



จริยธรรมและความปลอดภัย ในระบบคอมพิวเตอร์



บุคลากรในแวดวงคอมพิวเตอร์/ไอที

บุคลากรคอมพิวเตอร์ หมายถึง ผู้ที่เกี่ยวข้องกับการใช้งาน การดูแลและควบคุมระบบคอมพิวเตอร์ อาจเป็นบุคคลเดี่ยวหรือ กลุ่มบุคคล ตามการจัดแบ่งโครงสร้างขององค์กร ซึ่งแบ่งได้เป็น 3 กลุ่มใหญ่ๆ คือ

- ผู้ใช้งาน
- ผู้ดูแลระบบ
- ผู้ปฏิบัติงาน

บุคลากรในแวดวงคอมพิวเตอร์ / ไอที

❖ ผู้ใช้งาน

- จะเป็นบุคคลที่เข้าถึงสารสนเทศที่ได้จากระบบคอมพิวเตอร์ไปใช้ เช่น
 - รายงานลูกค้าค้างชำระ
จะเป็นสารสนเทศที่ส่งให้พนักงานฝ่ายสินเชื่อเพื่อนำไปใช้ติดตามเก็บเงินจากลูกค้า
 - รายงานสรุปผลยอดการขาย
จะถูกส่งให้ผู้บริหารระดับสูง เพื่อใช้ในการตัดสินใจในการลงทุนผลิตผลิตภัณฑ์

บุคลากรในแวดวงคอมพิวเตอร์ / ไอที

❖ ผู้ดูแลระบบ

- เป็นผู้ควบคุมและพัฒนาโปรแกรม
(**System Programmer and Application Programmer**)
- **System Programmer** เป็นผู้นำหน้าที่ ควบคุมระบบทางด้าน Hardware เช่น ควบคุมเครื่องคอมพิวเตอร์ให้ปฏิบัติงานได้อย่างราบรื่น คอยแก้ไขปัญหาที่อาจเกิดขึ้นในระบบ ขณะปฏิบัติงานของเครื่องคอมพิวเตอร์
- **Application Programmer** สำหรับผู้พัฒนาโปรแกรม จะเป็นบุคคลที่ทำหน้าที่พัฒนาโปรแกรมประยุกต์ต่างๆ เพื่อสั่งให้คอมพิวเตอร์พัฒนาประมวลผล และสร้างสารสนเทศในระบบงานใด ๆ

บุคลากรในแวดวงคอมพิวเตอร์ / ไอที

❖ ผู้ปฏิบัติงาน

- เป็นผู้ที่ทำหน้าที่ นำข้อมูลเข้าสู่ระบบคอมพิวเตอร์
- มีหน้าที่ เรียกใช้งานโปรแกรมประยุกต์ต่าง ๆ
 - เพื่อสั่งให้คอมพิวเตอร์ทำการประมวลผล
 - สร้างสารสนเทศออกมา
 - คอยรับผลลัพธ์จากระบบคอมพิวเตอร์ เพื่อนำส่งให้แก่ผู้ใช้งานต่อไป

บุคลากรในแวดวงคอมพิวเตอร์ / ไอที

มี 5 ประเภท

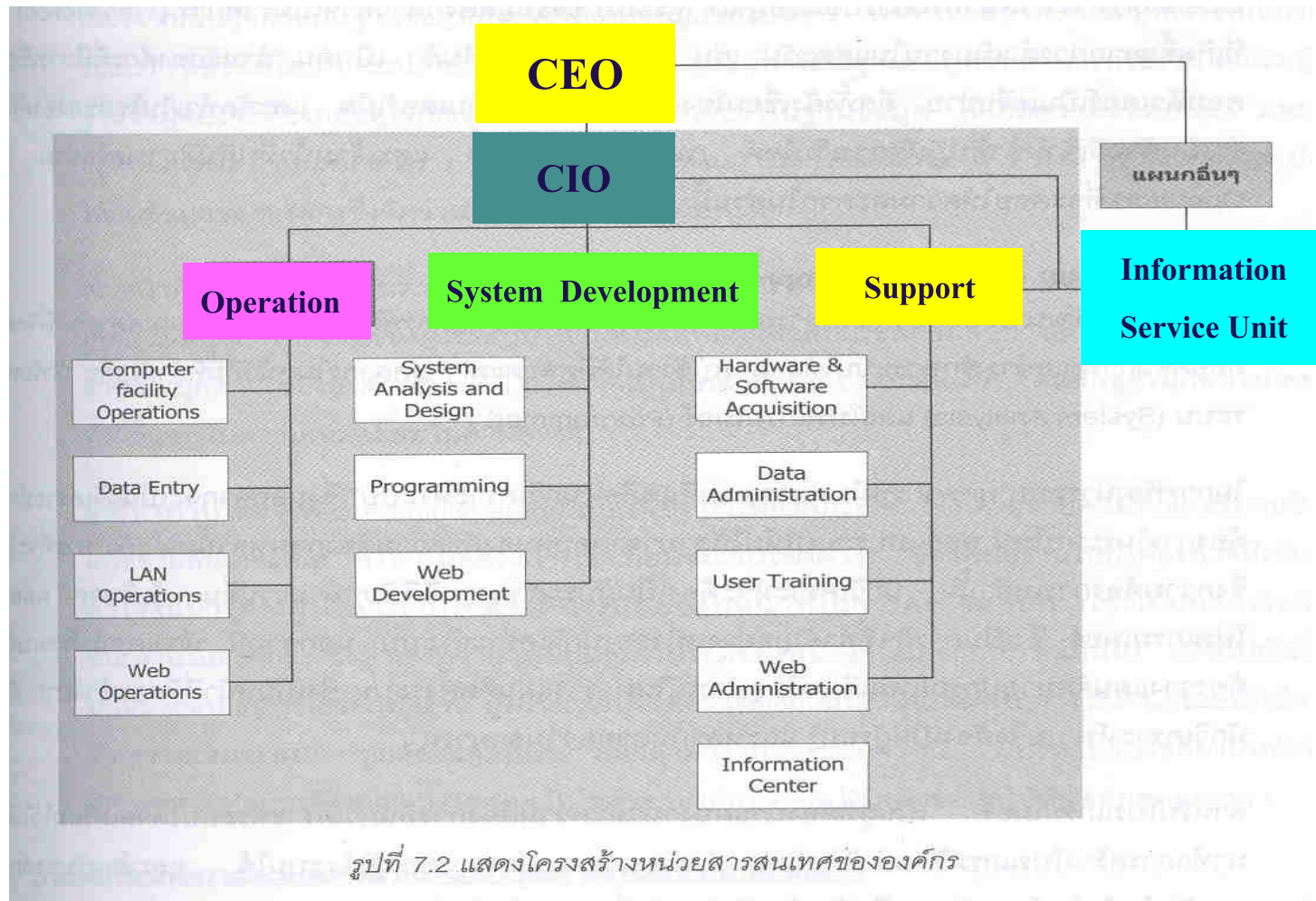
1. ผู้ใช้งานคอมพิวเตอร์ (User)
2. ผู้เขียนโปรแกรมคอมพิวเตอร์ (Programmer)
3. ผู้ดูแลและซ่อมบำรุงเครื่องคอมพิวเตอร์
(Supporter หรือ Technician)
4. ผู้บริหารระบบคอมพิวเตอร์
(System Manager or Administrator)
5. ผู้วิเคราะห์แบบออกแบบระบบคอมพิวเตอร์ (System Analyst)



อาชีพที่เกี่ยวข้องกับคอมพิวเตอร์ / ไอที



1. อุตสาหกรรมการผลิตอุปกรณ์คอมพิวเตอร์
2. อุตสาหกรรมการผลิตซอฟต์แวร์คอมพิวเตอร์
3. อาชีพนักสารสนเทศในหน่วยงานรัฐบาลและเอกชน
4. อาชีพเกี่ยวกับการสอนและฝึกอบรมบุคลากรทางคอมพิวเตอร์
5. อาชีพอื่นในอุตสาหกรรมคอมพิวเตอร์





Information Service Unit

Operation

- Computer Facility Operator
- Data Entry
- LAN Operators
- Web Operators

System Development

- System Analysis and Design
- Programming
- Web Development

Support

- Hardware & Software Acquisition
- Data Administration
- User Training
- Web Administration
- Information Center

12 ตำแหน่ง

❖ คำว่า จริยธรรม แยกออกเป็น จริย + ธรรม

- **จริย** หมายถึง ความประพฤติหรือกิจที่ควรประพฤติ
- **ธรรม** มีความหมายหลายประการ เช่น คุณความดี, หลักคำสอนของศาสนา, หลักปฏิบัติ
- เมื่อนำคำทั้งสองมารวมกันเป็น “จริยธรรม” จึงมีความหมายตามตัวอักษรว่า “หลักแห่งความประพฤติ” หรือ “แนวทางของการประพฤติ”

❖ พจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ. ๒๕๓๕ ให้คำนิยามว่า จริยธรรม... คือ ธรรมที่เป็นข้อประพฤติปฏิบัติ, ศีลธรรม, กฎศีลธรรม

❖ จริยธรรม เป็นศาสตร์แขนงหนึ่งของปรัชญาที่เกี่ยวข้องกับหลักในการประพฤติปฏิบัติตนของมนุษย์ ที่มุ่งเน้นแต่การทำดี คิดดี

ความหมายของ จริยธรรม (ethics)

- ❖ หลักศีลธรรมจรรยาที่กำหนดขึ้นเพื่อใช้เป็นแนวทางปฏิบัติหรือ ควบคุมการใช้ระบบคอมพิวเตอร์และสารสนเทศ
- ❖ หลักของความถูกต้องและความผิดที่บุคคลใช้เป็นแนวทางในการปฏิบัติ
- ❖ สรุปล เป็นหลักเกณฑ์ที่ประชาชนตกลงร่วมกันเพื่อใช้เป็นแนวทางในการปฏิบัติร่วมกันในสังคม

★ จริยธรรมและกฎหมาย (Ethics and Laws)

ข้อกำหนดในการใช้คอมพิวเตอร์นั้นถูกกำหนดกฎเกณฑ์และสิทธิในการเข้าถึงข้อมูลได้ด้วย 2 วิธี คือ กำหนดด้วยจริยธรรม และ กำหนดด้วยกฎหมาย

จุดประสงค์คือ

- การสร้างความเป็นระเบียบและความเรียบร้อย
- คุ้มครองสิทธิส่วนบุคคลในระบบสารสนเทศ

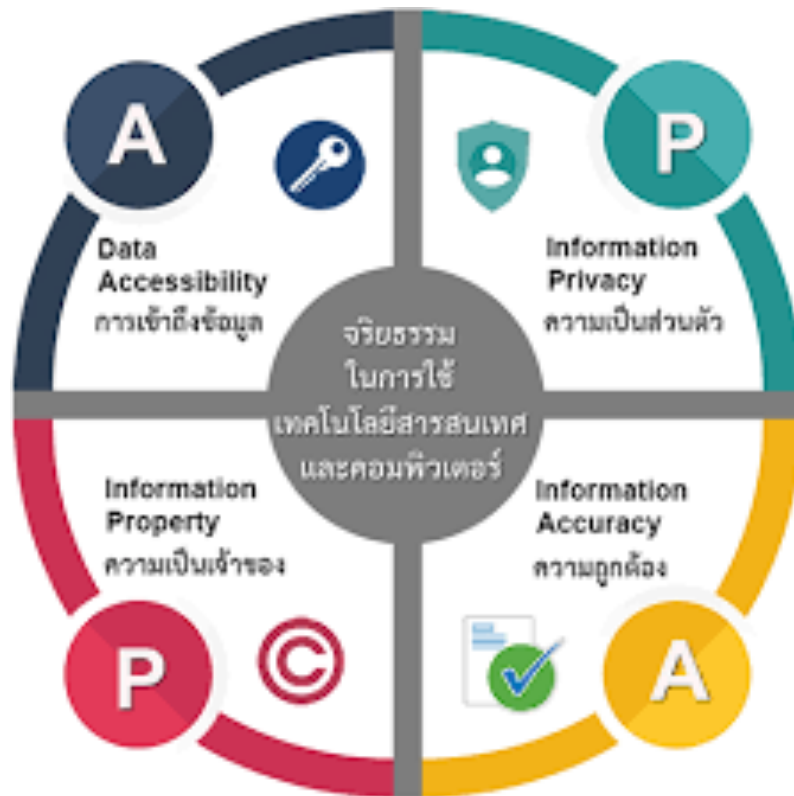
จริยธรรมทางด้านคอมพิวเตอร์

ความแตกต่างระหว่างกฎหมายและจริยธรรม		
หัวข้อ	จริยธรรม	กฎหมาย
หลักการพื้นฐาน	ไม่มีหลักการตายตัว และขึ้นอยู่กับ จิตสำนึกของบุคคลในสังคม	เป็นหลักและกฎเกณฑ์ตายตัว เปลี่ยนแปลงได้ยาก มีความซับซ้อน
ผู้ตัดสินความผิด	บุคคลผู้กระทำ	การตัดสินเป็นไปตามกระบวนการที่ รัฐบาลกำหนดขึ้น
บทลงโทษ	การวิพากษ์วิจารณ์ หรือถูกรังเกียจจาก ผู้คนในสังคม	ปรับ หรือจำคุก หรือทั้งจำทั้งปรับ
การบังคับใช้	ขึ้นอยู่กับสังคมนั้น	ขึ้นอยู่กับสังคมนั้น

4 ประเด็นของจริยธรรม (PAPA)

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

4 ประเด็นของจริยธรรม (PAPA)



- ❖ สิทธิในการควบคุมข้อมูลของตนเองในการเปิดเผยให้กับผู้อื่น
- ❖ การละเมิดความเป็นส่วนตัว
 - เข้าไปอ่าน e-mail, ใช้คอมพิวเตอร์ตรวจจับการทำงานของพนักงาน, รวบรวมข้อมูลส่วนบุคคลสร้างเป็นฐานข้อมูลแล้วเอาไปขาย
 - ทำธุรกรรมผ่านเว็บไซต์เพื่อรวบรวมข้อมูลไปขาย เช่น บริษัท doubleclick ,enage
 - ใช้โปรแกรม sniffer วิเคราะห์อัตราการใช้อินเทอร์เน็ต ติดตามผู้ใช้เพื่อทำการส่ง e-mail ขายนินจาค้า ทำให้เกิด อีเมลขยะ (junk mail) ที่ผู้รับไม่ต้องการ เรียกว่า สปแอม
- ❖ Tool ใช้ในการตรวจจับ spyware ได้แก่ ad-ware , spybot

Information Privacy



คำชี้แจงสิทธิส่วนบุคคลของ MSN

(ปรับปรุงล่าสุด: มกราคม 2547)

MSN มีความมุ่งมั่นอย่างจริงใจที่จะปกป้องความเป็นส่วนตัวของคุณ คำชี้แจงสิทธิส่วนบุคคลของ MSN นี้ มีผลใช้กับ การเก็บรวบรวมและการใช้ข้อมูล บนเว็บไซต์และบริการของ MSN แต่ไม่มีผลกับเว็บไซต์ออนไลน์และ ออฟไลน์ ตลอดจนผลิตภัณฑ์และบริการอื่นๆ ของ Microsoft โปรดอ่าน คำชี้แจงสิทธิส่วนบุคคลของ MSN ด้านล่างนี้ รวมทั้งอ่านข้อมูลเพิ่มเติม ที่ด้านล่างของคำชี้แจงนี้ เพื่อศึกษารายละเอียดเพิ่มเติมเกี่ยวกับเว็บไซต์และบริการบางตัวของ MSN ที่คุณอาจใช้อยู่

MSN เป็นเว็บไซต์สำหรับผู้ชมทั่วไป เหมาะสำหรับผู้ใช้ทุกวัย ข้อมูล ส่วนบุคคลของผู้ใช้จะถูกรวบรวม ใช้ และเปิดเผยดังที่อธิบายใน คำชี้แจงสิทธิส่วนบุคคลนี้ คำชี้แจงนี้มีส่วนหนึ่งที่ระบุนายละเอียด เกี่ยวกับการเก็บข้อมูลส่วนบุคคลของเด็กโดยเฉพาะ คลิก [ที่นี่](#) เพื่ออ่านเพิ่มเติม

บริการอื่นๆ ของ Microsoft ซึ่งเชื่อมโยงไปจากเว็บไซต์นี้ [.NET Passport](#), [MapPoint](#), [bCentral](#) และ [WindowsMedia.com](#) ต่างมีคำชี้แจงสิทธิส่วนบุคคลของตัวเองซึ่งเปิดอ่านได้โดย คลิกที่การเชื่อมโยง

การรวบรวมข้อมูลส่วนบุคคลของคุณ

ในบางเว็บไซต์ MSN จะเก็บรวบรวมข้อมูลส่วนบุคคล เช่น ที่อยู่อีเมล ชื่อ ที่อยู่ หรือหมายเลขโทรศัพท์ที่บ้านหรือที่ทำงาน MSN อาจมีการรวบรวมข้อมูลทางประชากรศาสตร์เช่น รหัสไปรษณีย์ อายุ เพศ สิ่งที่ชอบ ความสนใจ และสิ่งที่โปรดปรานเป็นพิเศษ ข้อมูลที่รวบรวมโดย MSN อาจถูกนำไปรวมกับ ข้อมูลที่ได้จากบริการอื่นๆ ของ Microsoft และจากบริษัทอื่นๆ

ความถูกต้อง Information Accuracy

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

ข้อมูลข่าวสารที่เผยแพร่บนอินเทอร์เน็ต



การสำรวจความคิดเห็นและเผยแพร่ข้อมูลบนเว็บไซต์

Which Cola Giant Do You Prefer?

Cast your vote below and let the world know what you think



Total Votes: 29205



15528 Votes
(53%)



13677 Votes
(47%)

ข้อมูลที่ปราศจาก
การตรวจสอบ

ความเป็นเจ้าของ Intellectual Property

กรรมสิทธิ์ในการถือครองทรัพย์สิน 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

ความเป็นเจ้าของ Intellectual Property

orange

■ english

หน้าหลัก | เกี่ยวกับอเรนจ์ | สินค้าและบริการ | มาเป็นลูกค้าอเรนจ์ | พบอเรนจ์ได้ที่ไหน | เครือข่ายของอเรนจ์ | การดูแลลูกค้า | คำแนะนำ

เงื่อนไขการให้บริการ

เงื่อนไขการให้บริการ

คำชี้แจงเกี่ยวกับกฎหมายสำหรับเว็บไซต์ของ อเรนจ์ ในประเทศไทย

1. เครื่องหมายการค้า Orange และ wirefree™ และผลิตภัณฑ์อื่นใดหรือชื่อของบริการของอเรนจ์ ที่ปรากฏหรืออ้างถึงใน orange.co.th เว็บไซต์ เป็นเครื่องหมายการค้าของ Orange Personal Communications Services Limited
2. เนื้อหา (ข้อมูล, การติดต่อสื่อสาร, ภาพ และ เสียง) ที่ปรากฏอยู่ในเว็บไซต์ หรือ มีให้ใช้ได้ในเว็บไซต์ orange.co.th) เป็นสิ่งที่จัดทำขึ้นโดย อเรนจ์, บริษัทในเครือ อเรนจ์, ผู้ให้บริการสร้างเนื้อหาของเว็บไซต์ และ บุคคลที่สาม เนื้อหาของ orange.co.th เป็นลิขสิทธิ์ของ Orange Personal Communications Services Limited หรือบริษัทในเครือ และถือเป็นสิ่งที่สงวนสิทธิ์ทุกประการ ห้ามทำซ้ำ, คัดแปลง, ดัดแปลง, ถ่ายโอน, ถ่ายทอด, แจกจ่าย, ตีพิมพ์ซ้ำ, คาว์ปี้, คัดลอก, ดัดแปลง, หรือการกระจายเสียง/ภาพ/ข้อมูล ไม่ว่าในรูปแบบใดๆ และ/หรือ ไม่ว่าในรูปแบบของสื่ออิเล็กทรอนิกส์ หรือการถ่ายสำเนา หรือการอัปเดตบันทึก เนื้อหาของ orange.co.th โดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรจาก Orange Personal Communications Services Limited ท่านยินยอมรับทราบว่าสิ่งเหล่านี้และเนื้อหาที่อยู่ในสิ่งเหล่านี้ หรือที่ได้รับมาจาก orange.co.th ปรากฏในเว็บไซต์นี้สำหรับให้ท่านใช้เพื่อการส่วนตัวเท่านั้น และไม่อาจนำไปใช้เพื่อวัตถุประสงค์ทางธุรกิจ หรือนำไปแจกจ่ายเพื่อผลทางธุรกิจได้
3. อเรนจ์ จะพยายามอย่างดีที่สุดที่จะรักษาเว็บไซต์ orange.co.th ให้อยู่ในสภาพที่ใช้การได้อย่างสมบูรณ์ แต่ไม่ถือเป็นความรับผิดชอบของอเรนจ์หากเกิดผลอันเกิดจากข้อบกพร่องที่เกิดขึ้นใน เว็บไซต์ orange.co.th ท่านไม่ควรถือว่า เว็บไซต์ orange.co.th หรือเนื้อหาที่อยู่ใน เว็บไซต์นี้ปราศจากข้อผิดพลาดใดๆ หรือถือว่าเนื้อหาเหล่านี้จะเหมาะสมกับวัตถุประสงค์ที่ท่านต้องการเมื่อใช้เนื้อหาเหล่านั้น อเรนจ์ ขอสงวนสิทธิ์ที่จะเปลี่ยนแปลงเนื้อหาของ เว็บไซต์นี้ในภายหลังรวมทั้งขอสงวนสิทธิ์ที่จะปรับเปลี่ยน แทราเลียม หรือยกเลิก บริการใดๆของ อเรนจ์

การแสดงความ
เป็นเจ้าของข้อมูลบนเว็บ
ของผู้ให้บริการ

การละเมิดลิขสิทธิ์ทางซอฟต์แวร์

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

การเข้าถึงข้อมูล Data Accessibility

- ❖ กำหนดสิทธิตามระดับผู้ใช้งาน
- ❖ ป้องกันการเข้าไปดำเนินการต่าง ๆ กับข้อมูลของผู้ที่ไม่เกี่ยวข้อง
- ❖ ต้องมีการออกแบบระบบรักษาความปลอดภัยในการเข้าถึงข้อมูลของผู้ใช้

การเข้าถึงข้อมูล Data Accessibility

 Research Databases

การป้องกันการเข้าถึงข้อมูล
โดยไม่ได้รับอนุญาต

[Athens Users Login](#)

Login [EBSCOhost Support](#)

User ID	
Password	
Login	

จรรยาบรรณในการใช้งานคอมพิวเตอร์

1. จะต้องไม่ใช้คอมพิวเตอร์เพื่อก่ออาชญากรรมหรือละเมิดสิทธิของผู้อื่น
2. จะต้องไม่ใช้คอมพิวเตอร์รบกวนผู้อื่น
3. จะต้องไม่ทำการสอดแนม แก้ไข หรือเปิดดูไฟล์เอกสารของผู้อื่นก่อนได้รับอนุญาต
4. จะต้องไม่ใช้คอมพิวเตอร์ในการโจรกรรมข้อมูล ข้อมูลข่าวสาร
5. จะต้องไม่ใช้คอมพิวเตอร์สร้างหลักฐานเท็จ
6. จะต้องไม่ใช้คอมพิวเตอร์ในการ...คัดลอกโปรแกรมที่มีลิขสิทธิ์
7. จะต้องไม่ใช้คอมพิวเตอร์ใน..การละเมิดการใช้ทรัพยากรคอมพิวเตอร์โดยที่ตนเองไม่มีสิทธิ์
8. จะต้องไม่ใช้คอมพิวเตอร์ เพื่อนำเอาผลงานของผู้อื่นมาเป็นของตนเอง
9. จะต้องคำนึงถึงสิ่งที่จะเกิดขึ้นกับสังคม ที่จะตามมาจากการกระทำนั้น
10. จะต้องใช้คอมพิวเตอร์ โดยการเคารพกฎ ระเบียบ กติกา และมารยาท

ประเด็นที่เกี่ยวกับ จริยธรรมคอมพิวเตอร์ที่สำคัญ

1. ประเด็นด้านทรัพย์สินทางปัญญา

- ไทยมีกฎหมายลิขสิทธิ์ที่ให้ความคุ้มครองโปรแกรมคอมพิวเตอร์แล้ว
- หากใครละเมิด คือนำโปรแกรมที่ไม่ได้ซื้อสิทธิ์การนำมาให้ก็อาจจะเข้าข่ายละเมิด และอาจถูกผู้เป็นเจ้าของลิขสิทธิ์ฟ้องร้องได้
- เวลานี้กลุ่มบริษัทซอฟต์แวร์ต่างประเทศได้ให้สิทธิบนแก่ผู้ที่แจ้งเบาะแสการใช้ซอฟต์แวร์ที่ละเมิด

ประเด็นที่เกี่ยวกับจริยธรรมคอมพิวเตอร์ที่สำคัญ

2. ประเด็นด้านข้อมูล

ข้อมูลคือทรัพย์สินที่สำคัญอย่างหนึ่ง

ท่านจะต้องดูแลข้อมูลของท่านอย่างรอบคอบ

- การดูแลข้อมูล
- การเก็บบันทึกข้อมูลให้ถูกต้อง
- ควบคุมให้ผู้มีสิทธิ์ในการใช้ข้อมูลเท่านั้นที่เข้าถึงข้อมูลได้
- ตรวจสอบว่าใครคือผู้ใช้
- การใช้ข้อมูลนั้นเป็นไปตามหลักเกณฑ์และเงื่อนไขที่กำหนดไว้หรือไม่

3. ประเด็นด้านเครือข่าย สิ่งที่ต้องพิจารณา คือ

- ต้องอย่างให้แฮกเกอร์บุกรุกเข้ามาทำลายโปรแกรมและข้อมูลในระบบของเราได้
- ต้องตรวจสอบการแพร่กระจายของไวรัสคอมพิวเตอร์ ซึ่งปัจจุบันได้เริ่มระบาดมากขึ้นและส่งผลเสียให้แก่ระบบต่าง ๆ อย่างกว้างขวาง
- จะต้องตรวจสอบไม่ให้งานของเราประพัตติตเป็นแฮกเกอร์เสียเอง หรือเป็นผู้สร้างไวรัสแล้วปล่อยออกไปอาละวาดทำลายทรัพย์สินของผู้อื่น

ประเด็นที่เกี่ยวกับจริยธรรมคอมพิวเตอร์ที่สำคัญ

4. ตัวพนักงานเอง

- หน่วยงานและห้างร้านหลายแห่งมักจะปล่อยให้เจ้าหน้าที่คอมพิวเตอร์ทำงานไปตามลำพังเพราะเห็นว่าเป็นงานด้านเทคนิคที่ผู้บริหารไม่เข้าใจ
- การปล่อยปละละเลยเช่นนี้ไม่ถูกต้อง
- จำเป็นที่ผู้บริหารจะต้องตรวจสอบการทำงานของพนักงานว่าได้ทำงานที่เกี่ยวข้องเฉพาะกับเรื่องของหน่วยงานเท่านั้นหรือไม่
- พนักงานทำงานข้างนอกเข้ามาอาศัยสถานที่ทำให้บุคคลอื่น
- พนักงานอาจทำงานอยู่ดี ๆ เพื่ออาศัยระบบอินเทอร์เน็ตสร้างความเดือดร้อนให้แก่ผู้อื่น

ประเด็นที่เกี่ยวกับจริยธรรมคอมพิวเตอร์ที่สำคัญ

5. เอกสารต่าง ๆ ตลอดจนอีเมล

- หน่วยงานห้างร้านต่าง ๆ มักไม่ค่อยเข้มงวดในด้านการรักษาความปลอดภัยของเอกสาร
- อาจเป็นไปได้ว่าเอกสารต่าง ๆ รวมทั้งอีเมลที่สำคัญ ๆ ได้หลุดรอดออกไปถึงผู้ไม่ปรารถนาดี หรือผู้ที่อาจจะดำเนินการร้ายแก่หน่วยงาน
- ผู้เป็นตัวการในด้านนี้ส่วนใหญ่ก็อาจจะเป็นพนักงานซึ่งอาจจะทำไปเพราะจงใจ หรือรู้เท่าไม่ถึงการณ์ก็ได้

กฎหมายเทคโนโลยีสารสนเทศ

❖ ความก้าวหน้าทางเทคโนโลยีสารสนเทศทำให้เกิดการทำธุรกิจแบบให้บริการโดยไม่จำกัดสถานที่และเวลา คือให้บริการแบบ 24x7x365

❖ ปี 2546 ประเทศไทยมีกฎหมาย 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

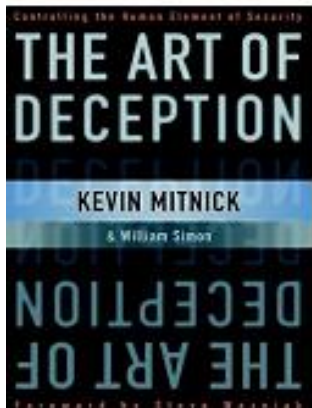
❖ อาชญากรคอมพิวเตอร์

- Hacker คนที่ลักลอบเข้าไปยังเครื่องคอมพิวเตอร์อื่นโดยผ่านเครือข่าย เพื่อทดสอบความสามารถ หรือ การอวดอ้าง
- cracker คือ hacker ที่ทำไปเพื่อผลประโยชน์ในทางธุรกิจ
- สคริปต์คิตตี้ (Script Kiddy)
- Hacktivist หรือ cyber terrorist คือ hacker ที่ทำไปเพื่อผลประโยชน์ทางการเมือง

- ❖ เป็นกลุ่มคนที่มีความรู้ทางด้านคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์เป็นอย่างดี
- ❖ ทำเพื่อต้องการทดสอบความรู้ของตนเอง
- ❖ โดยเจตนาแล้วไม่ได้มีความมุ่งร้ายต่อข้อมูลแต่อย่างใด
- ❖ บางครั้งจึงมักนิยมเรียกว่าเป็นพวก กลุ่มคนหมวกขาว หรือ *white hat*

- ❖ เป็นกลุ่มคนที่มีความรู้ความสามารถเช่นเดียวกับกลุ่มแฮกเกอร์ มักเรียกว่าเป็น *กลุ่มคนหมวกดำ* หรือ *black hat*
- ❖ มุ่งทำลายระบบหรือลักลอบนำเอาข้อมูลที่ไม่ได้รับอนุญาตนั้นไปแก้ไขเปลี่ยนแปลงหรือทำลายทิ้ง
- ❖ มีเจตนาจงใจให้เกิดความเสียหายของข้อมูลมากกว่าแฮกเกอร์
- ❖ เป็นกลุ่มคนที่มีความชำนาญทางด้านคอมพิวเตอร์ ระบบเครือข่าย หรือเขียนโปรแกรม เป็นบุคคลซึ่งถือได้ว่าร้ายแรงที่สุดในปัจจุบัน

เควิน มิตนิก (Kevin Mitnick)



-บุคคลที่เป็นทั้งแฮกเกอร์และแครกเกอร์ในคนเดียว

-ขณะวัยรุ่นได้ใช้ความรู้ของตัวเองก่อความเสียหายให้กับหน่วยงานอื่นๆ อย่างมาก

- ปัจจุบันหันมาให้ความรู้เกี่ยวกับระบบรักษาความปลอดภัยบนเครือข่ายแทน

Script Kiddy

- ❖ เป็นกลุ่มคนที่ถือได้ว่าเป็นอันตรายมากเป็นทวีคูณ
- ❖ มีการแลกเปลี่ยนโปรแกรมหรือสคริปต์ (scripts) ที่มีคนเขียนและนำออกมาเผยแพร่ให้ทดลองใช้กันอย่างมาก
- ❖ มักเป็นคนอยากรู้อยากเห็น ไม่จำเป็นต้องมีความรู้เกี่ยวกับการเจาะระบบมากนักก็สามารถเป็นได้
- ❖ อาศัยโปรแกรมหรือเครื่องมือบางอย่างที่หามาได้ เช่น การแฮกอีเมล
- ❖ การขโมยรหัสผ่านของผู้อื่น การใช้โปรแกรมก่อวินาศกรรมอย่างง่าย



Hacktivisต์ หรือ cyber terroisต์



- ❖ **Hackivism: computer hacking for political purposes.**
- ❖ **Hackivism is defined as the use of haking to promote a political cause.**

การใช้คอมพิวเตอร์ในฐานะเป็นเครื่องมือการก่ออาชญากรรม

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 ข่าวหลอกหลวง

❖ การขโมยข้อมูลและอุปกรณ์คอมพิวเตอร์

- ใช้กล้องวงจรปิด ใช้กุญแจลิ็อค ใช้สัญญาณกันขโมย การใช้รหัสผ่านเพื่อควบคุม harddisk



❖ ดัดแปลงการทำงานของโปรแกรมอื่น

❖ ความเสียหาย

- แสดงข้อความรบกวนหรือทำให้คอมพิวเตอร์ทำงานช้าลง
- ทำลายการทำงานของระบบคอมพิวเตอร์ เช่น ลบไฟล์ ปิดเครื่อง หรือรบกวนการทำงานของโปรแกรมอื่น เช่น โปรแกรม word

ชนิดของ Virus

❖ ทำงานเมื่อเปิดเครื่องหรือเรียกโปรแกรม

- ทำงานบน boot sector หรือ system virus ฝังตัวที่ boot sector ของดิสก์ และหน่วยความจำของเครื่อง ทำงานเมื่อเปิดเครื่อง
- ติดมากับแฟ้มงานหรือโปรแกรม ฝังตัวอยู่ต่างๆไฟล์ต่างๆ ส่วนใหญ่เป็นไฟล์ .exe และ .com เพราะเรียกใช้บ่อย มักมากับการ download file หรือเปิดไฟล์ที่แนบมากับอีเมล
- Macro virus ทำงานบนโปรแกรมที่มีการยอมให้ใช้ภาษา macro เช่น word excel

❖ ทำงานตามกำหนดเวลาที่ตั้งไว้

- Logic bomb หรือ time bomb เช่น michelangelo ที่ทำลายข้อมูลทุกวันเกิดของไมเคิลแองเจโล

❖ แตกต่างจากไวรัส ตรงที่สามารถแพร่กระจายตัวเองจากคอมพิวเตอร์เครื่องหนึ่งไปยังเครื่องคอมพิวเตอร์อื่นโดยผ่านระบบเครือข่าย

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

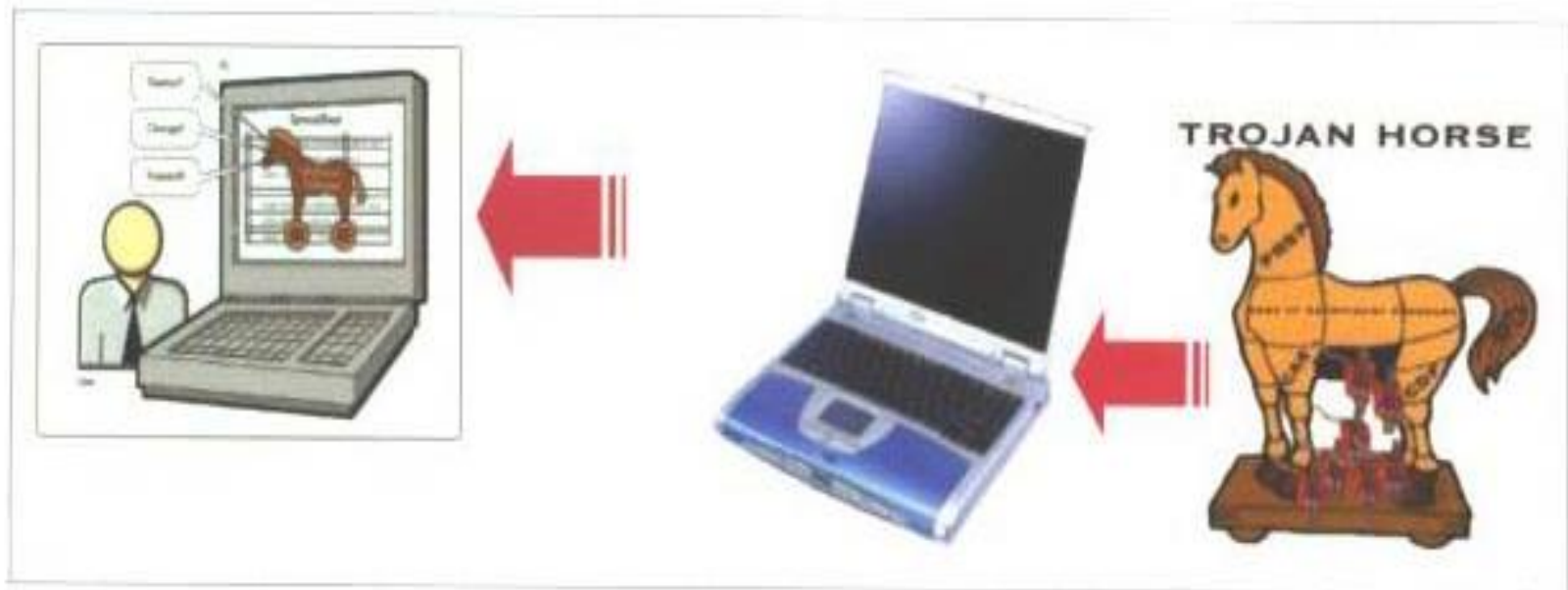


❖ จะทำลายระบบทรัพยากรคอมพิวเตอร์ให้มีประสิทธิภาพลดลง และไม่อาจทำงานต่อไปได้ เช่น

- ฮาร์ดดิสก์มีข้อมูลเต็ม
- เครื่องคอมพิวเตอร์ไม่สามารถทำงานได้
- สั่งพิมพ์งานไม่ได้
- หน้าจอดับไปเอง
- เครื่องปิดลงไปเองโดยไม่มีสาเหตุ

Trojan Horse

- ❖ ไม่มีการแพร่กระจายไปยังเครื่องอื่น จะแฝงตัวมากับโปรแกรมอื่น ๆ ที่ส่งมา เช่น zip file เมื่อมีการเรียกใช้ โปรแกรมจะลบไฟล์ที่อยู่ใน hard disk



Trojan Horse

- ❖ ทำงานโดยอาศัยการฝังตัวอยู่ในระบบคอมพิวเตอร์เครื่องนั้น และจะไม่มี การแพร่กระจายตัวแต่อย่างใด
- ❖ โปรแกรมจะถูกตั้งเวลาการทำงานหรือควบคุมการทำงาน ระยะไกลจากผู้ไม่ประสงค์ดี เพื่อให้เข้ามาทำงานยังเครื่อง คอมพิวเตอร์เป้าหมายได้
- ❖ เช่น แสร้งทำเป็นโปรแกรมยูทิลิตี้ให้ใช้งานแต่แท้จริงคือ
- ❖ โปรแกรมอันตรายเมื่อถึงเวลา ก็จะทำงานบางอย่างทันที

❖ อาการโดนม้าโทรจัน

- เปิดปิดไดร์ CD-ROM
- เปลี่ยนแปลง ลบ แก้ไขข้อมูล
- ควบคุมคีย์บอร์ดและดูภาพการทำงานที่หน้าจอ

- ❖ ข่าวดังปลอม เป็นการส่งข้อความต่อ ๆ กันเหมือนจดหมายลูกโซ่เพื่อให้เกิดความเข้าใจผิด โดยอาศัยเทคนิคทางจิตวิทยาเพื่อให้เกิดความน่าเชื่อถือ
- ❖ เช่น โปรดอย่าใช้มือถือนี้อีก..... เครื่องดื่มนี้.....เป็นอันตราย

Denial of service

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

ข้อสังเกตเกี่ยวกับการได้รับไวรัสคอมพิวเตอร์

- ❖ มีข้อความหรือภาพแปลก ๆ แสดงบนจอภาพ
- ❖ มีเสียงผิดปกติหรือเสียงเพลงเปิดขึ้นเป็นบางเวลา
- ❖ หน่วยความจำคอมพิวเตอร์ลดน้อยลงกว่าที่ควรจะเป็น
- ❖ โปรแกรมหรือไฟล์หายไป โดยที่ไม่ได้ลบทิ้ง
- ❖ มีโปรแกรมแปลกปลอมเข้ามา
- ❖ ขนาดของไฟล์ใหญ่ผิดปกติ
- ❖ ทำงานของไฟล์หรือโปรแกรมผิดปกติจากเดิม

การป้องกันการเข้าถึงข้อมูลและคอมพิวเตอร์

❖ การใช้ username และ password

❖ การใช้วัตถุใด ๆ เพื่อการเข้าสู่ระบบ ได้แก่ บัตร กุญแจ

- การใช้บัตร ATM ควบคู่กับ PIN 4 หลัก(personal identification number)

❖ การใช้อุปกรณ์ทางชีวภาพ (biometric devices)

- เสี่ยง ลายนิ้ว ฝ่ามือ ลายเซ็นต์ ม่านตา รูปหน้า โดยแปลงลักษณะบุคคลให้อยู่ในรูปดิจิทัลที่สามารถเปรียบเทียบได้

❖ ระบบเรียกกลับ callback system

- ผู้ใช้ระบุชื่อและรหัสผ่านเพื่อขอใช้ระบบปลายทาง ถ้าข้อมูลถูกต้อง ระบบจะเรียกกลับให้เข้าใช้งานเอง

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 สังเกตหัวข้อจดหมายก่อนเปิดอ่าน
- Antivirus must be install ติดตั้งโปรแกรมป้องกันไวรัส เช่น norton antivirus , PC-cillin, Dr.solomon
- Interest on virus news ให้ความสนใจเกี่ยวกับข่าวสารไวรัส
- Learn to be cautious ให้ระวังให้มาก อย่าเปิดอีเมลล์แบบไม่ยั้งคิด

❖ ติดตามข่าวสารเกี่ยวกับการป้องกันการก่อวิน ได้ที่ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์แห่งประเทศไทย

<http://thaicert.nectec.or.th>

ข้อควรระวังเมื่อเข้าไปใช้งานเครือข่าย (ต่อ)

ThaiCERT : ศูนย์ประสานงานการรับมือภัยคุกคามคอมพิวเตอร์ ประเทศไทย - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media

Address <http://www.thaicert.nectec.or.th> Go

ThaiCERT
Thai Computer Emergency Response Team

ECTI-21
NECTEC
National Electronics and Computer Technology Center

ประกาศเว็บไซต์ ThaiCERT งดให้บริการชั่วคราว

เนื่องจากจะปิดการจ่ายกระแสไฟฟ้า ดังนั้นเว็บไซต์ ThaiCERT จึงไม่สามารถให้บริการได้ในวันนี้ และช่วงระยะเวลาดังกล่าวนี้ วันเสาร์ที่ 24,31 กรกฎาคม 2547 และวันอาทิตย์ที่ 4,11,18,25 กรกฎาคม 2547 ตั้งแต่เวลา 08.00 - 20.00 น. ทางทีมงานต้องขออภัยมา ณ ที่นี้

ThaiCERT: Thai Computer Emergency Response Team
ศูนย์ประสานงานการรับมือภัยคุกคามคอมพิวเตอร์ ประเทศไทย

Alerts

- ปัญหาความปลอดภัยของ [Download.Ject](#) ที่ทำให้เครื่องถูกติดตั้งซอฟต์แวร์ที่ไม่ประสงค์ดี 30 มิถุนายน 2547 !! **New !!**
- [MS04-016](#) Vulnerability in DirectPlay Could Allow Denial of Service (839643) 11 มิถุนายน 2547 !! **New !!**
- [W32.Sasser.Worm](#) และ [W32.Sasser.B.Worm](#) 4 พฤษภาคม 2547 !! **Update !!**
- [W32.Bagle.W@mm](#), [W32.Bagle.X@mm](#), [W32.Bagle.Y@mm](#) หรือ [W32.Bagle.Z@mm](#) 27 เมษายน 2547
- [W32.Netsky.S@mm](#) 7 เมษายน 2547
- [W32.Bagle.Q@mm](#) หรือ [W32.Bagle.O@mm](#) 19 มีนาคม 2547
- [W32.Bagle.H@mm](#) 3 มีนาคม 2547
- [W32.Netsky.B@mm](#), [W32.Netsky.C@mm](#) และ [W32.Netsky.D@mm](#) 2 มีนาคม 2547

Advisories & Alerts
Security Bulletins
เอกสารเผยแพร่
เครื่องมือ
บริการ
FAQ
เกี่ยวกับ ThaiCERT
ความรู้พิเศษ
บริการระบบแจ้งข่าว
สาร
ผ่านทางอี-เมล
(Mailing List)
ประกาศรับสมัครงาน

ค้นหา

[Powered by Sansam]

ข้อควรระวังเมื่อเข้าไปใช้งานเครือข่าย (ต่อ)

The screenshot shows the CERT Coordination Center website as viewed in Microsoft Internet Explorer. The browser's address bar displays <http://www.cert.org>. The website header includes the Carnegie Mellon Software Engineering Institute logo and navigation links: Home, Site Index, Search, Contact, and FAQ. Below these are links for vulnerabilities, incidents & fixes, security practices & evaluations, survivability research & analysis, and training & education. A search bar with a 'GO' button and a 'customize...' link is also present.

The main content area features a large graphic celebrating the CERT Coordination Center's 15th anniversary (1988 - 2003). To the right of this graphic, a text block states: "Established in 1988, the CERT® Coordination Center (CERT/CC) is a center of Internet security expertise, located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University."

On the left side, there are several menu sections: "Options" with links for Vulnerabilities, Incidents & Fixes; Security Practices & Evaluations; Survivability Research & Analysis; and Training & Education. Below this is a "Related" section with links for CERT Contact Information, CERT Statistics, Meet the CERT/CC, and CERT/CC Overview and Intruder Trends.

The "What's New" section, dated June 29, 2004, features a "Press Release: 2004 E-Crime Watch Survey Shows Significant Increase in Electronic Crimes". The text describes the survey findings: "The 2004 E-Crime Watch survey shows a significant number of organizations reporting an increase in electronic crimes (e-crimes) and network, system or data intrusions." A second entry is dated May 28, 2004.

The "React to Today's Problems" section lists several advisories and incident notes, including: "US-CERT Technical Cyber Security Alert TA04-184A: Internet Explorer Update to Disable ADODB.Stream ActiveX Control", "US-CERT Technical Cyber Security Alert TA04-174A: Multiple Vulnerabilities in ISC DHCP 3", and "US-CERT Technical Cyber Security Alert TA04-163A: Cross-Domain Redirect Vulnerability in Internet Explorer". It also includes a link to "US-CERT Vulnerability Notes" and a link to the "US-CERT vulnerability notes database".

การสร้างสังคมและรักษาสีงแวดล้อม

❖ ป้องกันไม่ให้เด็กเข้าไปดูเว็บไซต์ที่ไม่เหมาะสม

- Web filtering software

❖ วางแผนเพื่อจัดการกับเครื่องคอมพิวเตอร์ที่ไม่ใช้แล้ว

- บริจาคให้โรงเรียน เอาส่วนประกอบบางส่วนไปขายใหม่ในราคาถูก

❖ การใช้พลังงาน

- กำหนดเป็น sleep mode

การรักษาความปลอดภัยของระบบคอมพิวเตอร์

❖ การติดตั้งโปรแกรมป้องกันไวรัส (Antivirus Program)

❖ การใช้ระบบไฟร์วอลล์ (Firewall System)

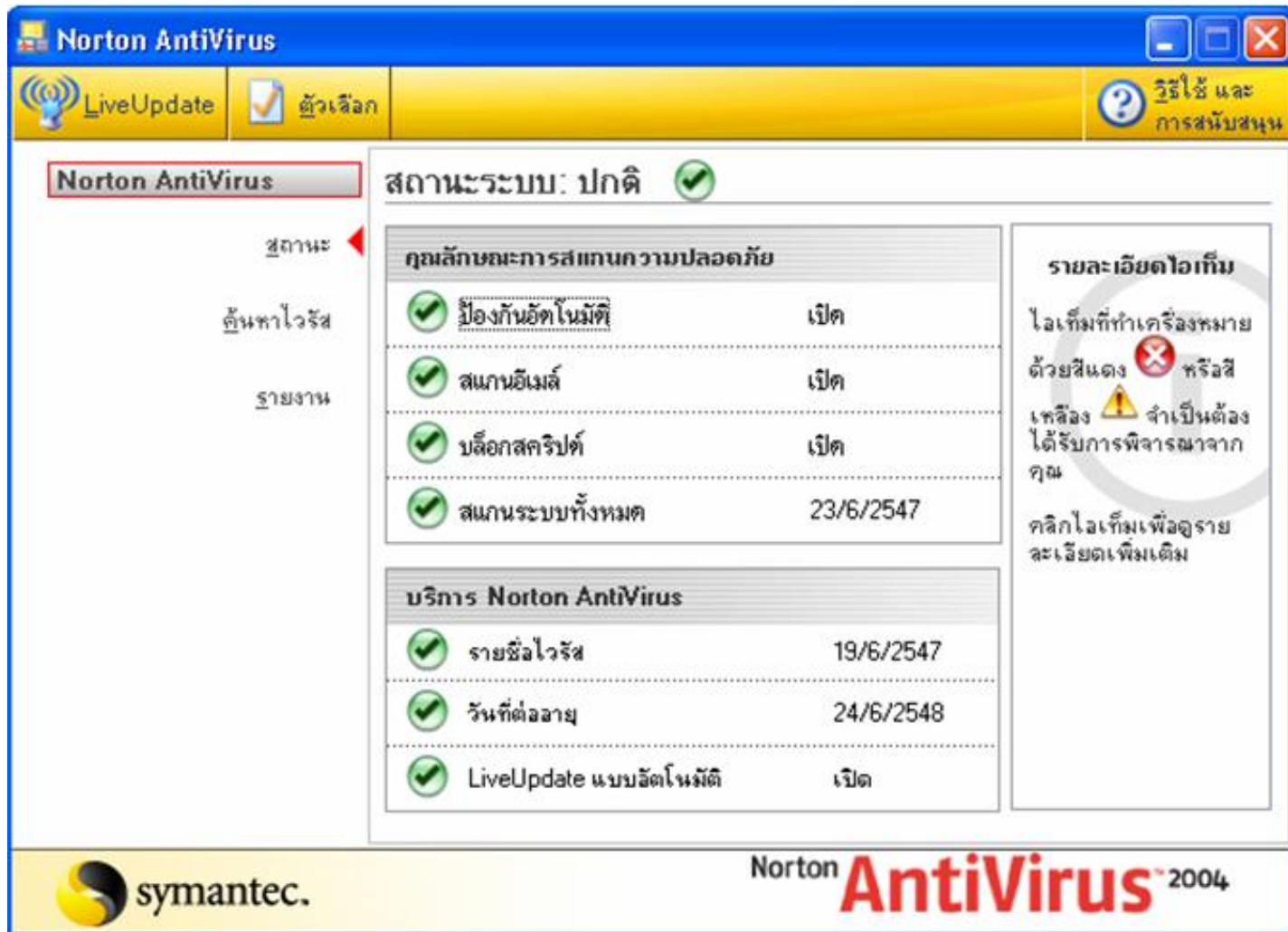
❖ การเข้ารหัสข้อมูล

❖ การสำรองข้อมูล

Antivirus Program

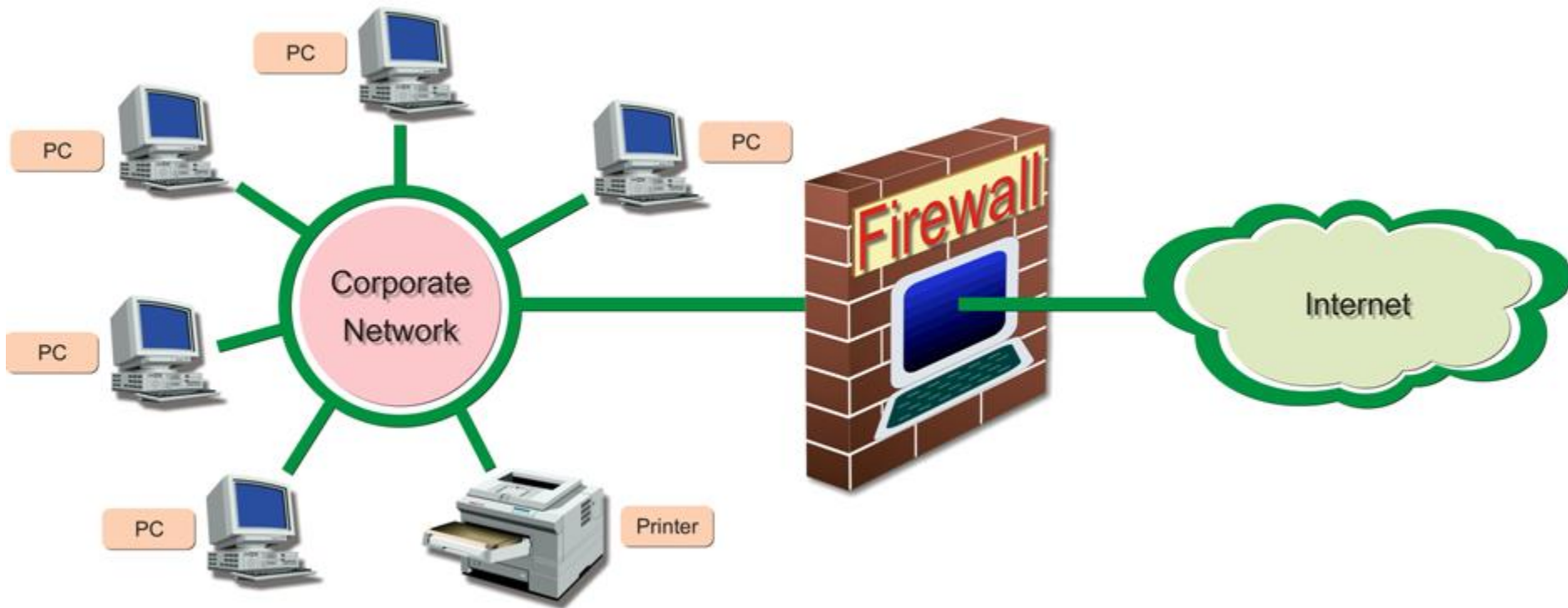
- ❖ ทำหน้าที่คอยตรวจสอบและติดตามการบุกรุกของโปรแกรมประสงค์ร้าย
- ❖ เมื่อพบจะสามารถกำจัดและแจ้งให้ผู้ใช้ทราบได้ทันที
- ❖ จำเป็นต้องทำให้ตัวโปรแกรมอัปเดตตัวข้อมูลใหม่อยู่เสมอเพื่อให้ได้ผลดีมากขึ้นไป
- ❖ เช่น Norton antivirus,

ตัวอย่างโปรแกรมป้องกันไวรัส (Antivirus Program)



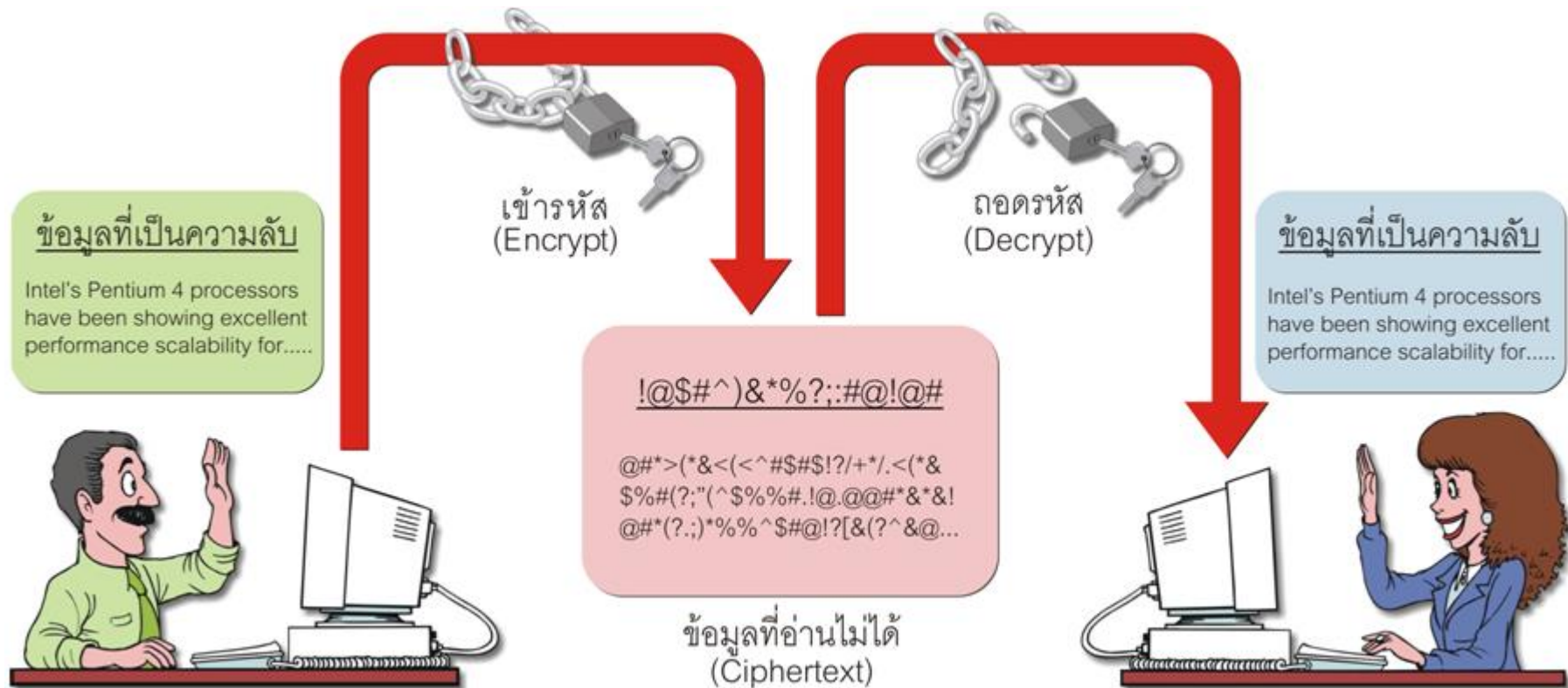
- ❖ เป็นระบบรักษาความปลอดภัยที่ประกอบด้วยฮาร์ดแวร์หรือซอฟต์แวร์ก็ได้
- ❖ ทำหน้าที่คอยดักจับ ป้องกันและตรวจสอบการบุกรุก (intrusion) รวมถึงการเข้าถึงที่ไม่ได้รับอนุญาตจากผู้ไม่ประสงค์ดี ภายนอก
- ❖ ระบบจะให้ข้อมูลบางอย่างที่ได้รับการอนุญาตผ่านเข้าออกเท่านั้น หากไม่ตรงกับเงื่อนไขจะไม่สามารถผ่านไปมาได้

การติดตั้งระบบไฟร์วอลล์สำหรับเครือข่าย



- ❖ การเข้ารหัสข้อมูล (Encryption)
- ❖ อาศัยสมการทางคณิตศาสตร์ที่ซับซ้อนทำการเปลี่ยนแปลงข้อมูลที่สามารถอ่านได้ปกติ (plaintext) ให้ไปอยู่ในรูปแบบที่ไม่สามารถอ่านได้ (ciphertext)
- ❖ ผู้ไม่ประสงค์ดีที่แอบเอาข้อมูลไปใช้จะไม่สามารถอ่านข้อมูลที่มีความสำคัญนั้นได้ เพราะมีการเข้ารหัส (encryption) ไว้
- ❖ การจะอ่านจำเป็นต้องถอดรหัสข้อมูล (decryption) เสียก่อน

เทคนิคการเข้ารหัสและถอดรหัสของข้อมูล



การสำรองข้อมูล Back up

- ❖ Down load คือ การสำเนาข้อมูล ไฟล์ข้อมูล หรือโปรแกรมที่อยู่ในพื้นที่เก็บข้อมูลหลักไปยังพื้นที่อื่น เพื่อให้นำมาใช้งานได้อีก หากข้อมูลต้นฉบับนั้นเกิดสูญหายหรือถูกทำลาย
- ❖ Up load คือการนำข้อมูลที่เก็บสำรองไว้กลับมาใช้อีก
- ❖ วิธีการสำรองข้อมูลอาจทำทั้งระบบหรือแค่บางส่วน โดยเก็บลงหน่วยเก็บบันทึกข้อมูลสำรอง เช่น ฮาร์ดดิสก์หรือ CD-ROM
- ❖ หากข้อมูลมีความสำคัญมากอาจต้องสำรองข้อมูลทุกวัน หรือทุกสัปดาห์แต่หากข้อมูลมีความสำคัญน้อย การสำรองเพียงเดือนละครั้ง หรือนานๆ ครั้งก็เพียงพอ

แบบฝึกหัดท้ายบท

1. อะไรคือแนวโน้มการพัฒนากฎหมายด้านเทคโนโลยีที่มีส่วนสำคัญต่อความกังวลทางด้านจริยธรรม
2. ระบบอินเทอร์เน็ตมีผลกระทบต่อการปกป้องสิทธิส่วนบุคคลอย่างไร
3. อะไรคือสาเหตุที่สำคัญต่อปัญหาด้านคุณภาพของซอฟต์แวร์
4. อธิบายกระบวนการปกป้องสิทธิในทรัพย์สินทางปัญญา และระบบอินเทอร์เน็ตมีส่วนทำลายต่อสิทธิในทรัพย์สินทางปัญญาอย่างไร
5. อธิบายความหมายของ ความเป็นส่วนตัว และ การปฏิบัติอย่างเป็นธรรมต่อข่าวสาร ระบบอินเทอร์เน็ตมีส่วนทำลายต่อสิทธิส่วนบุคคลอย่างไร