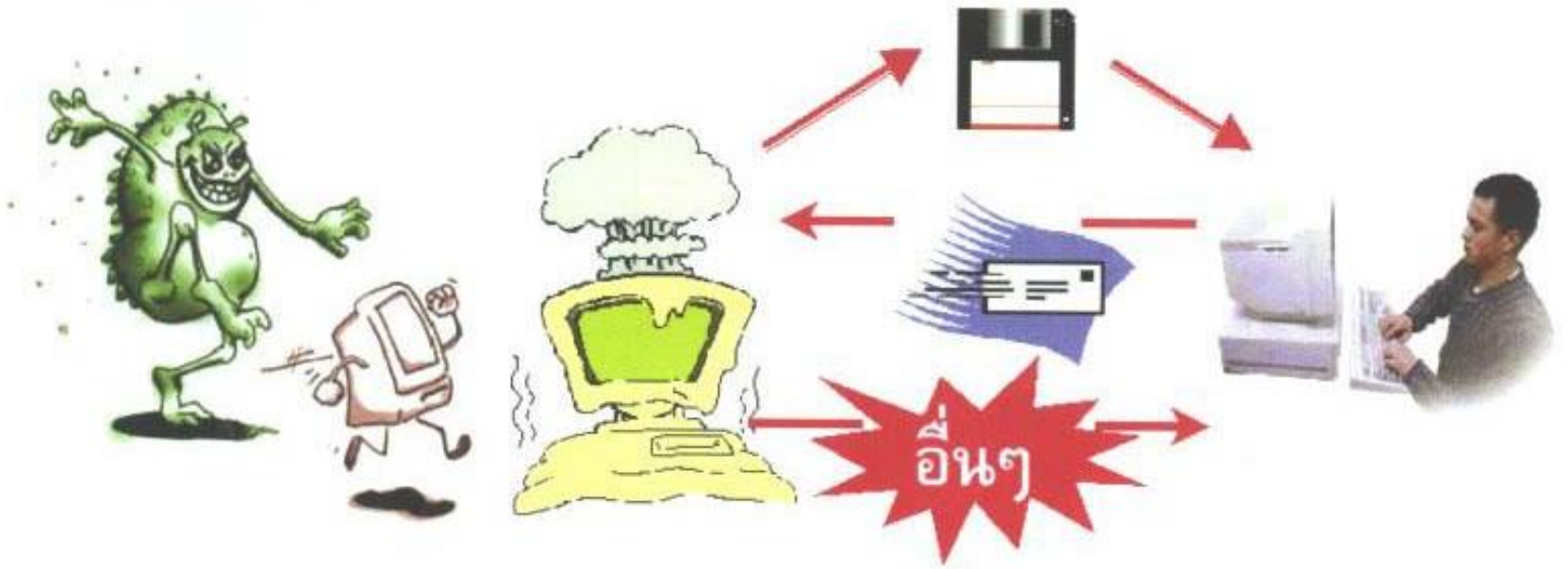
- การแอบอ้างตัว
- **การสแกมทางคอมพิวเตอร์**

อาชญากรรมคอมพิวเตอร์

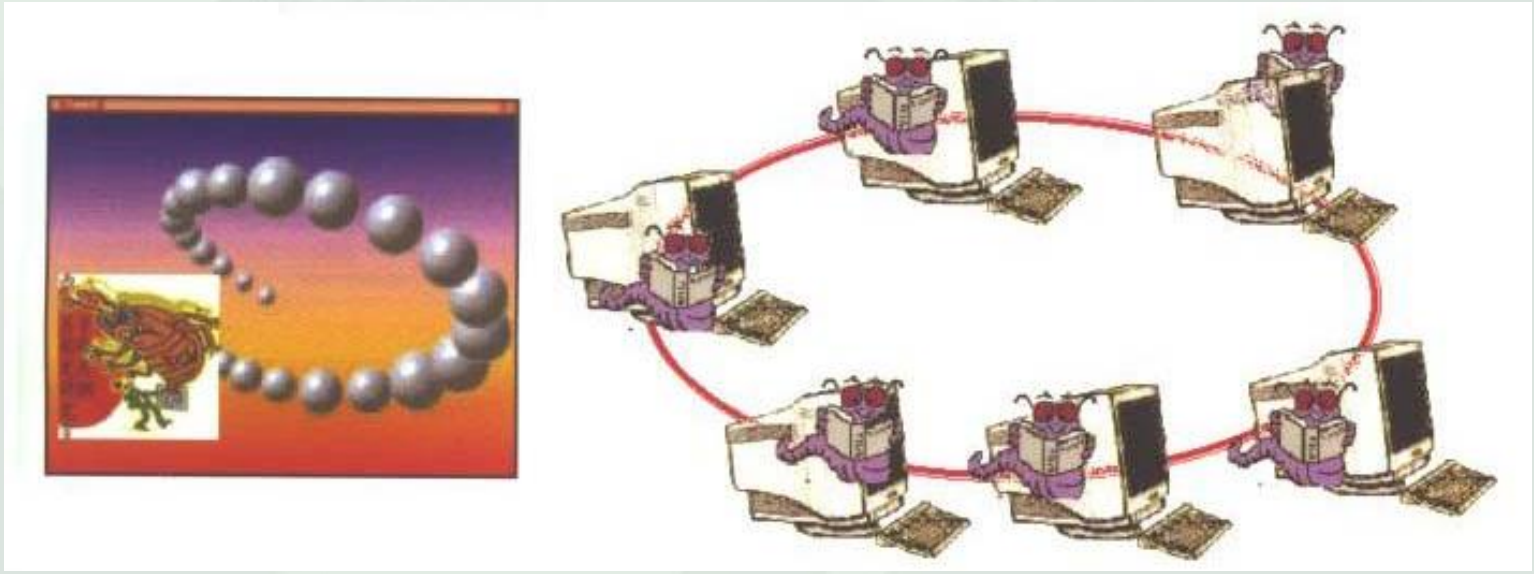
2. การเปลี่ยนแปลงและทำลายข้อมูล : ทำให้การทำงานล่าช้า ข้อมูลเสียหาย

- ไวรัสคอมพิวเตอร์ (การทำงานร่วมกับโปรแกรมอื่น) code red, michelangelo, nimda
- Worm (จำลองตัวเอง) เช่น Love Bug
- logic bomb (ทำงานตามวัน-เวลาที่กำหนด)

ไวรัสคอมพิวเตอร์



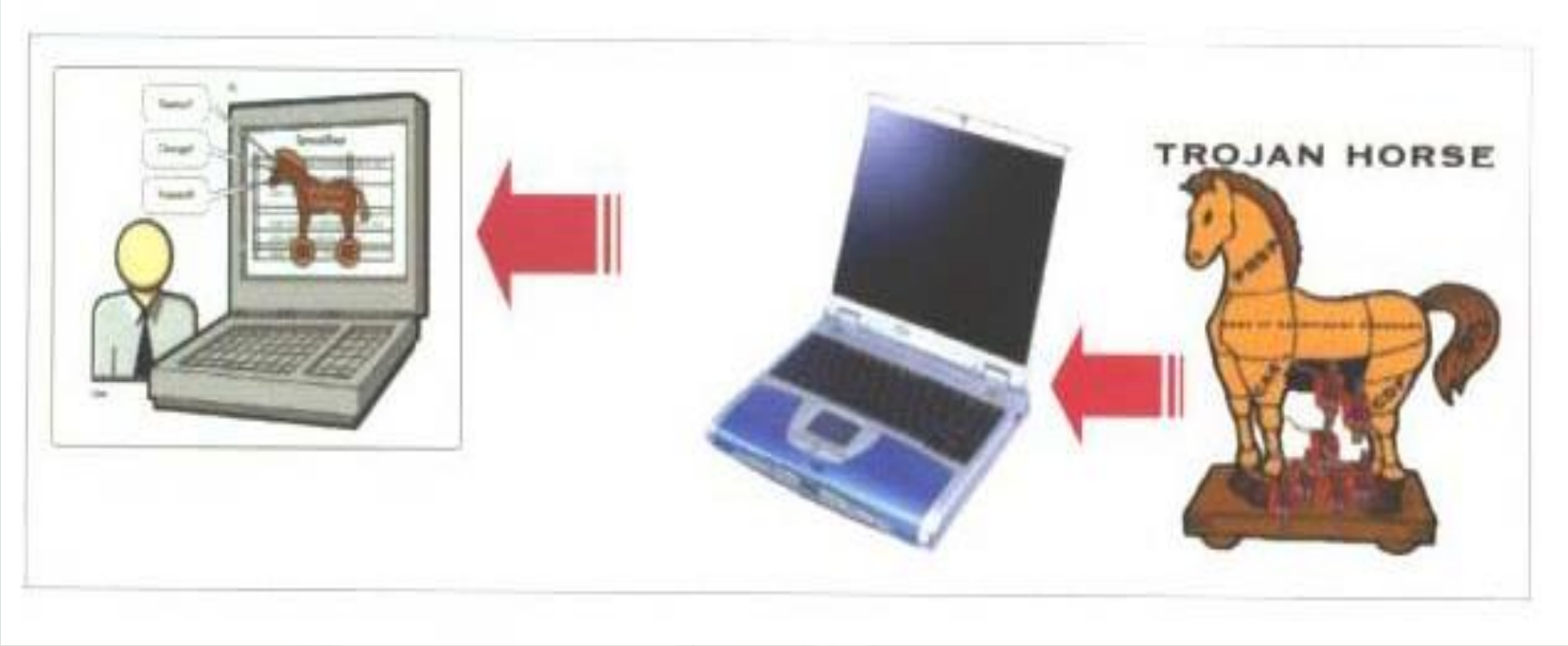
ตัวอย่างการทำงานของเวิร์ม



อาชญากรรมคอมพิวเตอร์

- Trojan horse (การฝังรหัสมากับโปรแกรมที่มีลิขสิทธิ์)
- Hoax (ข่าวหลอกลวง)

ตัวอย่างการทำงานของม้าโทรจัน



อาชญากรรมคอมพิวเตอร์

- Denial-of-Service (การทำให้ระบบปฏิเสธการให้บริการ)
- การขโมยอุปกรณ์คอมพิวเตอร์

ตัวอย่างการป้องกันการขโมยอุปกรณ์คอมพิวเตอร์

อาชญากรรมคอมพิวเตอร์

ที่มาของไวรัส:

- Shareware – freeware
- Software packages
- E-mail
- Network
- คน – พนักงาน ผู้ก่อการร้าย สายลับ

อาชญากรรมคอมพิวเตอร์ (ต่อ)

3. การขโมยข้อมูล/ข่าวสาร

- credit card
- ข้อมูลทางการค้า การเมือง

4. การสแกมทางคอมพิวเตอร์ (scams)

- การหลีกเลี่ยงการเสียภาษี การเสนอข้อมูลที่บิดเบือน เช่น ธนาคาร หุ้น

"ตัวเสี่ยง"

- ผู้ที่ไม่ได้รับอนุญาต
  - เอาข้อมูลอีเมล์มาแจกพวกส่งเมล์ขยะ
- ผู้รับอนุญาต แต่ทำงานไม่ระมัดระวัง
  - แปะ password ไว้บนเครื่อง
  - ไม่เคย backup แฟ้มใดๆ
- พวกอยากรู้อยากเห็น
  - เจาะระบบเล่นอยากลอง
  - ขโมยข้อมูลในเครื่อง
- พวกชอบแกล้งชาวบ้าน
  - เปลี่ยน password
  - เน้นเรื่องทำลายข้อมูล
- ไวรัส
  - โปรแกรมที่คัดลอกตัวเองไปที่อื่นได้ และอาจทำลายข้อมูล
- ภัยธรรมชาติ

ข้อพึงปฏิบัติเพื่อการระวังและป้องกัน

- การให้ข้อมูล โดยเฉพาะบัตรเครดิต และอีเมล์ (การสมัครใจให้ข้อมูลเมื่อมีโปรโมชัน หรือการลงทะเบียนผ่านเว็บ)
- แนวทางการป้องกัน (อะไรต้องป้องกัน ป้องกันจากอะไร และป้องกันอย่างไร)

  - ตรวจสอบสิทธิการใช้ (การใช้รหัสผ่าน)

  - การสังเกตรูปกุญแจ และ https://

ข้อพึงปฏิบัติเพื่อการระวังและป้องกัน

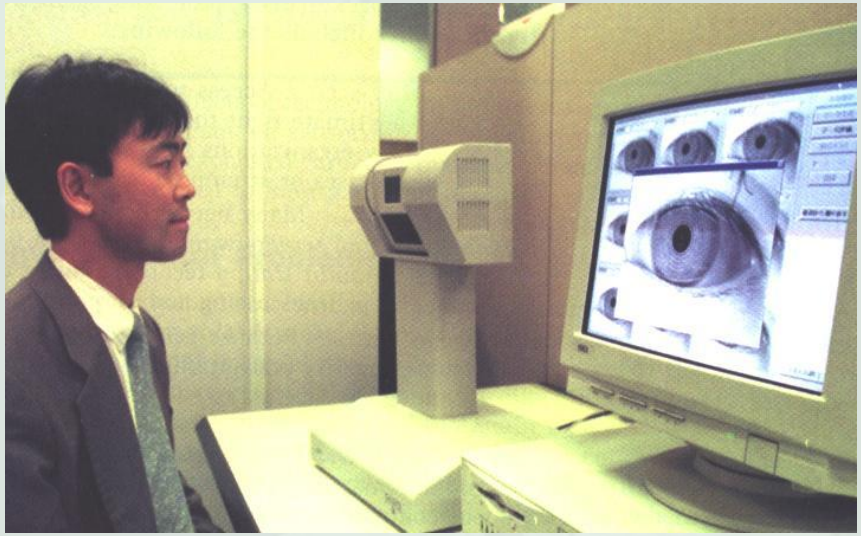
- ติดตั้ง anti-virus เช่น Norton (www.symantec.com) หรือ McAfee (www.mcafee.com)
- การ write protect และ การทำ backup ข้อมูล
- การล็อกเครื่องคอมพิวเตอร์

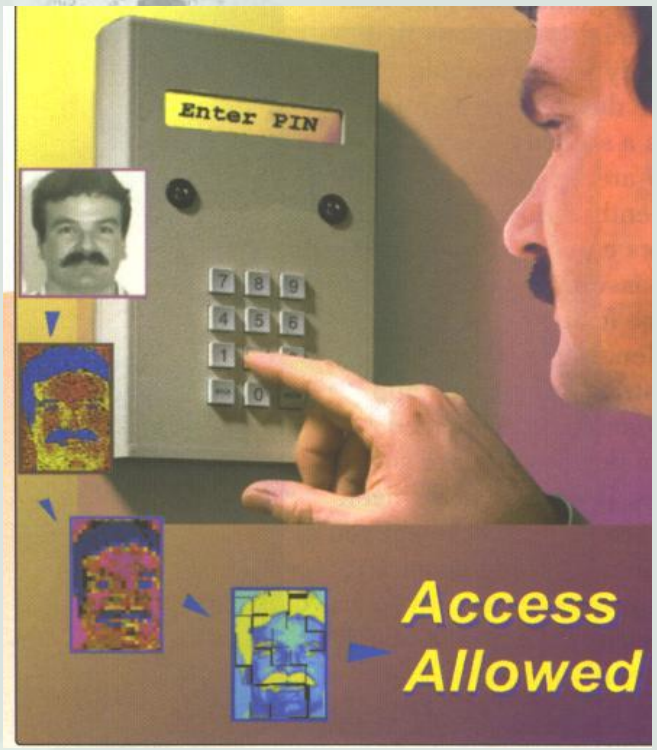
ข้อพึงปฏิบัติเพื่อการระวังและป้องกัน

- การจดลิขสิทธิ์
- การใช้วัตถุใด ๆ เพื่อการเข้าสู่ระบบ เช่น บัตร หรือกุญแจ
- การใช้อุปกรณ์ทางชีวภาพ (biometric device)
- การใช้ระบบเรียกกลับ (callback system)

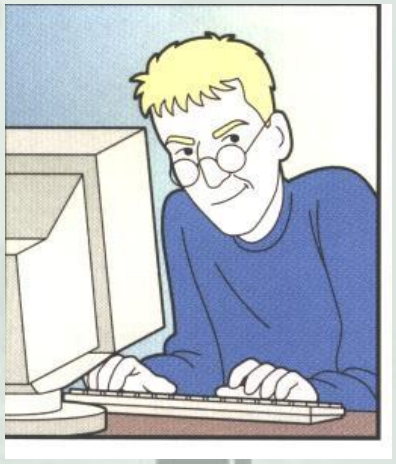
รูปแบบการป้องกันอาชญากรรมคอมพิวเตอร์

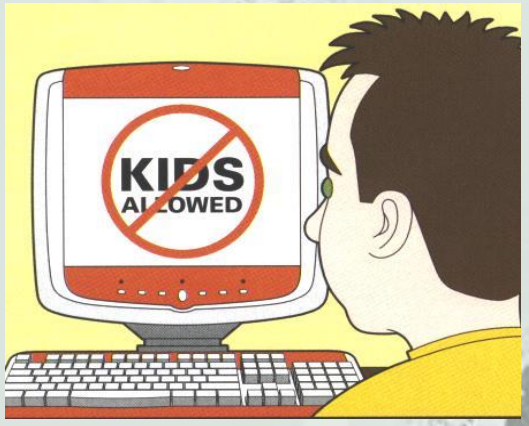
รูปแบบการป้องกันอาชญากรรมคอมพิวเตอร์ (ต่อ)

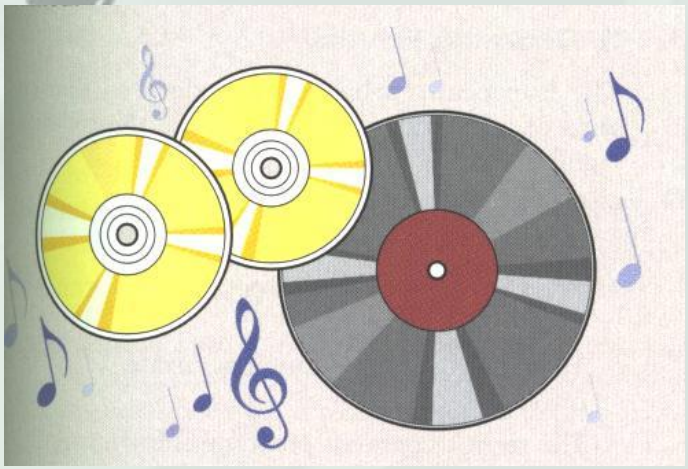




รูปแบบการป้องกันอาชญากรรมคอมพิวเตอร์ (ต่อ)







บทสรุป

- เทคโนโลยีเป็นเครื่องมือของการเรียนรู้ ขณะเดียวกันก็สามารถบั่นทอนความรู้ได้
- ผู้บริหารต้องเข้าใจความเสี่ยง --ป้องกัน – หาแนวทางแก้ไข
- การกำหนดนโยบายเกี่ยวกับจริยธรรมการใช้เป็นสิ่งจำเป็น