

ความปลอดภัยและความเป็นส่วนตัว ในการใช้ คอมพิวเตอร์และอินเทอร์เน็ต

ทัศนวรรณ ศูนย์กลาง

ภาควิชาคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยศิลปากร



บทนำ

ความปลอดภัย

- การดูแลจัดการ ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูล ให้พ้นจากอันตรายต่าง ๆ เช่น อาชญากรรมคอมพิวเตอร์ ภัยธรรมชาติ ภัยคุกคามอื่นๆ

ความเป็นส่วนตัว

- การปกป้องข้อมูลส่วนตัวที่ไม่ต้องการเปิดเผยของผู้ใช้

อาชญากรรมคอมพิวเตอร์

อาชญากรคอมพิวเตอร์

- ◎ พนักงานหรือลูกจ้าง
- ◎ แฮกเกอร์ (Hacker)
- ◎ แครกเกอร์ (Cracker)
- ◎ บุคคลภายนอก

Kevin Mitnick : แฮกเกอร์ & แครกเกอร์

- ◎ แครกเกอร์

- ◎ เจาะระบบโทรศัพท์

- ◎ สร้างโปรแกรมขโมยรหัสผ่าน

- ◎ ลักลอบดาวน์โหลดซอฟต์แวร์
ที่มีลิขสิทธิ์คุ้มครอง



- ◎ แฮกเกอร์

- ◎ เปิดบริษัทรับปรึกษาและ
เผยแพร่ความรู้เกี่ยวกับ
ระบบรักษาความปลอดภัย

- ◎ เขียนหนังสือเกี่ยวกับระบบ
รักษาความปลอดภัย

รูปแบบของอาชญากรรม

- ◎ การปลอมแปลงข้อมูล/บัตรเครดิต
- ◎ การลักลอบเข้าระบบผ่านทาง การสื่อสารข้อมูล
- ◎ การเข้าถึงข้อมูลโดยผู้ไม่มีสิทธิ
- ◎ การทำสำเนาซอฟต์แวร์ที่มีลิขสิทธิ์
- ◎ การขโมยและทำลายอุปกรณ์
- ◎ การก่อวินาศกรรมด้วยโปรแกรมประสงค์ร้าย

วิธีก่ออาชญากรรมคอมพิวเตอร์

- ◎ การวางระเบิดเวลา (Bomb)
- ◎ การโกงข้อมูล (Data diddling)
เปลี่ยนแปลงแก้ไขก่อน/ขณะป้อนข้อมูลเข้าสู่ระบบ
- ◎ การโจมตีเว็บไซต์ (Denial of service-[DOS] attract)
ทำให้ผู้มีสิทธิ์ใช้เข้าไม่ได้
- ◎ การหลอกลวงข้อมูล ผ่านทางอีเมล/โทรศัพท์/พูดคุย
(Social engineering)

วิธีก่ออาชญากรรมคอมพิวเตอร์

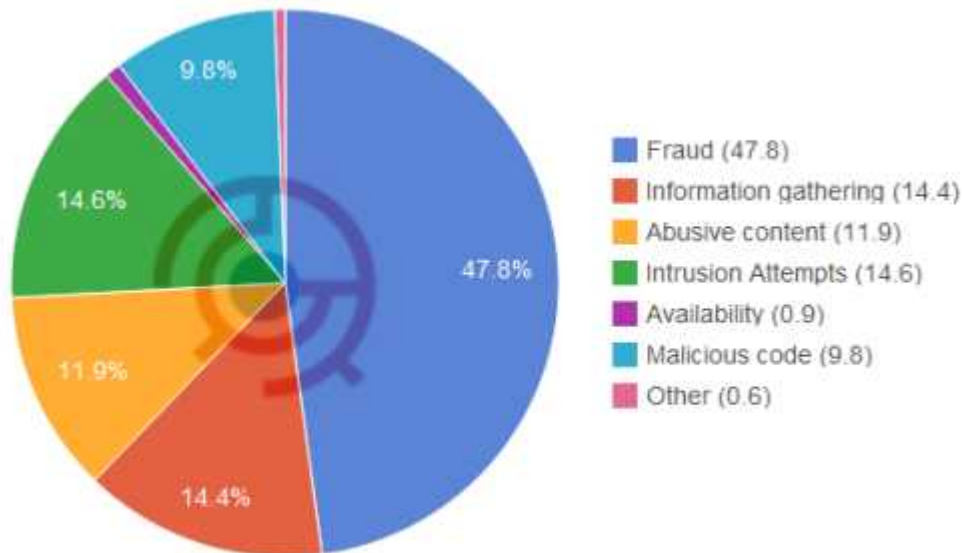
- ◎ การแอบใช้ (Piggybacking)
ฉวยโอกาสใช้งานกรณีที่ผู้ใช้ไม่ logout
- ◎ การขโมยทีละเล็กละน้อย (Salami technique)
เงินเล็กละน้อยที่อาจมองข้าม
- ◎ การเก็บจากขยะ (Scavenging) ค้นหาข้อมูลที่สำคัญจากถังขยะ

วิธีก่ออาชญากรรมคอมพิวเตอร์

- ◎ โปรแกรมกับดัก (Trapdoor/backdoor)
แอบทำช่องทางในการเข้าถึงโปรแกรมได้
- ◎ โปรแกรมม้าโทรจัน (Trojan horse)
ทำลายโปรแกรม/ข้อมูล เมื่อมีการคัดลอก
- ◎ โปรแกรมแซบ (Zapping) โปรแกรมใช้เจาะระบบ

วิธีก่ออาชญากรรมคอมพิวเตอร์

- ◎ Phishing - การหลอกลวงโดยใช้อีเมลล์หรือหน้าเว็บไซต์ปลอม เพื่อให้ได้มาซึ่งข้อมูล
- ◎ ไม่เปิดลิงก์ที่แนบมาในอีเมลล์
- ◎ พึงระวังอีเมลล์ที่ขอให้กรอกข้อมูลส่วนบุคคล โดยเฉพาะหากเป็นอีเมลล์ที่มาจากสถาบันการเงิน
- ◎ สังเกตให้แน่ใจว่าเว็บไซต์ที่ใช้งานเป็น [HTTPS](#) ก่อนให้ข้อมูลส่วนบุคคลที่สำคัญ เช่น เลขบัตรเครดิต หรืออื่น ๆ
- ◎ ลบอีเมลล์น่าสงสัยออกไป เพื่อไม่ให้พลังเมลออกดเปิดครั้งถัดไป
- ◎ ติดตั้งโปรแกรม Anti-Virus, Anti-Spam และ Firewall



สถิติภัยคุกคาม ในช่วงปี 2554

MICROSOFT OFFICIAL WINNING

ดดย.mail ไม่ดี x

Microsoft Corporation Remittance Desk mikefowler@charter.net

to undisclosed recipients

The Microsoft Mega Jackpot Lottery, United Kingdom wishes to inform you that the International Program held in Great Britain is out. Your e-mail account has been selected as the winning account of £1,550,952.00 (One Million Five Hundred And Fifty Thousand Nine Hundred And Fifty Two Pounds) (LOTTERY) CHIP NO:9465206. The winning ticket was selected from a Draw on 10/05/2011. You came out as the winning coupon in this category "A" ballot lottery. You are the winner.

You are to contact the Claims Consultant with the details below:
 Contact Person: Mr. Nicholas Caldwell.
 E-mail : m.corporationclaimsdesk2011@xmsn.com

THE BENEFICIARY/OWNER OF THE WINNING E-MAIL SHOULD COMPLETE OUR CLAIMS FORM.

FILL THE INFORMATION BELOW:

Name:
 Age:

From: PayPal Billing Department <Billing@PayPal.com>
 Subject: **Credit/Debit card update**
 Date: May 4, 2006 08:16:08 PDT
 To: @bustspammers.com
 Reply-To: Billing@PayPal.com



Dear Paypal valued member,

Due to concerns, for the safety and integrity of the paypal account we have issued this warning message.

It has come to our attention that your account information needs to be updated due to inactive members, frauds and spoof reports. If you could please take 5-10 minutes out of your online experience and renew your records you will not run into any future problems with the online service. However, failure to update your records will result in account suspension. This notification expires on 48.

Once you have updated your account records your paypal account service will not be interrupted and will continue as normal.

Please follow the link below and login to your account and renew your account information

https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

Sincerely,
 Paypal customer department

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.

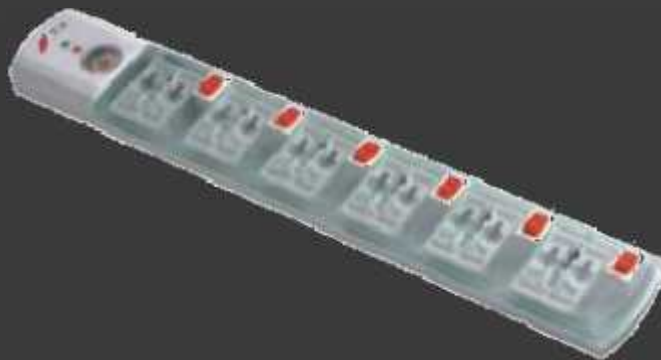
To receive email notifications in plain text instead of HTML, update your preferences [here](#).

ความปลอดภัย

- ◎ ความปลอดภัยของเครื่องคอมพิวเตอร์
- ◎ ความปลอดภัยของซอฟต์แวร์
- ◎ ความปลอดภัยของข้อมูล

ความปลอดภัยของคอมพิวเตอร์

- การป้องกันการโจรกรรม
- การใช้งานอย่างระมัดระวัง
- การใช้อุปกรณ์ไฟฟ้าสำรอง
- การป้องกันความเสียหาย



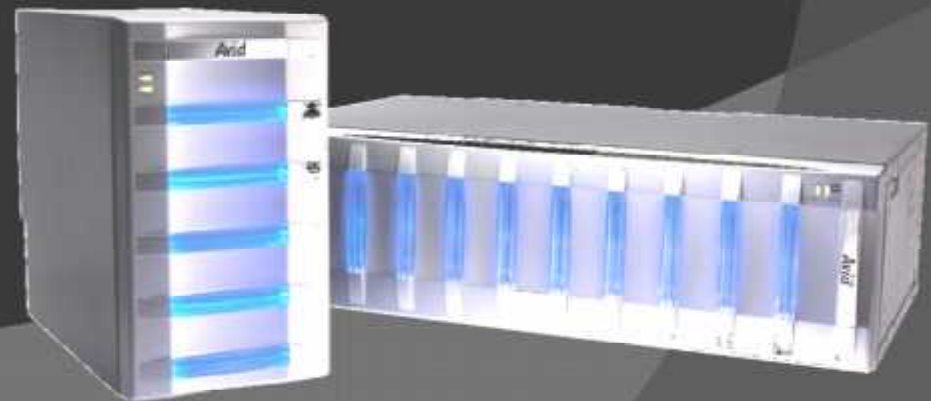
ความปลอดภัยของซอฟต์แวร์

- ◎ กรรมสิทธิ์ของซอฟต์แวร์
 - Freeware
 - Shareware/trial ware
- ◎ การละเมิดลิขสิทธิ์
- ◎ การโจรกรรมซอฟต์แวร์
- ◎ การป้องกันความเสียหาย



ความปลอดภัยของข้อมูล

- ◎ แผนการป้องกันข้อมูล
- ◎ การโจรกรรมข้อมูล
- ◎ การเข้าถึงข้อมูลเฉพาะผู้มีสิทธิ
- ◎ การป้องกันความเสียหาย
- ◎ การสำรองข้อมูล



การป้องกัน

◎ การระบุตัวผู้ใช้และการเข้าถึงข้อมูล

- การใช้รหัสผ่าน
- การระบุผู้ใช้โดยใช้ลักษณะทางพันธุกรรม:
ลายนิ้วมือ ลายมือ ใบหน้า ม่านตา
- การใช้ลายเซ็น เสียงพูด
- การบัตรผ่าน
- การปฏิบัติตน



การป้องกัน

- ◎ การทำลายข้อมูลทิ้ง
- ◎ การควบคุมภายใน (log file)
- ◎ การตรวจเช็คจากผู้ตรวจสอบ
- ◎ การตรวจสอบผู้สมัคร
- ◎ โปรแกรมป้องกัน

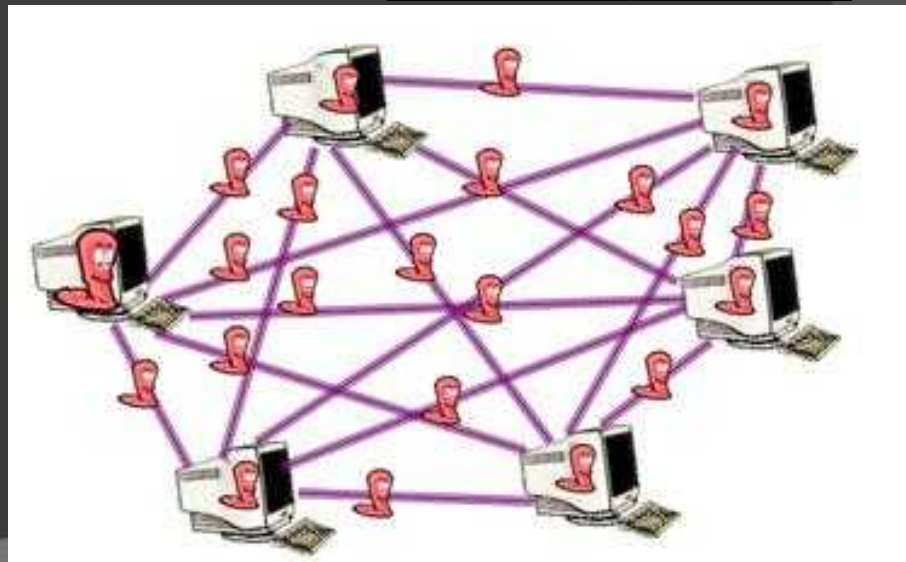
ไวรัสคอมพิวเตอร์

- ◎ โปรแกรมที่ออกแบบให้สามารถแพร่กระจายตัวเองภายในคอมพิวเตอร์ได้
- ◎ แพร่กระจายโดยเกาะติดไปกับไฟล์
- ◎ ความเสียหายขึ้นอยู่กับรายละเอียดการทำงานภายใน
- ◎ การป้องกัน
 - ทำได้โดยติดตั้งโปรแกรมตรวจสอบไวรัส
 - ไม่นำไฟล์จากแหล่งอื่นเข้าสู่เครื่อง



ชนิดของไวรัสคอมพิวเตอร์

- ไวรัสบูตเซ็กเตอร์ (boot sector virus)
- ไวรัสคลัสเตอร์ (cluster virus)
- ไวรัสโปรแกรม (file-infecting virus)
- ไวรัสมาโคร (macro virus)
- เวิร์ม (worm)
- บอมบ์ (bomb)
- ม้าโทรจัน (trojan horse)



ความเสียหายจากไวรัส

- ◎ ทำลายข้อมูล
- ◎ ขโมยข้อมูลสำคัญ
- ◎ ฟอรัมแฮตฮาร์ดดิสก์
- ◎ ทำให้โปรแกรมทำงานผิดพลาด
- ◎ ก่อความรำคาญ
- ◎ ทำให้เครื่องทำงานช้า/ทำงานต่อไม่ได้
- ◎ ทำให้ระบบเครือข่ายขององค์กรช้า

ความปลอดภัยและความเป็นส่วนตัว บนอินเทอร์เน็ต

- ◎ Hoax mail
- ◎ Spam mail
- ◎ Junk mail
- ◎ Cookie
- ◎ Adware
- ◎ Spyware

<http://www.thaicert.org/>



ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย

ThaiCERT:

Thai Computer Emergency Response Team

การใช้งานอินเทอร์เน็ตอย่างปลอดภัย

- ◎ อ่านข้อตกลง นโยบายให้ดีก่อนตอบตกลงใดๆ
- ◎ ระมัดระวังการใช้บริการเครื่องคอมพิวเตอร์สาธารณะ
 - แอบดูการใช้งาน
 - หลีกเลี่ยงการใส่ข้อมูลสำคัญมากๆ
 - ไม่ให้ระบบช่วยจำ username และ password
- ◎ หมั่นเปลี่ยน password บ่อยๆ
- ◎ หมั่นลบ temporary internet files, cookies และ history
- ◎ Logoff หรือ logout ทุกครั้งหลังใช้งาน

การตั้งรหัสผ่าน

◎ ตัวอย่างที่เดาง่าย

- ชื่อตัวเอง ชื่อบริษัท
- วันเกิด
- เลขพนักงาน
- คำที่ใช้ทั่วไป
- ตัวอักษรซ้ำๆ
- รหัสที่สั้น

◎ ตัวอย่างที่เดายาก

- ประกอบด้วยคำหลายคำ
- มีทั้งตัวเลข ตัวอักษร และสัญลักษณ์พิเศษผสมกัน
- ความยาวตั้งแต่ 8 ตัวขึ้นไป

◎ ไม่ควร

- เขียนรหัสผ่านใส่กระดาษ
- ไม่ส่งรหัสผ่านไปทางอีเมล หรือแจ้งทางโทรศัพท์

กฎหมายที่เกี่ยวข้อง

พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
พ.ศ. 2550 (ผู้ใช้บริการ)

- ⦿ การเผยแพร่ข้อมูลที่ไม่เหมาะสม
- ⦿ การติดต่อภาพผู้อื่น
- ⦿ การเข้าถึงคอมพิวเตอร์โดยมิชอบ
- ⦿ การเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ
- ⦿ การรบกวนระบบคอมพิวเตอร์
- ⦿ การรบกวนข้อมูลคอมพิวเตอร์
- ⦿ การดักข้อมูลคอมพิวเตอร์
- ⦿ การเปิดเผยมาตรการป้องกันการเข้าถึง
- ⦿ การจำหน่าย/เผยแพร่ชุดคำสั่ง
- ⦿ การกระทำต่อความมั่นคง
 - ก่อความเสียหายแก่ข้อมูล
 - กระทบต่อความมั่นคง
 - อันตรายแก่ร่างกาย/ชีวิต

กฎหมายที่เกี่ยวข้อง

พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
พ.ศ. 2550 (ผู้ให้บริการ)

ข้อมูลผู้ใช้บริการ

- ชื่อ-สกุล, วัน-เวลาที่ใช้งาน
- การออกสู่อินเทอร์เน็ตของทุกคน รวมทั้งอินเทอร์เน็ต
- การเข้าใช้งานweb server
- การเข้าใช้งานเครือข่าย
- การรับส่งอีเมล

วิธีการ

- เก็บข้อมูลสำคัญของผู้ใช้บริการไม่น้อยกว่า 90 วัน
- มีระบบ login เข้าใช้งานเครือข่าย
- มีระบบ gateway authentication
- ตั้ง time server เดียวกัน
- มีผู้ดูแลฝัง IP address ของผู้ใช้