ระบบรักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์

introducing

Computer Network Security

หัวข้อการบรรยาย (Agenda)

1.
2. แนวคิดเกี่ยวกับระบบรักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์
3. ปล[illegible]กร
4. การป้องกัน
5. สรุป

1 แนะนำตัว

นายเกรียงศักดิ์ เหล็กดี
ตำแหน่งวิศวกรระบบเครือข่าย
ฝ่ายบริหารระบบเครือข่าย
สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา
โทร: 02-3545678 ต่อ 5006
E-MAIL: NOC@UNI.NET.TH

UniNet

ชั้น 9 อาคารสำนักงานคณะกรรมการการอุดมศึกษา

แนวคิดเกี่ยวกับ ระบบรักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์

สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา

แนวคิดเกี่ยวกับระบบรักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์

- เกิดขึ้นเนื่องจากบุคคลที่ไม่ประสงค์ดีเข้ามาทำลายข้อมูลภายในระบบคอมพิวเตอร์ด้วยรูปแบบต่างๆ
  - การส่งไวรัสเข้าสู่ระบบคอมพิวเตอร์
  - การละเมิดข้อมูลส่วนบุคคลของผู้อื่น โดยการหลอกลวงด้วยวิธีต่างๆ
  - ความพยายามที่จะใช้อุบายหรือขโมยรหัสผู้ใช้งาน เพื่อข้ามผ่านระบบรักษาความปลอดภัยเข้าสู่ระบบข้อมูลและเครือข่าย
- ต้องมีการเพิ่มความสามารถในการรักษาความปลอดภัยให้กับระบบคอมพิวเตอร์ของตนให้มากขึ้น

คำศัพท์ หรือ คำจำกัดความในด้าน security

- **Security** การปกป้องที่ทำให้เกิดความมั่นใจว่าการกระทำหรืออิทธิพล ที่ไม่เป็นมิตรไม่สามารถจะมีผลกระทบได้
- **Information Security** การรักษาความปลอดภัย โดยการใช้นโยบายหรือ ระเบียบปฏิบัติ
- **Hacking** การใช้โดยไม่ได้รับอนุญาต หรือ การพยายามที่จะใช้อุบายหรือข้ามผ่านระบบรักษาความปลอดภัยเพื่อเข้าสู่ระบบข้อมูลและ เครือข่าย

คำศัพท์ หรือ คำจำกัดความในด้าน security

- Hacker
  - เสาะค้นหารายละเอียดเกี่ยวกับเครื่องคอมพิวเตอร์และวิธีการที่จะใช้เครื่องให้ได้เต็มหรือเกินขีดความสามารถของเครื่อง
  - พยายามจะให้ได้มาซึ่งข้อมูลโดยการสอดแนมในที่ต่างๆ
  - เรียนรู้และใช้โปรแกรมให้ได้เต็มหรือเกินขีดความสามารถ ซึ่งตรงข้ามกับผู้ใช้ทั่วๆ ไปที่ต้องการที่จะเรียนรู้เพียงเท่าที่จำเป็นต้องใช้งานเท่านั้น
  - โจมตีเครื่องคอมพิวเตอร์เพื่อความท้าทาย ความมีชื่อเสียง หรือความตื่นเต้นที่จะได้มาเมื่อประสบความสำเร็จ

คำศัพท์ หรือ คำจำกัดความในด้าน security

- **Cracker** ผู้ที่ใช้ทักษะในการ hacking เพื่อจุดประสงค์ในการบุกรุก ทำลาย ระบบ และ รวมทั้งการลักลอบขโมยข้อมูลของบุคคลอื่น
- **Ethical hacker** ผู้เชี่ยวชาญทางด้าน security ผู้ซึ่งใช้ทักษะในการ hacking เพื่อจุดประสงค์ในการป้องกันระบบ
- **Threat** ภัยคุกคามหรือ สิ่งที่ละเมิดระบบรักษาความปลอดภัย และอาจก่อให้เกิดผลกระทบซึ่งเป็นอันตรายต่อระบบ

คำศัพท์ หรือ คำจำกัดความในด้าน security

- Vulnerability
  - ช่องโหว่หรือจุดบกพร่องในระบบ
  - รูปแบบการทำงานทาง ฮาร์ดแวร์ เฟิร์มแวร์ หรือซอฟท์แวร์ ที่สามารถเปิดโอกาสให้ระบบข้อมูลอัตโนมัติถูกเจาะได้
  - ข้อบกพร่องในระเบียบปฏิบัติด้านความปลอดภัย การควบคุมการจัดการ การวางแผนผังทางกายภาพ การควบคุมภายใน และอื่นๆ ของระบบอัตโนมัติที่เปิดโอกาสให้สิ่งที่เป็นภัยคุกคามสามารถเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตหรือสามารถสร้างความเสียหายให้กับกรรมวิธีที่มีความสำคัญได้

คำศัพท์ หรือ คำจำกัดความในด้าน security

- Attack
  - การโจมตี หรือ ความพยายามที่จะข้ามผ่านระบบการรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ ซึ่งการโจมตีนั้นอาจทำให้เกิดการเปลี่ยนแปลงของข้อมูล ข้อมูลถูกเปิดเผย ข้อมูลหายไป หรืออาจจะเป็นการโจมตีเพื่อให้ระบบหรือเครื่องคอมพิวเตอร์นั้น ไม่สามารถให้บริการได้ โดยการโจมตีจะประสบผลสำเร็จหรือไม่นั้นขึ้นอยู่กับช่องโหว่ของระบบคอมพิวเตอร์และประสิทธิผลของมาตรการรักษาความปลอดภัยของระบบนั้นๆ

การรักษาความปลอดภัยในองค์กร

ภัยคุกคามที่เกิดขึ้นกับระบบรักษาความปลอดภัยคอมพิวเตอร์มี 5 รูปแบบคือ

1) ภัยคุกคามแก่ระบบ ได้แก่ การปรับปรุง,แก้ไข,เปลี่ยนแปลง,หรือลบไฟล์คอมพิวเตอร์
2) ภัยคุกคามความเป็นส่วนตัว เข้ามาเจาะข้อมูลส่วนบุคคล,การใช้โปรแกรม Spyway
3) ภัยคุกคามต่อทั้งผู้ใช้และระบบ เช่น JavaScript,JavaApplet หรือบังคับให้ผู้ใช้งานปิดโปรแกรม Browser ขณะที่ทำงานอยู่
4) ภัยคุกคามที่ไม่มีเป้าหมาย เพียงสร้างจุดสนใจ , Spam
5) ภัยคุกคามที่สร้างความรำคาญ แอบเปลี่ยนค่าการทำงานของคอมพิวเตอร์

การรักษาความปลอดภัยในองค์กร

- บุคคลผู้ไม่ประสงค์ดีต่อองค์กรสามารถแบ่งออกเป็น 2 ประเภทได้แก่

1. การบุกรุกทางกายภาพ (เข้าถึงระบบได้โดยตรง) การคัดลอกข้อมูล,การขโมย
2. การบุกรุกทางเครือข่ายคอมพิวเตอร์ การปล่อยไวรัส,การเจาะข้อมูล

ความปลอดภัยจากคอมพิวเตอร์ (Computer Security)

- Computer Viruses
- Virus Detection and Removal
- Unauthorized Access and Use
- Hardware Theft
- Software Theft
- Information Theft
- System Failure
- Backup Procedures

ไวรัสคอมพิวเตอร์(Computer Viruses)

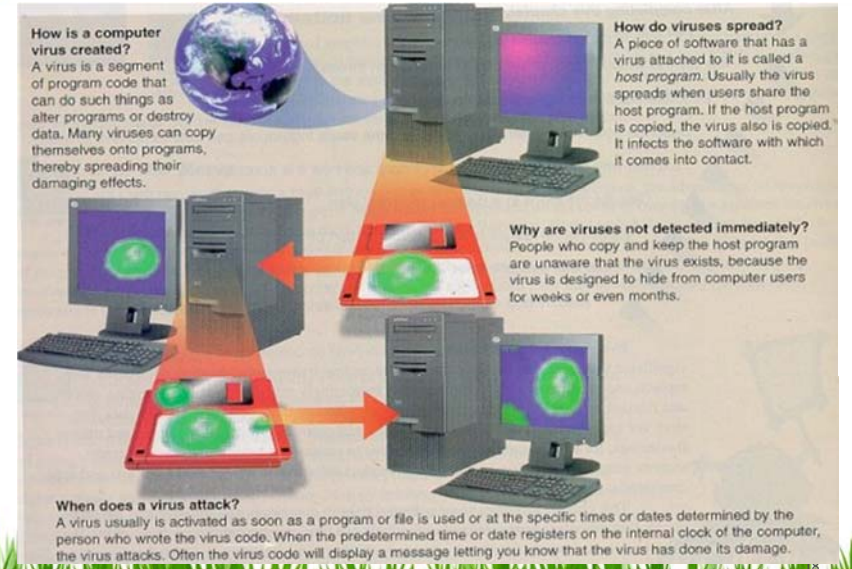
- ไวรัสเป็นกลุ่มของคำสั่ง ที่ถูกสร้างขึ้นมาด้วยเหตุผลหลายประการ เช่นรบกวนการทำงาน ก่อให้เกิดความรำคาญ เปลี่ยนแปลงข้อมูล ทำให้ข้อมูลเสียหาย หรือทำลายอุปกรณ์คอมพิวเตอร์
- โดยส่วนใหญ่มักติดต่อโดยที่ผู้ใช้ไม่ทราบ
- Worm เป็นไวรัสที่สามารถทำงานได้โดยตัวเอง
- ไวรัส เป็นกลุ่มคำสั่งที่ติดหรือแฝงกับสิ่งอื่นๆ

ไวรัสคอมพิวเตอร์(Computer Viruses)

ลักษณะการทำงานของไวรัส

- สามารถสำเนาตัวเองไปยังไฟล์ข้อมูลอื่นหรือคอมพิวเตอร์เครื่องอื่นๆได้
- รบกวนการทำงานของผู้ใช้เช่น แสดงเสียงหรือทำให้การแสดงผลบนจอภาพผิดปกติ
- เปลี่ยนแปลงหรือทำลายไฟล์ข้อมูล
- เปลี่ยนแปลงหรือทำให้อุปกรณ์เสียหาย

ไวรัสคอมพิวเตอร์(Computer Viruses)

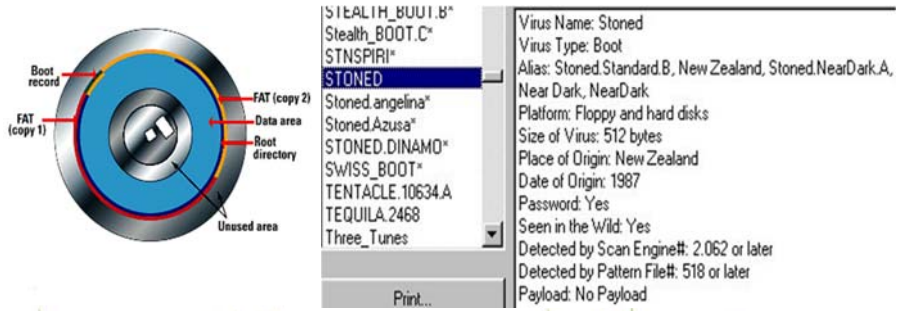


ชนิดของไวรัสคอมพิวเตอร์

1. ไวรัสบูตเซกเตอร์ (Boot Sector Virus)
2. ไวรัสไฟล์ข้อมูล (File Virus)
3. โทรจันไวรัส (Trojan Horse Virus)
4. มาโครไวรัส (Macro Virus)
5. อีเมลล์ไวรัส (Email Virus)

ไวรัสบูตเซกเตอร์ (Boot Sector Virus)

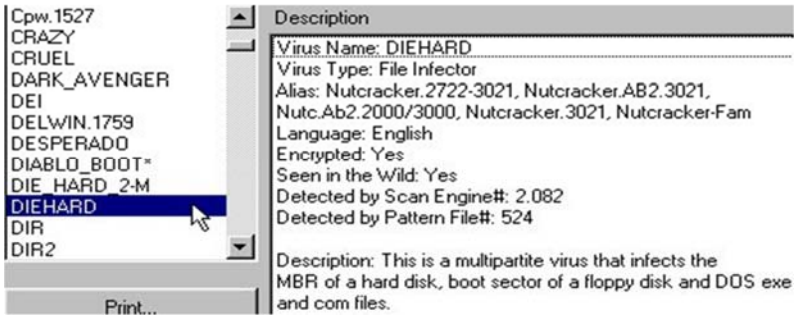
- เป็นไวรัสที่แฝงตัวในบูตเซกเตอร์ของแผ่นดิสก์ ทุกครั้งที่มีการใช้แผ่นดิสก์จะต้องมีการอ่านข้อมูลในบูตเซกเตอร์ทุกครั้ง ทำให้โอกาสติดไวรัสได้ง่าย ต.ย. Stoned, Angelina, Beijing



ไวรัสไฟล์ข้อมูล (File Virus)

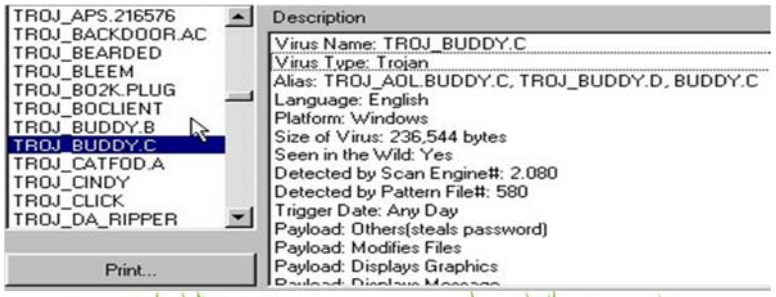
เป็นไวรัสที่ติดกับไฟล์ข้อมูลหรือไฟล์โปรแกรมต่างๆ โดยมากจะติดกับๆ ไฟล์ที่มักเรียกใช้บ่อย เช่น ไฟล์นามสกุล .exe, .dll, .com

ตัวอย่าง Jerusalem, Die Hard II



โทรจันไวรัส (Trojan Horse Virus)

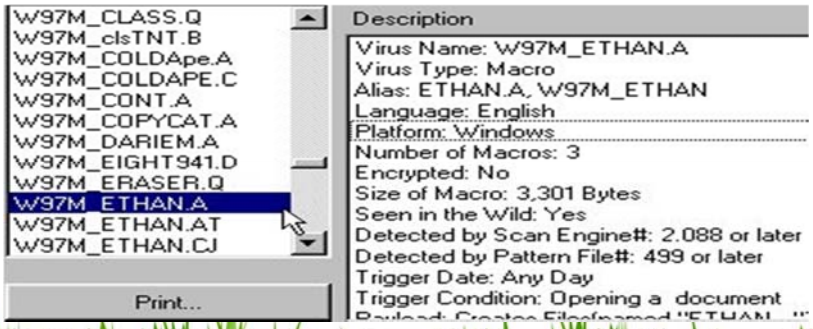
เป็นไวรัสที่แฝงมากับไฟล์อื่นๆ ที่ดูแล้วไม่น่าจะมีอันตรายใดๆ เช่น เกมส์ โปรแกรมฟรีแวร์หรือแชร์แวร์เมื่อใช้ไประยะเวลาหนึ่งแล้ว ไวรัสก็จะแสดงตัวออกมา ซึ่งอาจทำลายระบบคอมพิวเตอร์ของเรา



มาโครไวรัส (Macro Virus)

เป็นไวรัสที่เขียนขึ้นมาจากคำสั่งภาษามาโคร ที่มีอยู่ใน โปรแกรมประมวลผลคำ, หรือโปรแกรมในชุดไมโครซอฟต์ออฟฟิส เมื่อเราเปิดเอกสารที่มีไวรัส ไวรัสก็จะแพร่กระจายไปยังไฟล์อื่น

เช่น Concept, Bandung



อีเมลล์ไวรัส (Email Virus)

ปัจจุบันมีการใช้อีเมลล์ในการสื่อสารกันมาก แม้เพียงเราเข้าไปดูรายชื่อของจดหมายก็ติดไวรัสได้แล้ว ซึ่งอาจมีไวรัสแพร่กระจายมาด้วย ความร้ายแรงก็อยู่ที่ปริมาณอีเมลล์ที่แพร่กระจายไปจนอาจทำให้เครื่อง Server ไม่สามารถทำงานได้

เช่น Love Bug, Anna Kunicova

การกระตุ้นการทำงานของไวรัส (Activate Virus)

1. การเรียกใช้โปรแกรมหรือเข้าใช้ข้อมูลที่ติดไวรัส (Access or run an infected files)
2. เมื่อทำตามเงื่อนไขที่กำหนดไว้ (Logic bomb) เช่น เงื่อนไขหากผู้ใช้ Save ข้อมูลไวรัสก็จะทำงาน
3. เมื่อถึงเวลาที่กำหนดไว้ (Time Bomb)

   เช่น Michelangelo จะทำงานเมื่อถึงวันที่ 6 มีนาคม

การป้องกันและกำจัดไวรัส

Virus Detection and Removal

1. Hardware

   ใช้อุปกรณ์ฮาร์ดแวร์ในการป้องกันและกำจัดไวรัส เช่น Antivirus card ราคาประมาณ 1000 กว่าบาท

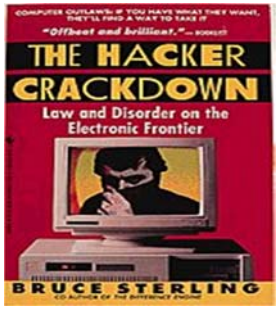
2. Software

   ใช้ซอฟแวร์ในการป้องกันและกำจัดไวรัส ซึ่งสามารถอัพเกรดได้ง่ายกว่า เช่น Mcafee, Norton, TrendMicro

การเข้าสู่ระบบและใช้คอมพิวเตอร์โดยไม่ได้รับอนุญาติ

Unauthorized Access and Use

เป็นการเข้าสู่ระบบและใช้คอมพิวเตอร์โดยไม่ได้รับอนุญาติ โดยพวก Cracker หรือ Hacker ซึ่งพยามยามที่เจาะเข้าสู่ระบบและโขมยข้อมูล ส่วนใหญ่ผ่านทางระบบเครือข่าย เช่นขโมยข้อมูลบัตรเครดิต เจาะระบบหน่วยงานของรัฐบาลหรือองค์กรหรือเจาะเวปไซต์ของบริษัทต่างๆ



การป้องกัน

การป้องกันโดยการควบคุมการเข้าถึง(Access Control)

- **Access Control** คือ ระบบควบคุมการเข้าใช้งาน เป็นวิธีการป้องกันการโจรกรรมข้อมูลจากผู้ไม่มีสิทธิ์ในการเข้าใช้ระบบ ปัจจุบันแบ่งออกเป็น 5 รูปแบบดังนี้

1. ชื่อผู้ใช้และรหัสผ่าน (UserName and Password)
2. วัตถุครอบครอง (Possessed Object)
3. ใช้อุปกรณ์ Biometric
4. ซอฟต์แวร์ตรวจจับการบุกกรุก
5. ผู้ให้บริการจัดการความปลอดภัย

1.ชื่อผู้ใช้และรหัสผ่าน (UserName and Password)

การกำหนดรหัสผ่านกับรหัสการเข้าใช้โดยซึ่งที่ต้องพิจารณามี 2 อย่างคือเพื่อให้สามารถรักษาความปลอดภัยได้ดียิ่งขึ้น เช่น

- ต้องมีความยากมากพอสมควรอย่างน้อยขั้นต่ำ 6 อักษร
- ไม่ควรเป็นชื่อเล่น,วันเกิด,หรือสิ่งที่คาดเดาได้ง่าย

2. วัตถุครอบครอง (Possessed Object)

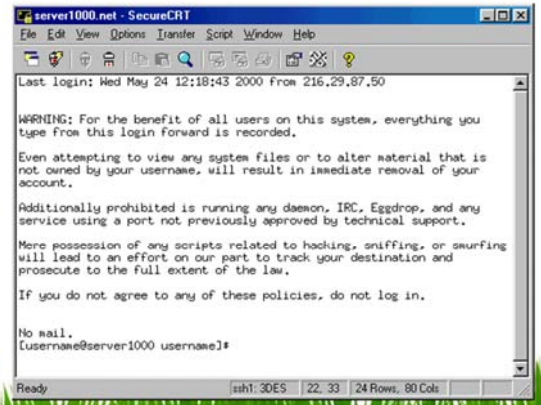
เป็นรูปแบบหนึ่งที่นิยมใช้ในปัจจุบัน การเข้าใช้คอมพิวเตอร์ต้องมีกุญแจในการเข้าใช้ระบบเช่น ATM , Keycard เป็นต้น

3.ใช้อุปกรณ์ Biometric

- เป็นอุปกรณ์รักษาความปลอดภัยโดยใช้คุณลักษณะเฉพาะของร่างกาย ได้แก่ ตา, นิ้วมือ,ฝ่ามือเป็นต้น

4.ซอฟต์แวร์ตรวจจับการบุกรุก

- คอยตรวจสอบการเข้าใช้ทรัพยากรของเครือข่าย แล้วรายงานไปยังผู้ดูแลระบบรักษาความปลอดภัยการตรวจสอบการ Login การเข้าใช้งาน



5.ผู้ให้บริการจัดการความปลอดภัย

คอยตรวจสอบและดูแลรักษาฮาร์ดแวร์และซอฟต์แวร์ ตลอดจนรักษาความปลอดภัยของเครือข่ายให้เหมาะสมกับองค์กรขนาดเล็ก-ขนาดใหญ่

Hardware Theft

เป็นการป้องกันการโจรกรรมอุปกรณ์ฮาร์ดแวร์ อาจใช้อุปกรณ์เสริมเพื่อป้องกันหรือถ่วงเวลาให้ได้มากที่สุด

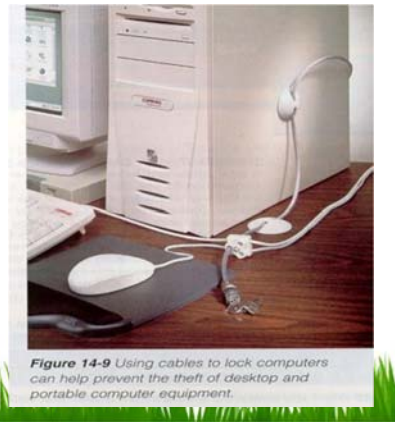


Figure 14-9 Using cables to lock computers can help prevent the theft of desktop and portable computer equipment.

Software Theft

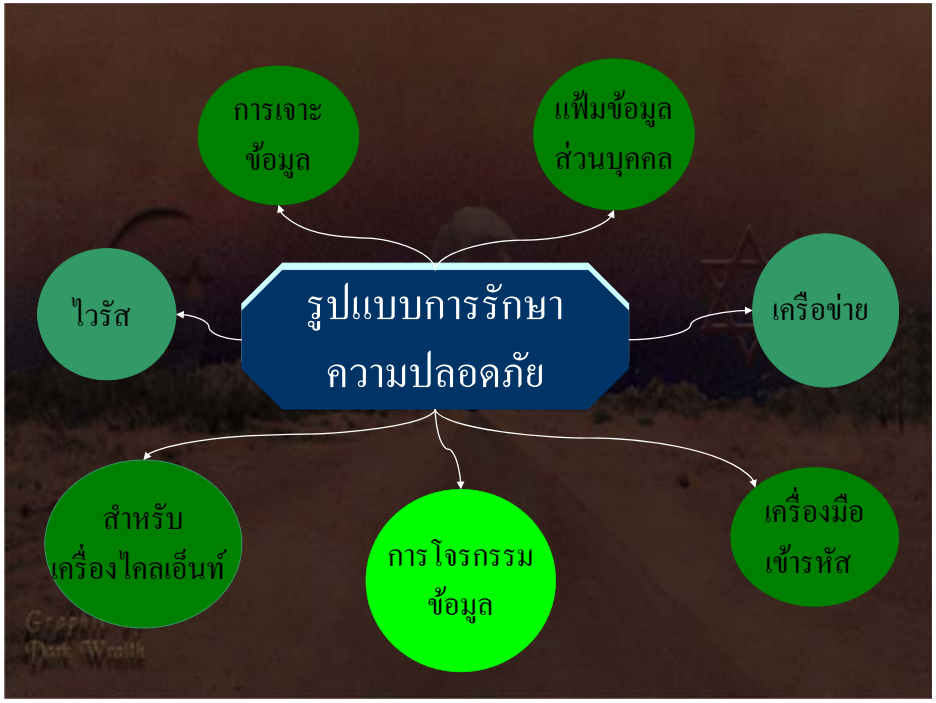
โดยทั่วไปผู้ใช้ซอฟแวร์ต้องปฏิบัติตามข้อตกลงการนำไปใช้จากผู้ผลิต (Software License) เช่น

1. ผู้ซื้อต้องใช้กับคอมพิวเตอร์ได้เพียงเครื่องเดียวเท่านั้น
2. ผู้ซื้อทำสำเนาได้เพียง 1 ชุดสำหรับการสำรองเท่านั้น
3. ผู้ซื้อไม่สามารถทำสำเนาเพื่อแจกจ่ายหรือให้ผู้อื่นยืมหรือนำไปใช้
4. ห้ามโหลดซอฟแวร์ลงเครื่อง Server

การกระทำอื่นใดที่นอกเหนือจากที่กำหนดไว้ถือเป็นการละเมิดสิทธิ์ของผู้ผลิตทั้งสิ้น ซึ่งถือว่าผิดกฎหมาย

สรุป ระบบรักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์

สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา



ช่วงตอบคำถาม?