Computer Security and Safety, Ethics, and Privacy

Computer Security Risks

เหตุการณ์ใด ๆ ที่เป็นการกระทำที่อาจก่อให้เกิดการสูญเสียหรือความเสียหายของฮาร์ดแวร์คอมพิวเตอร์,ซอฟแวร์, ข้อมูล, ข้อมูลหรือความสามารถในการประมวลผล

- **computer crime** การฝ่าฝืนเจตนาของการรักษาความปลอดภัยคอมพิวเตอร์มักจะเกี่ยวข้องกับการกระทำโดยเจตนาที่ผิดกฎหมาย การกระทำใด ๆ ที่ผิดกฎหมายเกี่ยวกับคอมพิวเตอร์โดยทั่วไปจะเรียกว่าอาชญากรรมคอมพิวเตอร์
- **crimeware** ซอฟต์แวร์ที่ใช้โดยอาชญากรไซเบอร์
- **hacker** คนที่เข้าถึงคอมพิวเตอร์หรือเครือข่ายอย่างผิดกฎหมาย แฮกเกอร์บางคนเรียกร้องความตั้งใจที่จะละเมิดความปลอดภัยของพวกเขาคือเพื่อปรับปรุงการรักษาความปลอดภัย
- **cracker** คนที่เข้าถึงคอมพิวเตอร์หรือเครือข่ายอย่างผิดกฎหมาย แต่มีความตั้งใจที่จะทำลายข้อมูลการขโมยข้อมูลหรือการกระทำที่เป็นอันตรายอื่น ๆ
- **script kiddie** มีเจตนาเช่นเดียวกับ cracker แต่ไม่ได้มีความรู้ทางด้านเทคนิค script kiddie มักจะใช้prewritten โปรแกรมแฮ็คและ Crack เข้าไปในระบบคอมพิวเตอร์
- **cyberextortionist** คือคนที่ใช้e-mail เป็นพาหะสำหรับการถูกกรรโชก
- **cyberterrorist** คือคนที่ใช้อินเทอร์เน็ตหรือเครือข่ายคอมพิวเตอร์ที่ทำลายหรือสร้างความเสียหายด้วยเหตุผลทางการเมือง

Internet and Network Attacks

- **online security service** เป็นเว็บไซต์ที่ประเมินคอมพิวเตอร์ของคุณเพื่อตรวจสอบช่องโหว่ของอินเทอร์เน็ตและอีเมล

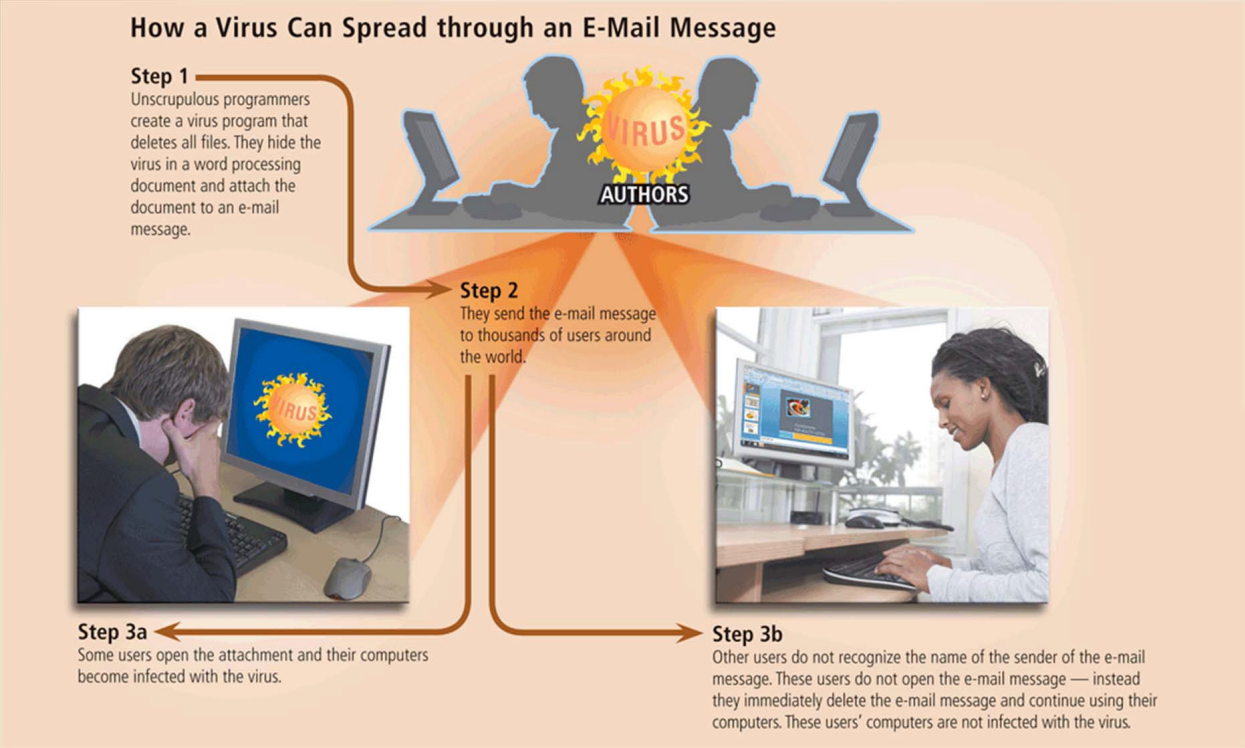
Popular Online Security Services for Personal Computers

Name of Online Service	Web Address
Audit My PC	http://www.auditmypc.com/firewall-test.asp
McAfee FreeScan	http://home.mcafee.com/Downloads/FreeScan.aspx
Symantec Security Check	http://security.symantec.com/sscv6/home.asp
Trend Micro House Call	http://housecall.trendmicro.com/

- **Computer Emergency Response Team Coordination Center, or CERT/CC** กองทุนและศูนย์พัฒนาวิจัยการรักษาความปลอดภัยทางอินเตอร์เน็ตของสหรัฐฯ
- **computer virus** คืออันตรายของโปรแกรมคอมพิวเตอร์ที่มีผลต่อคอมพิวเตอร์ในเชิงลบโดยการเปลี่ยนวิธีการทำงานของคอมพิวเตอร์โดยผู้ใช้ไม่รู้และยังไม่ได้อนุญาต
- **worm** เป็นโปรแกรมที่คัดลอกตัวเองซ้ำแล้วซ้ำเล่าทำให้คอมทำงานช้าลง
- **Trojan horse** (ชื่อมาจาก the Greek myth หรือตำนานกรีก) เป็นโปรแกรมที่ซ่อนอยู่ภายในโปรแกรม ทำให้มีลักษณะเหมือนโปรแกรมที่ถูกต้องตามกฎหมาย
- **rootkit** เป็นโปรแกรมที่ซ่อนอยู่ในคอมพิวเตอร์และใครบางคนจากสถานที่ห่างไกลอนุญาตให้ควบคุมการใช้เต็มรูปแบบของเครื่องคอมพิวเตอร์

ทั้ง virus worm Trojan horse และ rootkit จัดอยู่ใน malware (หรือชื่อเต็ม malicious software)

คอมพิวเตอร์ที่โดนพวก **malware** มีอาการหนึ่งอย่างหรือมากกว่าดังนี้



- OS รันช้ากว่าปกติ
- หน่วยความจำมีค่าเหลือน้อยผิดปกติ
- บางไฟล์จะมีลักษณะผิดปกติ
- บนหน้าจอ มีข้อความหรือรูปภาพที่ผิดปกติ
- มีเพลงหรือเสียงประหลาดๆเล่นขึ้นมาเมื่อไม่ต้องการ
- โปรแกรมที่มีอยู่หรือไฟล์หายไป
- โปรแกรมหรือไฟล์ไม่ทำงาน
- โปรแกรมหรือไฟล์ลึกลับปรากฏ
- ระบบเปลี่ยนแปลงเพี้ยนๆ
- OS boot ไม่ขึ้น
- ระบบปฏิบัติการปิดกะทันหัน

Safeguards against Computer Viruses and Other Malware quarantine
เป็นพื้นที่ที่แยกต่างหากจากฮาร์ดดิสก์ที่เก็บไฟล์ที่ติดไวรัสจนเชื้อสามารถลบออกได้

Tips for Preventing Viruses and Other Malware

1. Never start a computer with removable media inserted in the drives or plugged in the ports, unless the media are uninfected.
2. Never open an e-mail attachment unless you are expecting it *and* it is from a trusted source.
3. Set the macro security in programs so that you can enable or disable macros. Enable macros only if the document is from a trusted source and you are expecting it.
4. Install an antivirus program on all of your computers. Update the software and the virus signature files regularly.
5. Scan all downloaded programs for viruses and other malware.
6. If the antivirus program flags an e-mail attachment as infected, delete or quarantine the attachment immediately.
7. Before using any removable media, scan the media for malware. Follow this procedure even for shrink-wrapped software from major developers. Some commercial software has been infected and distributed to unsuspecting users.
8. Install a personal firewall program.
9. Stay informed about new virus alerts and virus hoaxes.

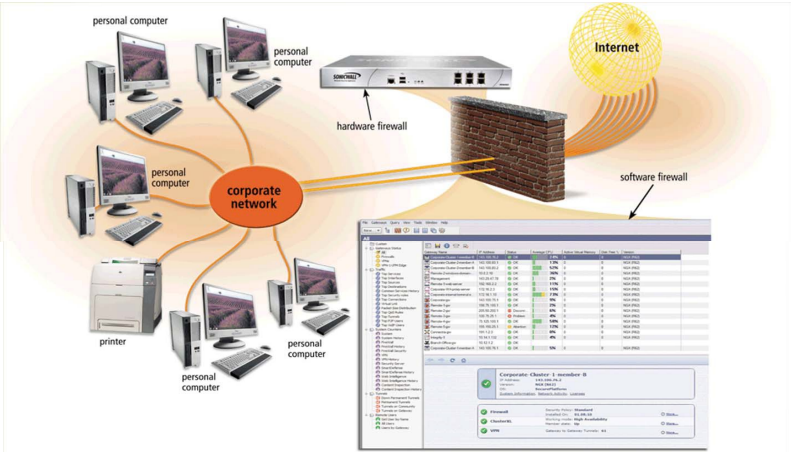
- **Botnets** คือกลุ่มที่ถูกบุกรุกคอมพิวเตอร์ที่เชื่อมต่อกับเครือข่ายเช่นอินเทอร์เน็ตที่ใช้เป็นส่วนหนึ่งของเครือข่ายที่การโจมตีเครือข่ายอื่น ๆ
- **Zombie** คอมพิวเตอร์ที่ถูกบุกรุกเป็นที่รู้จักกันในนาม **Zombie**
- **Bot** คือโปรแกรมที่มีประสิทธิภาพซ้ำซ้อนงานบนเครือข่าย
- **Denial of Service Attacks** (dos Attacks)คือการโจมตีที่มีจุดประสงค์คือเพื่อทำลายคอมพิวเตอร์เข้าถึงบริการอินเทอร์เน็ตเช่นเว็บหรือ e-mail

  DDoS (*distributed DoS*) *attack* มีความสามารถที่จะหยุดการดำเนินงานชั่วคราวที่เว็บไซต์ต่าง ๆ นานา

- **Back Doors**

  เป็นโปรแกรมหรือชุดคำสั่งในโปรแกรมที่ให้ผู้ใช้สามารถข้ามความปลอดภัยเมื่อมีการเข้าถึงการควบคุมโปรแกรมคอมพิวเตอร์หรือเครือข่าย
- **Spoofing** เป็นเทคนิคที่ผู้บุกรุกใช้เพื่อหลอกลวงและควบคุมระบบ ให้เข้าใจผิด

Safeguards against Botnets, DoS/DDoSAttacks, Back Doors, and Spoofing



Stand-Alone Personal Firewall Software
BitDefender Internet Security
CA Personal Firewall
McAfee Internet Security
Norton Personal Firewall
Webroot Desktop Firewall
ZoneAlarm Pro

- **Firewalls** ฮาร์ดแวร์และ / หรือซอฟต์แวร์ที่ปกป้องทรัพยากรเครือข่ายจากการบุกรุกของผู้ใช้บนเครือข่ายอื่น
- **personal firewall** เป็นโปรแกรมยูทิลิตี้ที่ตรวจจับและปกป้องคอมพิวเตอร์ส่วนบุคคล
- **Intrusion detection software** วิเคราะห์ traffic ภายในเครือข่ายทั้งหมดโดยอัตโนมัติและประเมินช่องโหว่ของระบบ ระบุถึงความเสี่ยง การป้องกันผู้บุกรุกและแจ้งผู้บริหารเครือข่ายของรูปแบบพฤติกรรมที่น่าสงสัยหรือระบบการละเมิด
- **Honeypots** ระบบจำลองเกี่ยวกับ network ที่คอยหลอกล่อจากการพยายามโดยไม่ได้รับอนุญาตหรือบุกรุก

Unauthorized Access and Use:

Unauthorized access คือการใช้เครื่องคอมพิวเตอร์หรือเครือข่ายโดยไม่ต้องขออนุญาต

Unauthorized use คือการใช้เครื่องคอมพิวเตอร์เข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรืออาจจะทำสิ่งที่ผิดกฎหมาย

องค์กรใช้มาตรการหลายอย่างเพื่อช่วยป้องกัน เช่น

- มีนโยบายความมั่นคงปลอดภัยในระบบสารสนเทศ
- ปิดการใช้งานการแชร์ไฟล์และ การใช้เครื่องพิมพ์ร่วมกัน
- ติดตั้งไฟร์วอลล์
- ติดตั้งซอต์ฟแวร์ Intrusion detection software

Access controls

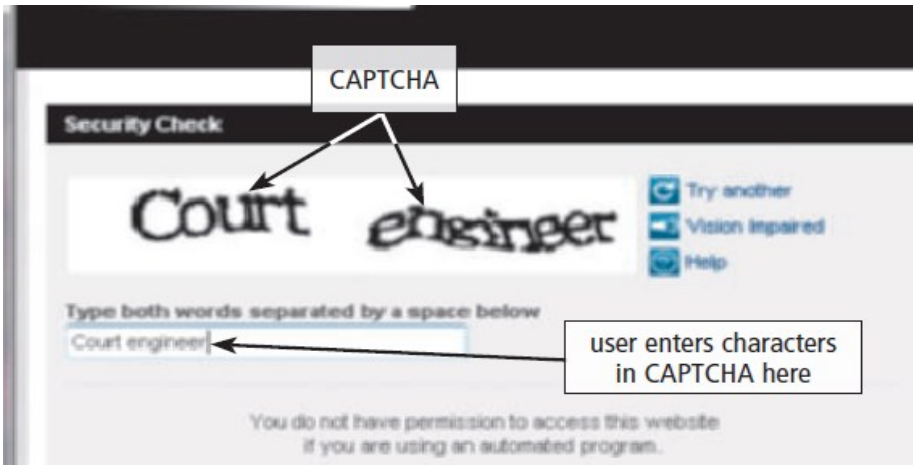
การควบคุมการเข้าใช้คอมพิวเตอร์ การเข้าออก สิ่งที่สามารถทำได้

- มี 2 กระบวนการ Identification and authentication
  1. **Username & Password**
  2. **Passphrase, CAPTCHA**

Password Protection

Number of Characters	Possible Combinations	AVERAGE TIME TO DISCOVER Human	Computer
1	36	3 minutes	.000018 second
2	1,300	2 hours	.00065 second
3	47,000	3 days	.02 second
4	1,700,000	3 months	1 second
5	60,000,000	10 years	30 seconds
10	3,700,000,000,000,000	580 million years	59 years

- *Possible characters include the letters A–Z and numbers 0–9*
- *Human discovery assumes 1 try every 10 seconds*
- *Computer discovery assumes 1 million tries per second*
- *Average time assumes the password would be discovered in approximately half the time it would take to try all possible combinations*



- Passphrase เป็นรหัสคล้ายกับ password แต่จะมีความยาวมากกว่าและ อาจจะเป็นในรูปแบบวลีที่เดายากแต่จำง่าย

- CAPTCHA เพื่อเพิ่มเติมการป้องกันรหัสผ่านของผู้ใช้

- **possessed object**
  คือรายการที่คุณจะต้องดำเนินการเพื่อให้เข้าถึงใด ๆ ที่เป็นสิ่งอำนวยความสะดวกเครื่องคอมพิวเตอร์หรือเครื่องคอมพิวเตอร์
- **personal identification number** (**PIN**)
  เป็นรหัสผ่านที่เป็นตัวเลขที่ได้รับมอบหมายทั้งโดยบริษัท หรือเลือกโดยผู้ใช้
- **Biometric Devices**
  คือเครื่องที่รับรอง เอกลักษณ์ของบุคคลโดยแปลลักษณะส่วนบุคคล
- **Digital forensics,** (หรือเรียกว่า computer forensics, network forensics, or cyberforensics) การเก็บหลักฐาน การค้นหา การวิเคราะห์และการเสนอหลักฐานทางดิจิตอลที่อยู่ในอุปกรณ์คอมพิวเตอร์และอิเล็กทรอนิกส์
- **Hardware theft** คือการกระทำของขโมยอุปกรณ์คอมพิวเตอร์
- **Hardware vandalism** คือการกระทำที่ทำให้เสียหายหรือทำลายอุปกรณ์คอมพิวเตอร์

Safeguards against Hardware Theft and Vandalism

เพื่อช่วยลดโอกาสของการขโมยในบริษัทและโรงเรียนจึงใช้ความหลากหลายของมาตรการรักษาความปลอดภัย
- a real time location system
- RFID tags

- Passwords, possessed objects, and biometrics
- Physical access controls
- Alarm systems เสียงแจ้งเตือน
- Cables to lock equipment สายเคเบิลล็อกอุปกรณ์ที่มีมูลค่าสูง

Software Theft

เกิดขึ้นเมื่อมีคน

(1) ขโมยสื่อซอฟต์แวร์

(2) จงใจลบโปรแกรม

(3) software เถื่อน

(4) crack program

Safeguards against Software Theft

license agreement คือสิทธิในการใช้ซอฟต์แวร์

the product activation คือการดำเนินการอย่างใดอย่างหนึ่งทางออนไลน์หรือทางโทรศัพท์โดยให้โค้ดยืนยันแก่ผู้ใช้

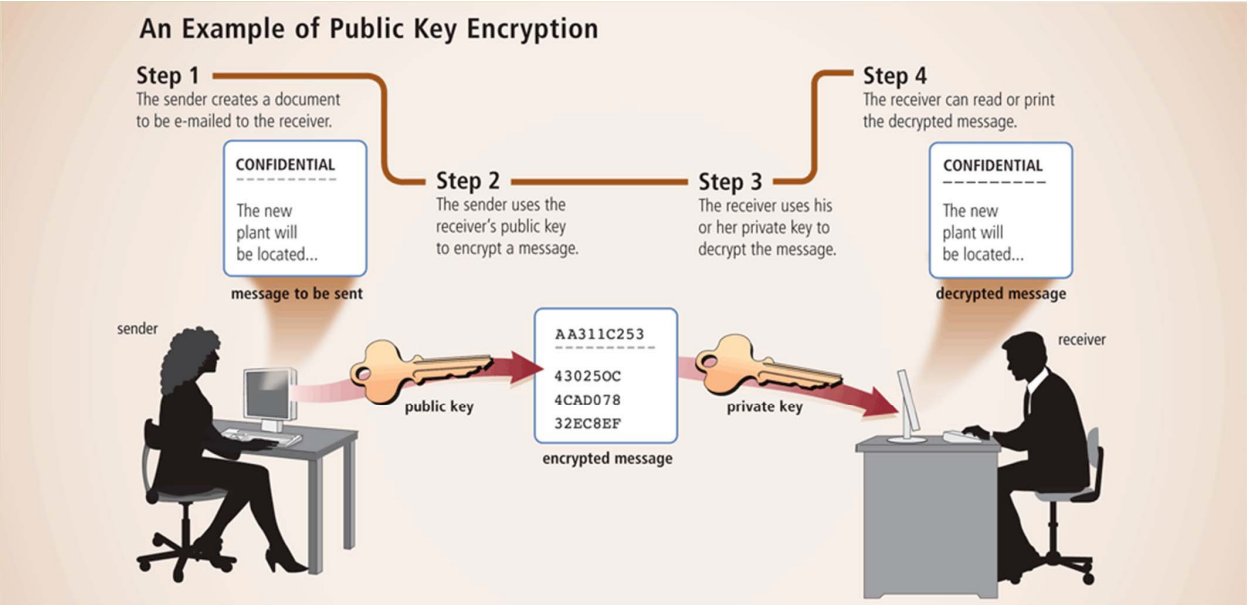
Information theft ชนิดของความเสี่ยงด้านความปลอดภัยคอมพิวเตอร์ เกิดขึ้นเมื่อมีคนขโมยข้อมูลส่วนบุคคลหรือเป็นความลับข้อมูล หากถูกขโมย, การสูญเสียข้อมูลที่สามารถทำให้เกิดความเสียหายมากอาจเกิดจากถูกขโมยฮาร์ดแวร์หรือซอฟแวร์

Safeguards against Information Theft

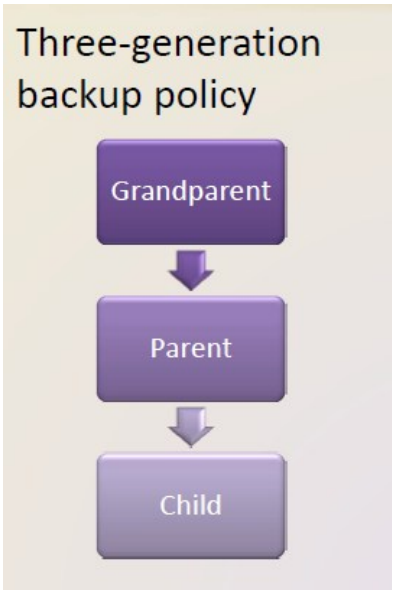
Encryption เป็นกระบวนการของการแปลงที่สามารถอ่านได้ข้อมูลเป็นตัวอักษรที่ไม่สามารถอ่านได้เพื่อป้องกันไม่ให้ไม่ได้รับอนุญาต

Simple Encryption Algorithms

Name	Algorithm	Plaintext	Ciphertext	Explanation
Transposition	Switch the order of characters	SOFTWARE	OSTFAWER	Adjacent characters swapped
Substitution	Replace characters with other characters	INFORMATION	WLDIMXQUWIL	Each letter replaced with another
Expansion	Insert characters between existing characters	USER	UYSYEYRY	Letter Y inserted after each character
Compaction	Remove characters and store elsewhere	ACTIVATION	ACIVTIN	Every third letter removed (T, A, O)



digital signature คือรหัสการเข้ารหัสที่คน, เว็บไซต์หรือองค์กรยึดติดกับข้อความอิเล็กทรอนิกส์เพื่อยืนยันตัวตนของผู้ส่งข้อความ
-มักจะใช้เพื่อให้แน่ใจว่านักต้มตุ๋นไม่ได้มีส่วนร่วมในการทำธุรกรรมทางอินเทอร์เน็ตเว็บไซต์ที่ใช้เทคนิคการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลที่เป็นที่รู้จักว่าเป็นเว็บไซต์ที่เชื่อถือได้
digital certificate เป็นการแจ้งที่รับประกันผู้ใช้หรือเว็บไซต์ถูกต้องตามกฎหมาย การใช้งาน E-commerce ทั่วไปใช้ใบรับรองดิจิทัล เว็บเบราเซอร์
certificate authority (CA) ผู้มีอำนาจหรือ บริษัท ที่ตรวจสอบใบรับรองดิจิทัล
Transport Layer Security คือการให้การเข้ารหัสลับของข้อมูลทั้งหมดที่ผ่านระหว่างไคลเอ็นต์และเซิร์ฟเวอร์อินเทอร์เน็ต
Secure HTTP อนุญาตให้ผู้ใช้สามารถเลือกรูปแบบการเข้ารหัสข้อมูลที่ส่งผ่านระหว่างไคลเอ็นต์และเซิร์ฟเวอร์
virtual private network (VPN) เครือข่ายส่วนตัวที่ทำงานโดยใช้โครงสร้างจากเครือข่ายสาธารณะ
system failure คือ ความผิดปกติของเครื่องคอมพิวเตอร์เป็นเวลานาน
undervoltage เกิดขึ้นเมื่อไฟฟ้าดับ หรือไม่มีไฟฟ้าใช้เพียงพอ
overvoltage, or power surge (ไฟกระชาก) เกิดขึ้นเมื่อพลังงานไฟฟ้าเข้ามาเพิ่มขึ้นมักจะเป็นมากขึ้นกว่าร้อยละห้า
วิธีการป้องกัน system failure
สองวิธีในการป้องกันจากความล้มเหลวของระบบที่เกิดจากไฟฟ้ากระชาก
- uninterruptable power supplies (UPS)
- Backing Up — The Ultimate Safeguard
เป็นการทำซ้ำ, โปรแกรม, ดิสก์ ที่จะสามารถนำมาใช้ได้ถ้าข้อมูลของเก่าหายไป, เสียหายหรือ ถูกทำลาย
- สำรองข้อมูลนอกสถานที่แยกจากเว็บไซต์คอมพิวเตอร์(cloud storage)
สองประเภทของ สำรองข้อมูล:
- Full backup
- Selective backup



Wireless Security

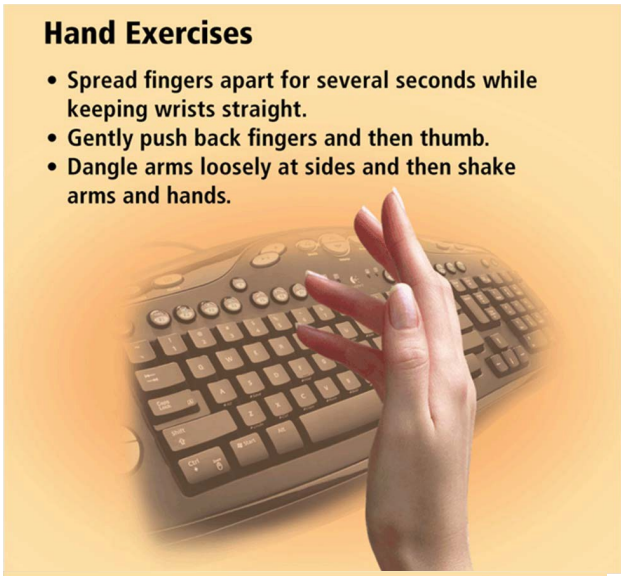
การเชื่อมต่อไร้สายจะเพิ่มความเสี่ยงการความปลอดภัย

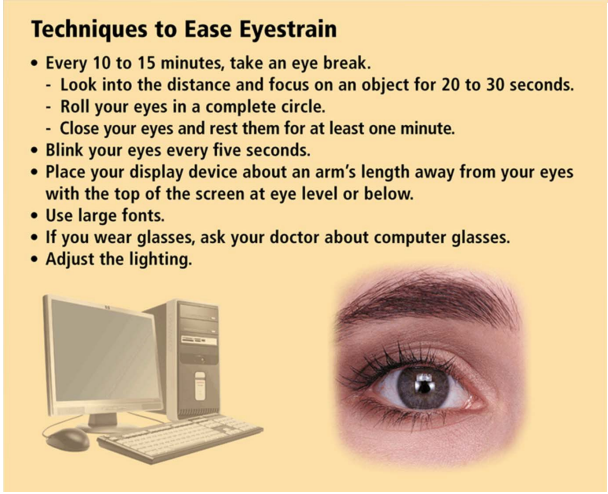
- ร้อยละ 80 ของเครือข่ายไร้สายไร้การป้องกัน
- War driving เป็นพฤติการณ์ค้นหา wifi ระหว่างบุคคลนั้นกำลังอยู่ในรถที่กำลังแล่นอยู่
- การเพิ่มการป้องกันโดยใช้ firewall, safeguards:
    - ไม่ควรตั้งให้เห็น SSID
    - เปลี่ยนค่าเริ่มต้น SSID
    - กำหนดค่า WAP ให้เข้าใช้ได้เฉพาะเครื่อง
    - ใช้มาตรฐานความปลอดภัย WPA หรือ WPA2

Health Concerns of Computer Use

สุขภาพกับการใช้คอมพิวเตอร์

- Repetitive strain injury(RSI)
  - Tendonitis
  - Carpal tunnel syndrome(CTS)
- Computer vision syndrome (CVS)





Ergonomics (การยศาสตร์)การศึกษาเกี่ยวกับการจัดวางรูปแบบของที่ทำงานและอุปกรณ์สำนักงานให้เหมาะสม สะดวก ปลอดภัย และมีประสิทธิภาพ

Computer addiction เกิดขึ้นเมื่อมีอาการติดคอมพิวเตอร์มากๆ จนไม่ทำอะไร จะมีอาการดังนี้

- โหยหาคอมพิวเตอร์ตลอดเวลา - เล่นคอมไม่หยุด - ดีใจเมื่อได้เล่นคอม
- หงุดหงิดเมื่อไม่ได้อยู่ที่คอมพิวเตอร์ - มีปัญหากับเพื่อนและที่โรงเรียน
- ละเลยเพื่อนและครอบครัว

Ethics and Society

จริยธรรมทางคอมพิวเตอร์เป็นแนวทางจริยธรรมที่ควบคุมการใช้งานคอมพิวเตอร์และระบบสารสนเทศ

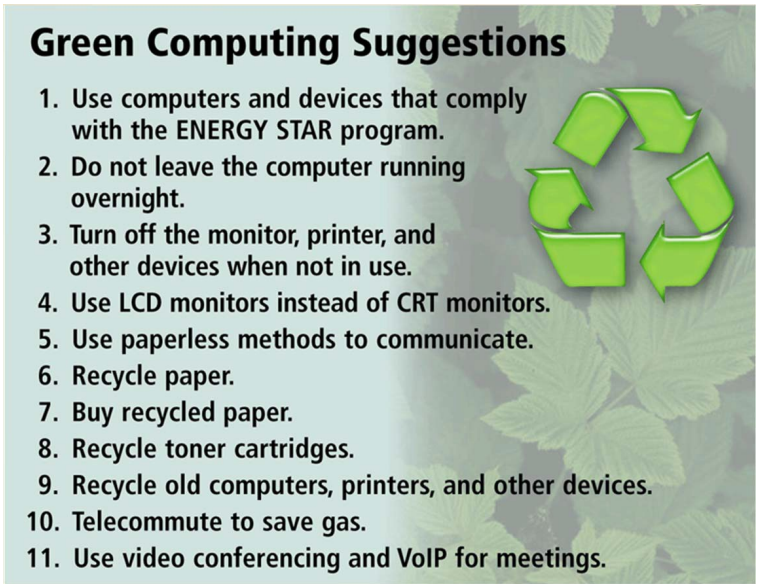
- ความแม่นยำของข้อมูล
- ไม่ข้องเกี่ยวกับข้อมูลทั้งหมดของเว็บ

Intellectual property rights สิทธิในทรัพย์สินทางปัญญาเป็นสิทธิที่ซึ่งผู้สร้างจะได้รับสิทธิในการทำงานของพวกเขา

copyright ลิขสิทธิ์เป็นการปกป้องรูปแบบที่สัมผัสในการแสดงออก

IT code of conduct เป็นแนวทางการเขียนที่จะช่วยให้ตรวจสอบเฉพาะการกระทำคอมพิวเตอร์เป็นจริยธรรมหรือผิดจรรยาบรรณ

Green computing ที่เกี่ยวข้องกับการลดค่าไฟฟ้าและของเสียสิ่งแวดล้อมขณะที่ใช้คอมพิวเตอร์



Information Privacy ความเป็นส่วนตัวของข้อมูลและสารสนเทศ บุคคล กลุ่มบุคคล บริษัท องค์กร

•ฐานข้อมูลออนไลน์ขนาดใหญ่

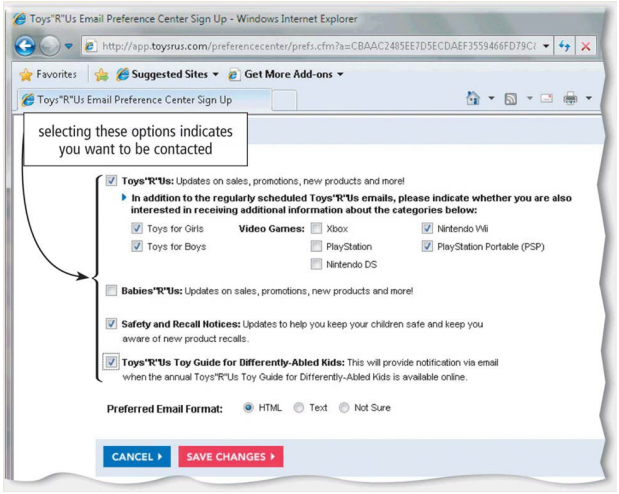
•มันเป็นสิ่งสำคัญในการปกป้องข้อมูล

How to Safeguard Personal Information

1. Fill in only necessary information on rebate, warranty, and registration forms.
2. Do not preprint your telephone number or Social Security number on personal checks.
3. Have an unlisted or unpublished telephone number.
4. If Caller ID is available in your area, find out how to block your number from displaying on the receiver's system.
5. Do not write your telephone number on charge or credit receipts.
6. Ask merchants not to write credit card numbers, telephone numbers, Social Security numbers, and driver's license numbers on the back of your personal checks.
7. Purchase goods with cash, rather than credit or checks.
8. Avoid shopping club and buyer cards.
9. If merchants ask personal questions, find out why they want to know before releasing the information.
10. Inform merchants that you do not want them to distribute your personal information.
11. Request, in writing, to be removed from mailing lists.
12. Obtain your credit report once a year from each of the three major credit reporting agencies (Equifax, Experian, and TransUnion) and correct any errors.
13. Request a free copy of your medical records once a year from the Medical Information Bureau.
14. Limit the amount of information you provide to Web sites. Fill in only required information.
15. Install a cookie manager to filter cookies.
16. Clear your history file when you are finished browsing.
17. Set up a free e-mail account. Use this e-mail address for merchant forms.
18. Turn off file and printer sharing on your Internet connection.
19. Install a personal firewall.
20. Sign up for e-mail filtering through your Internet access provider or use an anti-spam program such as Brightmail.
21. Do not reply to spam for any reason.
22. Surf the Web anonymously with a program such as Freedom WebSecure or through an anonymous Web site such as Anonymizer.com.

เมื่อกรอกข้อมูลรูปแบบการค้าที่ได้รับแบบฟอร์มมักจะเข้าไปในฐานข้อมูล

• ปัจจุบัน หลายบริษัทช่วยให้ผู้คนเพื่อระบุว่าพวกเขาต้องการส่วนตัวของพวกเขาข้อมูลกระจาย



Cookie คุกกี้เป็นแฟ้มข้อความขนาดเล็กที่เก็บเซิร์ฟเวอร์บนคอมพิวเตอร์ของคุณ

- เว็บไซต์ใช้คุกกี้เพื่อความหลากหลายของเหตุผล:
  - อนุญาตให้สำหรับส่วนบุคคล
  - รหัสผ่านที่ผู้ ใช้ร้านค้า

ช่วยให้มีการช้อปปิ้งออนไลน์
ติดตามว่าผู้ใช้มักจะเข้าเยี่ยมชมเว็บไซต์
โฆษณาเป้าหมาย

- **Spam** สแปมคือข้อความ e-mail หรือกลุ่มข่าวสารการโพสต์ที่ไม่พึงประสงค์
- **E-mail filtering** บล็อกข้อความอีเมลโดยการกำหนดที่มา
- **Anti-spam programs** โปรแกรมป้องกันสแปมพยายามที่จะลบสแปมก่อนที่จะถึงกล่องจดหมายของคุณ
- **Phishing** การหลอกลวงที่ผู้กระทำผิดจะส่ง e-mail ที่มองเหมือนเป็นทางการ พยายามที่จะขโมยข้อมูลส่วนบุคคลของคุณและข้อมูลทางการเงิน
- **Pharming** การหลอกลวงที่กระทำความผิด ความพยายามที่จะได้รับข้อมูลส่วนบุคคลและการเงินผ่านการปลอมแปลง

ความกังวลเกี่ยวกับความเป็นส่วนตัวได้นำไปสู่การตรากฎหมายของกฎหมายของรัฐบาลกลางและรัฐที่เกี่ยวข้องกับการจัดเก็บและการเปิดเผยข้อมูลส่วนบุคคล
- รายชื่อของยักษ์ใหญ่ในสหรัฐกฎหมายของรัฐบาลที่เกี่ยวข้องกับความเป็นส่วนตัว
- รายงานเครดิต 1970 งานพระราชบัญญัติ จำกัด สิทธิของผู้อื่นดูรายงานเครดิตเพียงผู้ที่มีธุรกิจที่ถูกกฎหมาย

Social engineering วิศวกรรมสังคม หมายถึง การไม่ได้รับอนุญาตหรือได้รับความลับ ข้อมูลโดยการใช้ประโยชน์จากความไว้วางใจและความไร้เดียงสา
Employee monitoring เกี่ยวข้องกับการใช้คอมพิวเตอร์ ให้สังเกตบันทึกและทบทวนการใช้พนักงานของจากคอมพิวเตอร์
Content filtering เป็นกระบวนการของการจำกัดการเข้าถึงเนื้อหาบางอย่างบนเว็บ
- ธุรกิจจำนวนมากที่ใช้การกรองเนื้อหา
- สมาคมจัดอันดับเนื้อหาอินเทอร์เน็ต Internet Content Rating Association (ICRA)

Web filtering software โปรแกรมที่จำกัด การเข้าถึงเว็บไซต์ที่ระบุไว้