แนวข้อสอบ (อัตนัย)
พระราชบัญญัติว่าด้วยการกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

1. พระราชบัญญัติว่าด้วยการกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 กำหนดฐานความผิดเกี่ยวกับคอมพิวเตอร์ไว้อย่างไรบ้าง ให้กล่าวถึงฐานความผิดและยกตัวอย่างลักษณะการกระทำความผิด ประกอบพอเข้าใจโดยสังเขป

ตอบ พระราชบัญญัติว่าด้วยการกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 กำหนดฐานความผิดเกี่ยวกับคอมพิวเตอร์ไว้ดังต่อไปนี้

1. การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ (มาตรา 5) เช่น การใช้โปรแกรมสปายแวร์ขโมยข้อมูลรหัสผ่านส่วนบุคคลของผู้อื่นเพื่อใช้บุกรุก เข้าไปในระบบคอมพิวเตอร์ของผู้นั้นโดยไม่ได้รับอนุญาต

2.การล่วงรู้ มาตรการป้องกันการเข้าถึงและนำไปเปิดเผยโดยมิชอบ (มาตรา 6) เช่น การใช้โปรแกรม Keystroke แอบบันทึกการกดรหัสผ่านของผู้อื่นแล้วนำไปโพสต์ในเว็บบอร์ดต่างๆเพื่อให้ บุคคลที่สามใช้เป็นรหัสผ่านเข้าไปในระบบคอมพิวเตอร์ของผู้ที่เป็นเหยื่อ

3.การ เข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ (มาตรา 7) เช่น การกระทำใดๆเพื่อเข้าถึงแฟ้มข้อมูลที่เป็นความลับโดยไม่ได้รับอนุญาต ด้วยการแอบเจาะเข้าระบบรักษาความปลอดภัย (hack) ไปล้วงข้อมูลของเขาโดยเขาไม่อนุญาต

4.การดักข้อมูลคอมพิวเตอร์โดยมิ ชอบ (มาตรา 8) หรือการดักรับข้อมูลของผู้อื่นในระหว่างการส่ง เช่น การใช้โปรแกรมสนิฟเฟอร์แอบดักชุดข้อมูลที่อยู่ระหว่างการส่งไปให้ผู้รับ

5.การ รบกวนข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์โดยมิชอบ (มาตรา 9 และ 10) เช่น การแอบส่งไวรัส หนอนอินเตอร์เน็ต หรือโทรจัน เข้าไปในระบบคอมพิวเตอร์ของผู้อื่นจนทำให้ข้อมูลหรือระบบของเขาเสียหาย

6.การส่ง สแปมเมล์ (spam) หรืออีเมล์ขยะ (มาตรา 11) ความผิดตามข้อมูลนี้เพิ่มเติมขึ้นมาเพื่อให้ครอบคลุมถึงการส่งสแปมเมล์ ซึ่งเป็นลักษณะการกระทำความผิดที่ใกล้เคียงกับมาตรา 10 และยังเป็นการทำความผิดโดยการใช้โปรแกรมหรือข้อความส่งไปให้เหยื่อจำนวนมากๆ โดยปกปิดแหล่งที่มา เช่น ไอพีแอดเดรส (IP address) ซึ่งมักก่อให้เกิดความเสียหายต่อการใช้คอมพิวเตอร์ ยกตัวอย่างเช่น การโฆษณาขายสินค้าทางอีเมล์ ที่ชอบส่งซ้ำๆจนทำให้เขาเบื่อหน่ายรำคาญ

7.การ กระทำความผิดที่ก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อความมั่นคงของประเทศ (มาตรา 12) การรบกวนหรือเจาะระบบและข้อมูลคอมพิวเตอร์ที่ก่อให้เกิดความ

เสียหายต่อ ประชาชนหรือกระทบต่อความมั่นคงของประเทศความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจและการบริการสาธารณะ

8. การจำหน่ายหรือเผยแพร่ชุดคำสั่งเพื่อใช้กระทำความผิด (มาตรา 13) เช่น การสร้างซอฟต์แวร์เพื่อช่วยให้ผู้ใดทำเรื่องที่เป็นความผิดต่างๆ เกี่ยวกับคอมพิวเตอร์

9.การปลอมแปลงข้อมูลคอมพิวเตอร์หรือเผยแพร่ เนื้อหาที่ไม่เหมาะสมและการรับผิดของผู้ให้บริการ (มาตรา 14 และมาตรา 15) สองมาตรานี้เป็นลักษณะที่เกิดจากการนำเข้าข้อมูลคอมพิวเตอร์ที่เป็นเท็จหรือ มีเนื้อหาไม่เหมาะสมในรูปแบบต่างๆ โดยมาตราที่ 14 กำหนดครอบคลุมถึงการปลอมแปลงข้อมูลคอมพิวเตอร์ หรือสร้างข้อมูลคอมพิวเตอร์อันเป็นเท็จที่ก่อให้เกิดความเสียหายแก่ผู้อื่น หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน หรือเป็นข้อมูลที่กระทบต่อสถาบันพระมหากษัตริย์ หรือก่อการร้าย รวมทั้งข้อมูลลามกอนาจาร และส่งต่อข้อมูลที่เป็นความผิดตามที่กล่าวไว้ข้างต้น เช่น การส่งภาพโป๊เปลือย ลามก หรือข้อความไม่เหมาะสมที่เกี่ยวกับสถาบันพระมหากษัตริย์ หรือข้อความที่เกี่ยวกับความมั่นคงของประเทศ หรือข้อความใส่ร้าย กล่าวหาผู้อื่น ทางจดหมายอิเล็กทรอนิกส์ การโพสต์ทางกระดานสนทนาและบล็อกต่างๆ

ในส่วนของมาตราที่ 15 มีการกำหนดโทษของผู้ให้บริการซึ่งหมายถึงบริษัทที่ยินยอมให้มีการกระทำความ ผิดตามที่กล่าวข้างต้นต้องรับโทษด้วยเช่นกันหากไม่ระงับการเผยแพร่ข้อมูลดัง กล่าว

10.การเผยแพร่ภาพจากการตัดต่อหรือดัดแปลงให้ผู้อื่นถูกดูหมิ่น หรืออับอาย (มาตรา 16) เป็นการกำหนดฐานความผิดในเรื่องของการตัดต่อภาพของบุคคลอื่นที่อาจทำให้ผู้ เสียหายเสียชื่อเสียง ถูกดูหมิ่น เกลียดชังหรือได้รับความอับอาย โทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ แต่ความผิดตามมาตรานี้เหมือนกับความผิดฐานหมิ่นประมาทคือยอมความกันได้

อาชญากรรมคอมพิวเตอร์ที่พนักงานสอบสวนควรรู้

กิจกรรมประจำวันต่างๆ ในยุคปัจจุบัน ล้วนมีความเกี่ยวข้องจากคอมพิวเตอร์ในรูปแบบต่างๆ เช่น การใช้บัตร ATM การสื่อสารทางโทรศัพท์ การควบคุมสัญญาณไฟจราจร การขายสินค้า การให้บริการ สาธารณะ เช่น รถประจำทางปรับอากาศ หรือกระทั่งสายการบิน งานการรักษาพยาบาล และการฝากเงินธนาคาร เป็นต้น นอกจากนั้น คอมพิวเตอร์ยังเก็บข้อมูลต่างๆ ที่ใช้ในวงการธุรกิจและแวดวงราชการ จากแนวความคิดที่ต้องการให้เครื่องคอมพิวเตอร์ 2 เครื่องสามารถติดต่อกัน และเปลี่ยนข้อมูลระหว่างกันได้ มาสู่ระบบเครือข่าย คอมพิวเตอร์ในปัจจุบันซึ่งใน 1 เครือข่ายนั้น อาจมีจำนวนเครื่องมากมายที่เป็นสมาชิก ความก้าวหน้าของเทคโนโลยีนำมาสู่ระบบเครือข่ายอินเทอร์เน็ต(Internet) ซึ่งก่อให้เกิดปัญหาอาชญากรรมคอมพิวเตอร์มากขึ้นเป็นเงาตามตัว

ความหมายของอาชญากรรมคอมพิวเตอร์

1 การกระทำใดๆ ก็ตาม ที่เกี่ยวกับการใช้ คอมพิวเตอร์อันทำให้เหยื่อได้รับความเสียหาย และผู้กระทำได้รับผลประโยชน์ตอบแทน

2 การกระทำผิดกฎหมายใดๆ ซึ่งใช้เทคโนโลยี คอมพิวเตอร์เป็นเครื่องมือ และในการสืบสวนสอบสวน ของเจ้าหน้าที่เพื่อนำตัวผู้กระทำผิดมาดำเนินคดี ก็ต้องใช้ความรู้ทางเทคโนโลยีคอมพิวเตอร์เช่นเดียวกัน

ลักษณะของอาชญากรคอมพิวเตอร์ (Categories of Computer Criminals)

1 พวกหัดใหม่(Novice) บุคคลประเภทนี้มิได้เป็นอาชญากรโดยแท้จริง เพียงแค่ใช้โอกาสในตำแหน่งหน้าที่ที่มีอยู่ เข้าไปดำเนินการกับข้อมูลคอมพิวเตอร์ เพื่อเข้าไปยังฐานข้อมูลนั้นๆ และมีเป็นจำนวนมาก ที่เป็นลูกจ้าง หรือพนักงานของหน่วยงานนั้นๆ เอง

2 พวกวิกลจริต(Deranged persons) ลักษณะของบุคคลประเภทนี้ มักกระทำอะไรโดยปราศจากเหตุผล ชอบทำลาย เป็นผู้ป่วยทางจิตและมีอันตรายโดยทั่วไป ไม่สามารถควบคุมตนเองได้ และจะทำลายระบบ ซอฟท์แวร์ หรือแฟ้มข้อมูลต่างๆ

3 เป็นกลุ่มที่ประกอบอาชญากรรมในลักษณะองค์กร(Organized crime) เป็นพวกที่ประกอบอาชญากรรมโดยหาผลประโยชน์จากคอมพิวเตอร์ มีการกระทำร่วมเป็นกลุ่มแก๊งค์ มีความรู้คอมพิวเตอร์เป็นอย่างดี สามารถใช้ในการหลบหลีกหรือยับยั้งการสืบสวนติดตามจับกุมของเจ้าหน้าที่ได้

4 พวกมืออาชีพ(Career) เป็นพวกกระทำผิด โดยสันดานถึงแม้ว่าจะถูกจับกุมแล้วเมื่อพ้นโทษออกมา ก็จะกระทำความผิดซ้ำอีก

5 พวกหัวพัฒนา(Con artists) เป็นพวกที่ชอบใช้ความก้าวหน้าทางคอมพิวเตอร์ ให้ได้มาซึ่งผลประโยชน์ทางการเงิน

6 พวกช่างคิดช่างฝัน(Ideologues) เป็นพวกที่กระทำผิดเนื่องจากมีความเชื่อถือในสิ่งหนึ่งสิ่งใดอย่างรุนแรง เป็นพวกก้าวร้าวชอบแสดงตัวเองว่ามีจุดเด่น หรือมีอำนาจเหนือบุคคลอื่น

7 พวก Hacker/Cracker เป็นพวกที่จงใจ และเจตนาเข้าถึงระบบของคอมพิวเตอร์ และแฟ้มข้อมูล โดยแยกความหมายของ Hacker/Cracker ได้ดังนี้

7.1 Hacker หมายถึง บุคคลผู้ที่เป็นอัจฉริยะ มีความรู้ในระบบคอมพิวเตอร์เป็นอย่างดี สามารถเข้าไปถึงข้อมูลในคอมพิวเตอร์โดยเจาะผ่านระบบ รักษาความปลอดภัยของคอมพิวเตอร์ได้ แค่อาจไม่แสวงหาผลประโยชน์

7.2 Cracker หมายถึง ผู้ที่มีความรู้และทักษะทางคอมพิวเตอร์เป็นอย่างดี จนสามารถเข้าสู่ระบบได้ เพื่อเข้าไปทำลายหรือลบแฟ้มข้อมูล หรือทำให้เครื่องคอมพิวเตอร์ เสียหาย รวมทั้งการทำลายระบบปฏิบัติการของเครื่องคอมพิวเตอร์

ความเสียหายอันเกิดจากอาชญากรรมคอมพิวเตอร์

ปัจจุบันอาชญากรรมคอมพิวเตอร์เป็นเรื่องสำคัญ เพราะเป็นอาชญากรรมเศรษฐกิจประเภทหนึ่ง ซึ่งไม่สามารถใช้อาวุธปราบปรามได้โดยตรง ผู้กระทำผิดด้านนี้ส่วนใหญ่เป็นผู้มีความรู้ มีตำแหน่งหน้าที่การงาน มีประสบการณ์และความชำนาญสูง และมีผลประโยชน์เข้ามาเกี่ยวข้องจำนวนมหาศาล แต่กฎหมายบ้านเราที่จะเข้าถึงเรื่องเหล่านี้ค่อนข้างยากแม้ว่าจะมีประมวลกฎหมายอาญาใช้มา 40 กว่าปีแล้วก็ตาม แต่ก็ยังไม่มีกฎหมายที่จะจัดการกับอาชญากรรมประเภทนี้โดยเฉพาะได้ อาชญากรรมคอมพิวเตอร์จึงได้สร้างความยุ่งยากในการหาและนำพยานหลักฐานมาสู่ศาล เนื่องจากตามกฎหมายไทยใช้ระบบองค์ประกอบความผิดในการตี่ความโดยขยายความค่อนข้างทำได้ยาก ถ้าสืบไม่พบ ฟังไม่ชัด ศาลก็จะยกฟ้องเสมอ จึงสามารถทำนายได้เลยว่า สภาพปัญหาและแนวโน้มอาชญากรรมคอมพิวเตอร์ในสังคมปัจจุบันจะยิ่งเพิ่มมากขึ้นในอนาคต

อาชญากรรมคอมพิวเตอร์ แบ่งเป็น 4 ลักษณะ คือ

ลักษณะแรก การเจาะระบบรักษาความปลอดภัย ทางกายภาพ ได้แก่ ตัวอาคาร อุปกรณ์และสื่อต่างๆ
ลักษณะที่สอง การเจาะเข้าไปในระบบสื่อสาร และการ รักษาความปลอดภัยของซอฟต์แวร์ข้อมูลต่างๆ
ลักษณะที่สาม เป็นการเจาะเข้าสู่ระบบรักษาความปลอดภัย ของระบบปฏิบัติการ(Operating System)
ลักษณะที่สี่ เป็นการเจาะผ่านระบบรักษาความปลอดภัยส่วนบุคคล เป็นช่องทางในการกระทำความผิด

แนวข้อสอบวิชา มาตรฐานการรักษาความปลอดภัยระบบคอมพิวเตอร์

1. **พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์มีผลบังคับ ใช้เมื่อใด**

   - วันที่ 18 กรกฎาคม พ.ศ. 2550

2. **การกระแบบใดจึงจะเรียกว่าเข้าข่ายความผิดตาม พ.ร.บ. ฉบับนี้**

   - การเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นโดยมิชอบ
   - การเปิดเผยข้อมูลมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ
   - การเข้าถึงข้อมูลคอมพิวเตอร์โดยไม่ชอบ
   - การดักรับข้อมูลคอมพิวเตอร์ของผู้อื่น
   - การทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง เพิ่มเติมข้อมูลคอมพิวเตอร์โดยไม่ชอบ
   - การกระทำเพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นไม่สามารถทำงานได้ตามปกติ
   - การส่งข้อมูลคอมพิวเตอร์รบกวนการใช้ระบบคอมพิวเตอร์ของคนอื่นโดยปกติสุข
   - การจำหน่ายชุดคำสั่งที่จัดทำขึ้นเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิด
   - การใช้ระบบคอมพิวเตอร์ทำความผิดอื่น ผู้ให้บริการจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิด
   - การตกแต่งข้อมูลคอมพิวเตอร์ที่เป็นภาพของบุคคล

3. **ผู้ให้บริการที่ระบุใน พ.ร.บ.คอมพิวเตอร์ คือบุคคลใดบ้าง**

   สำหรับผู้ให้บริการตามที่พ.ร.บ.นี้ได้ระบุไว้ สามารถจำแนกได้เป็น 4 ประเภทใหญ่ๆ ดังนี้

   1. ผู้ประกอบกิจการโทรคมนาคมไม่ว่าโดยระบบโทรศัพท์ ระบบดาวเทียม ระบบวงจรเช่าหรือบริการสื่อสารไร้สาย

   2. ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ไม่ว่าโดยอินเทอร์เน็ต ทั้งผ่านสายและไร้สาย หรือในระบบเครือข่ายคอมพิวเตอร์ภายในที่เรียกว่าอินเทอร์เน็ต ที่จัดตั้งขึ้นในเฉพาะองค์กรหรือหน่วยงาน

   3. ผู้ให้บริการเช่าระบบคอมพิวเตอร์ หรือให้เช่าบริการโปรแกรมประยุกต์ (Host Service Provider)

   4. ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่าน application ต่างๆ ที่เรียกว่า content provider เช่นผู้ให้บริการ web board หรือ web service เป็นต้น

4. **ลิขสิทธิ์ หมายถึง**

   ลิขสิทธิ์ เป็นทรัพย์สินทางปัญญาอย่างหนึ่ง ที่กฎหมายให้ความคุ้มครองโดยให้เจ้าของลิขสิทธิ์ถือสิทธิแต่เพียงผู้เดียวที่จะกระทำการใดๆ เกี่ยวกับงานสร้างสรรค์ที่ตนได้กระทำขึ้น

5. การกระทำที่ถือว่าถูกกฎหมายทางด้านลิขสิทธิ์ซอฟต์แวร์ทำได้อย่างไร

- ติดตั้งและใช้งานลิขสิทธิ์ซอฟต์แวร์ 1 ชุดในคอมพิวเตอร์เพียง 1 เครื่องเท่านั้น
- อย่าทำสำเนาโปรแกรมเพื่อการสำรองมากกว่า 1 สำเนา
- อย่าให้ผู้ใดขอยืมซอฟต์แวร์ของท่านไป

6. นักศึกษาทราบได้อย่างไรว่าซอฟแวร์ที่ใช้มีลิขสิทธิ์ถูกต้องหรือไม่

เมื่อท่านซื้อซอฟต์แวร์มาใช้งาน ท่านควรได้รับใบอนุญาตการใช้งานซึ่งระบุสิทธิที่เจ้าของลิขสิทธิ์อนุญาตให้ท่านใช้งานซอฟต์แวร์เหล่านี้ได้ รวมทั้งระบุขอบข่ายของการใช้งานอีกด้วย เช่น ซอฟต์แวร์บางประเภทอาจอนุญาตให้ท่านใช้งานสำเนาที่สองสำหรับการทำงานที่บ้านได้ท่านควรอ่านเอกสาร เหล่านี้ให้ละเอียดเพื่อประโยชน์ของท่านเอง และเก็บเอกสารเหล่านี้ไว้เป็นหลักฐานในการมีลิขสิทธิ์ที่ถูกต้องเสมอ

ข้อสังเกตของซอฟต์แวร์ละเมิดลิขสิทธิ์

- ซอฟต์แวร์ราคาถูกจนไม่น่าเชื่อ
- โปรแกรมนั้นอยู่ในแผ่น CD-ROM ที่บรรจุซอฟต์แวร์หลายชนิดซึ่งมักเป็นผลงานจากผู้ผลิตซอฟต์แวร์หลายบริษัท
- ซอฟต์แวร์จำหน่ายโดยบรรจุในกล่องพลาสติกใสโดยไม่มีกล่องบรรจุภัณฑ์
- ไม่มีเอกสารอนุญาตการใช้งาน หรือคู่มือการใช้งาน

7. **สิทธิบัตร (patent) หมายถึง**

หมายถึง หนังสือสำคัญที่รัฐออกให้เพื่อคุ้มครองการประดิษฐ์คิดค้นหรือการออกแบบผลิตภัณฑ์ ที่มีลักษณะตามที่กำหนดในกฎหมา ที่เกี่ยวกับการประดิษฐ์คิดค้นหรือการออกแบบเพื่อให้ได้สิ่งของ,เครื่องใช้หรือสิ่งอำนวยความสะดวกต่างๆที่เราใช้กันอยู่ในชีวิตประจำวัน เช่น การประดิษฐ์รถยนต์, โทรทัศน์, คอมพิวเตอร์

8. ประเภทของสิทธิบัตร

รูปแบบหรือประเภทของสิทธิบัตรตาม พ.ร.บ. สิทธิบัตรจะมีอยู่ 3 ประเภท คือ

1. **สิทธิบัตรการประดิษฐ์** หมายถึง การคิดค้นเกี่ยวกับ กลไก โครงสร้าง ส่วนประกอบ ของสิ่งของเครื่องใช้ เช่น กลไกของกล้องถ่ายรูป
2. **สิทธิบัตรการออกแบบผลิตภัณฑ์** หมายถึง การออกแบบรูปร่าง ลวดลาย หรือสีสัน ที่มองเห็นได้จากภายนอก เช่น การออกแบบแก้วน้ำให้มีรูปร่างเหมือนรองเท้า เป็นต้น
3. **อนุสิทธิบัตร** (Petty patent) เป็นการให้ความคุ้มครองสิ่งประดิษฐ์คิดค้น เช่นเดียวกับสิทธิบัตรการประดิษฐ์ แต่แตกต่างกันตรงที่การประดิษฐ์ที่จะขอรับอนุสิทธิบัตร เป็นการประดิษฐ์ที่มีเป็นการปรับปรุงเพียงเล็กน้อย และมีประโยชน์ใช้สอยมากขึ้นมากก

9. พาณิชย์อิเล็กทรอนิกส์ (Electronic commerce) หมายถึง

Electronic Commerce หรือ การพาณิชย์อิเล็กทรอนิกส์ หมายถึง การทำธุรกรรมทางเศรษฐกิจที่ผ่านสื่ออิเล็กทรอนิกส์ เช่น การซื้อขายสินค้าและบริหาร การโฆษณาสินค้า การโอนเงินทางอิเล็กทรอนิกส์ เป็นต้น จุดเด่นของ E-Commerce คือ ประหยัดค่าใช้จ่าย และเพิ่มประสิทธิภาพในการดำเนินธุรกิจ โดยลดความสำคัญขององค์ประกอบของธุรกิจที่มองเห็นจับต้องได้ เช่นอาคารที่ทำการ ห้องจัดแสดงสินค้า (show room) คลังสินค้า พนักงานขายและพนักงานให้บริการต้อนรับลูกค้า เป็นต้น ดังนั้นข้อจำกัดทางภูมิศาสตร์คือ ระยะทางและเวลาทำการแตกต่างกัน จึงไม่เป็นอุปสรรคต่อการทำธุรกิจอีกต่อไป

10. ข้อดีของการกระทำพาณิชย์อิเล็กทรอนิกส์มีดังนี้

1.เปิดดำเนินการค้า 24 ชั่วโมง

2.ดำเนินการค้าอย่างไร้พรมแดนทั่วโลก

3.ใช้งบประมาณลงทุนน้อย

4.ตัดปัญหาด้านการเดินทาง

5.ง่ายต่อการประชาสัมพันธ์โดย สามารถประชาสัมพันธ์ได้ทั่วโลก

11. อาชญากรทางคอมพิวเตอร์ ได้แก่

1. พวกเด็กหัดใหม่ (Novice)
2. พวกวิกลจริต (Deranged persons)
3. อาชญากรที่รวมกลุ่มกระทำผิด (Organized crime)
4. อาชญากรอาชีพ (Career)
5. พวกหัวพัฒนา มีความก้าวหน้า (Con artists)
6. พวกคลั่งลัทธิ(Dreamer) / พวกช่างคิดช่างฝัน(Ideologues)
7. ผู้ที่มีความรู้และทักษะด้านคอมพิวเตอร์อย่างดี (Hacker/Cracker)

12. ปัจจุบันทั่วโลก ได้จำแนกประเภทของอาชญากรรมทางคอมพิวเตอร์ได้ 9 ประเภท (ตามข้อมูลคณะอนุกรรมการเฉพาะกิจร่างกฎหมายอาชญากรรมทางคอมพิวเตอร์) คือ

1. การขโมยข้อมูลทางอินเตอร์เน็ต รวมถึงการขโมยประโยชน์ในการลักลอบใช้บริการ
2. การปกปิดความผิดของตัวเอง โดยใช้ระบบการสื่อสาร
3. การละเมิดลิขสิทธิ์ ปลอมแปลงรูปแบบเลียนแบระบบซอฟแวร์โดยมิชอบ
4. การเผยแพร่ภาพ เสียง ลามก อนาจาร และข้อมูลที่ไม่เหมาะสม
5. การฟอกเงิน
6. การก่อกวน ระบบคอมพิวเตอร์ เช่น ทำลายระบบสาธารณูปโภค เช่น ระบบจ่ายน้ำ จ่ายไฟจราจร

7. การหลอกลวงให้ร่วมค้าขาย หรือ ลงทุนปลอม (การทำธุรกิจที่ไม่ชอบด้วยกฎหมาย)

8. การลักลอบใช้ข้อมูลเพื่อแสวงหาผลประโยชน์ในทางมิชอบเช่น การขโมยรหัสบัตรเครดิต

9. การใช้คอมพิวเตอร์ในการโอนบัญชีผู้อื่นเป็นของตัวเอง

13. อาชญากรรมคอมพิวเตอร์ แบ่งเป็น 4 ลักษณะ คือ

1. การเจาะระบบรักษาความปลอดภัย ทางกายภาพ ได้แก่ ตัวอาคาร อุปกรณ์และสื่อต่างๆ

2. การเจาะเข้าไปในระบบสื่อสาร และการ รักษาความปลอดภัยของซอฟต์แวร์ข้อมูลต่างๆ

3. เป็นการเจาะเข้าสู่ระบบรักษาความปลอดภัย ของระบบปฏิบัติการ (Operating System)

4. เป็นการเจาะผ่านระบบรักษาความปลอดภัยส่วนบุคคล โดยใช้อินเตอร์เน็ตเป็นช่องทางในการกระทำความผิด

14. ระบบสนับสนุนการตัดสินใจคือ

เป็นซอฟต์แวร์ที่ช่วยในการตัดสินใจเกี่ยวกับการจัดการ การรวบรวมข้อมูล การวิเคราะห์ข้อมูล และการสร้างตัวแบบที่ซับซ้อน ภายใต้ซอฟต์แวร์เดียวกัน นอกจากนั้น DSS ยังเป็นการประสานการทำงานระหว่างบุคลากรกับเทคโนโลยีทางด้านซอฟต์แวร์ โดยเป็นการกระทำโต้ตอบกัน เพื่อแก้ปัญหาแบบไม่มีโครงสร้าง และอยู่ภายใต้การควบคุมของผู้ใช้ตั้งแต่เริ่มต้นถึงสิ้นสุด

15. คุณสมบัติของ DSS มีดังนี้

1. ง่ายต่อการเรียนรู้และใช้งาน เนื่องจากผู้ใช้อาจมีทักษะทางสารสนเทศที่จำกัด ตลอดจนความเร่งด่วนในการใช้งานและความต้องการของปัญหา ทำให้ DSS ต้องมีความสะดวกต่อผู้ใช้

2. สามารถโต้ตอบกับผู้ใช้ได้อย่างรวดเร็ว และมีประสิทธิภาพ โดยที่ DSS ที่ดีต้องสามารถสื่อสารกับผู้ใช้อย่างฉับพลัน โดยตอบสนองความต้องการและโต้ตอบกับผู้ใช้ได้ทันเวลา โดยเฉพาะในสถานการณ์ปัจจุบัน ที่ต้องการความรวดเร็วในการแก้ปัญหา

3. มีข้อมูล และแบบจำลองสำหรับสนับสนุนการตัดสินใจที่เหมาะสมและสอดคล้องกับลักษณะของปัญหา

4. สนับสนุนการตัดสินใจแบบกึ่งโครงสร้าง และไม่มีโครงสร้าง ซึ่งแตกต่างจากระบบสารสนเทศสำหรับปฏิบัติ งานที่จัดการข้อมูลสำหรับงานประจำวันเท่านั้น

5. มีความยืดหยุ่นที่จะสนองความต้องการที่เปลี่ยนแปลงไปของผู้ใช้ เนื่องจากลักษณะของปัญหาที่มีความไม่แน่นอน และเปลี่ยนแปลงตามสถานการณ์ นอกจากนี้ผู้จัดการจะเผชิญหน้ากับปัญหา ที่มีความไม่แน่นอนและเปลี่ยนแปลงทางสถานการณ์ นอกจากนี้ผู้จัดการจะเผชิญกับปัญหาในหลายลักษณะจึงต้องการระบบสารสนเทศที่ช่วยจัดรูปข้อมูลที่ไม่ซับซ้อนและง่ายต่อการตัดสินใจ

16. ระบบสารสนเทศสำหรับผู้บริหาร (Executive Information Systems) หรือที่เรียกว่า EIS หมายถึง

ระบบสารสนเทศที่ถูกพัฒนาขึ้นโดยเฉพาะ เพื่อให้สอดคล้องกับความต้องการ ทักษะ และความสามารถในการเข้าถึงสารสนเทศสำหรับ ผู้บริหาร

17. ระบบปัญญาประดิษฐ์ (Artificial intelligence: AI) หมายถึง

เครื่องจักรอัจฉริยะที่สร้างจากความรู้ทางด้าน วิทยาศาสตร์ และวิศวกรรมศาสตร์ โดยเฉพาะอย่างยิ่ง ความฉลาดทางด้านโปรแกรม คอมพิวเตอร์ซึ่งเป็นในลักษณะการใช้คอมพิวเตอร์ ให้เรียนรู้และเข้าใจความสามารถของมนุษย์

18. ประโยชน์ของระบบปัญญาประดิษฐ์ คือ

1. ข้อมูลถูกเก็บไว้ในหน่วยความจำขององค์กรกลายเป็นฐานความรู้องค์กรที่พนักงานสามารถสืบค้นแลหาคำปรึกษาได้ทุกเวลา

2. ช่วยสร้างกลไกที่ไม่มีความรู้สึก ความหนื่อยล้า หรือความกังกลมาเป็นองค์ประกอบ

3. ช่วยนำมาใช้ในงานประจำหรืองานที่น่าเบื่อหน่าย

4. เพิ่มความสามารถในฐานความรู้ขององค์กรด้วยวิธีเสนอปัญหา ที่มีปริมาณมากหรือความซับซ้อนมาก

19. **ระบบผู้เชี่ยวชาญ (Expert System: ES) หมายถึง**

ระบบคอมพิวเตอร์ ที่จำลองการตัดสินใจของมนุษย์ ผู้เป็นผู้เชี่ยวชาญในด้านใดด้านหนึ่ง โดยใช้ความรู้และการสรุปเหตุผลเชิงอนุมาน (inference) ในการแก้ปัญหายากๆ ที่ต้องอาศัยผู้เชี่ยวชาญ

20. ตัวอย่างของระบบ ES ที่นำไปใช้ในงานด้านต่าง ๆ ได้แก่

diagnosis of faults and diseases, automobile diagnosis, interpretation of data (เช่น sonar signals), mineral exploration, personnel scheduling, computer network management, weather forecasting, stock market prediction, consumer buying advice, diet advice

21. ระบบการประมวลผลรายการ (TPS) มีลักษณะการทำงานอย่างไร

คุณลักษณะของระบบการประมวลผลข้อมูล

1. สามารถจัดเก็บข้อมูลที่เกิดขึ้นประจำวันของการดำเนินธุรกิจได้ เช่น ประวัติลูกค้า รายการสั่งซื้อสินค้าจากลูกค้า

2. สามารถสร้างข้อมูลเพื่อดำเนินธุรกิจได้ เช่น ออกใบกำกับภาษี ออกใบแจ้งหนี้ ออกใบรายการสินค้า

3. บำรุงรักษาข้อมูล (Data Maintenance) โดยการปรับปรุงข้อมูล (เพิ่ม ลบ แก้ไข) ให้เป็นปัจจุบันมากที่สุดไม่ว่าจะเป็นการเปลี่ยนแปลงของราคาสินค้า ชื่อที่อยู่ของลูกค้า รหัสสินค้า เป็นต้น

22. ยกตัวอย่างงานที่นำระบบ TPS ไปใช้ มา 4 ข้อ

1. การลงเวลาตอกบัตร
2. รับชำระค่าสินค้า
3. บันทึกยอดขายประจำวัน
4. ออกใบเสร็จ

23. จงบอกประโยชน์ของระบบ EIS มา 3 ข้อ

1. ด้านคุณภาพของข่าวสาร
2. มีระบบการโต้ตอบกับผู้ใช้
3. จัดเตรียมเทคนิคที่มีประสิทธิภาพสำหรับจัดการกับข่าวสาร
4. เอื้อประโยชน์ต่อการทำงานขององค์กรในด้านต่าง ๆ

24. จงบอกประเภทของระบบ AI

1.การประมวลภาษาธรรมชาติ (Natural Language Processing)

2.ระบบภาพ (Vision System)

3.ระบบเครือข่ายเส้นประสาท (Natural Networks)

4.หุ่นยนต์ (Robotics)

5.ระบบผู้เชี่ยวชาญ (Expert System)

25. ระบบ OIS สามารถจัดแบ่งได้กี่ประเภท

แบ่งได้ 4 ประเภท คือ

ระบบการจัดการเอกสาร (Document management system)

ระบบการจัดการข่าวสาร (Message-handling systems)

ระบบประชุมทางไกล (Teleconferencing system)

ระบบสนับสนุนสำนักงาน (Office support systems)

26. จงบอกข้อแตกต่างระหว่าง M-Commerce กับ E-Commerce

1.ทั้ง E-Commerce และ M-Commerce ต่างก็เป็นส่วนหนึ่งของการค้าพาณิชย์อิเล็กทรอนิกส์

2. E-Commerce เป็นการค้าพาณิชย์อิเล็กทรอนิกส์ที่ทำการค้าบนเว็บไซต์ของเครื่องคอมพิวเตอร์

3. M-Commerce เป็นการค้าพาณิชย์อิเล็กทรอนิกส์ที่ทำการค้าบนโทรศัพท์มือถือ

4.การค้าแบบ M-Commerce สามารถทำการสั่งซื้อสินค้าได้สะดวกสบายกว่า E-Commerce

ภัยคุกคามและการรักษาความปลอดภัยบนระบบคอมพิวเตอร์

(Threats and Security on computer system)

หัวข้อ (Topic)

7.1 ประเภทของภัยคุกคาม

7.2 การรักษาความปลอดภัยบนระบบคอมพิวเตอร์

วัตถุประสงค์การเรียนรู้ (Learning Objective)

1. จำแนกประเภทของภัยคุกคามได้
2. เสนอแนะวิธีในการป้องกันภัยบนระบบคอมพิวเตอร์ได้
3. อธิบายมาตรการในการรักษาความปลอดภัยของข้อมูลได้
4. บอกความแตกต่างระหว่าง Hacker กับ Cracker ได้
5. บอกความแตกต่างระหว่าง Virus กับ Worm ได้
6. บอกความหมายของ Spam และข้อเสียของ Spam ได้
7. อธิบายภัยคุกคามบน E-Commerce และภัยคุกคามรูปแบบอื่น ๆ บน Internet ได้
8. บอกประโยชน์และโทษของ Cookie ได้
9. แนะนำวิธีการสังเกตุความปลอดภัยในการเลือกซื้อสินค้าบน Web Site ได้

7.1 ประเภทของภัยคุกคาม

ภัยภิบัติที่เกิดขึ้นกับระบบ (Disaster) เป็นความเสียหายทั้งทางด้านกายภาพและด้านข้อมูล ที่เกิดขึ้นกับระบบคอมพิวเตอร์ Hardware Programs แฟ้มข้อมูล และอุปกรณ์อื่น ๆ ถูกทำลายให้ให้เกิดความเสียหาย ซึ่งที่ร้ายแรงที่สุดอาจก็คือการที่ภัยนั้นทำให้ระบบล่มไม่สามารถใช้งานได้

ประเภทของภัยคุกคามที่เกิดขึ้นกับระบบคอมพิวเตอร์และเครือข่ายนั้น สามารถจำแนกได้ 2 ประเภท
หลัก ๆ ดังนี้

1. ภัยคุกคามทางตรรกะ (Logical) หมายถึง ภัยคุกคามทางด้านข้อมูล

2. ภัยคุกคามทางกายภาพ (Physical) หมายถึง ภัยที่เกิดกับตัวเครื่องและอุปกรณ์ เช่น ภัยภิบัติจากธรรมชาติ และภัยจากการกระทำของมนุษย์ที่ทำความเสียหายให้กับตัวเครื่องและอุปกรณ์

ภัยคุกคามทางด้านข้อมูล

Hacker คือ ผู้ที่แอบเข้าใช้งานระบบคอมพิวเตอร์ของหน่วยงานหรือองค์กรอื่น โดยมิได้รับอนุญาต แต่ไม่มีประสงค์ร้าย หรือไม่มีเจตนาที่จะสร้างความเสียหายหรือสร้างความเดือดร้อนให้แก่ใครทั้งสิ้น แต่เหตุผลที่ทำเช่นนั้นอาจเป็นเพราะต้องการทดสอบความรู้ความสามารถของตนเองก็เป็นไปได้

Cracker คือ ผู้ที่แอบเข้าใช้งานระบบคอมพิวเตอร์ของหน่วยงานหรือองค์กรอื่น โดยมีเจตนาร้ายอาจจะเข้าไปทำลายระบบ หรือสร้างความเสียหายให้กับระบบ Network ขององค์กรอื่น หรือขโมยข้อมูลที่เป็นความลับทางธุรกิจ

Note : ไม่ว่าจะเป็น Hacker หรือ Cracker ถ้ามีการแอบเข้าใช้งานระบบคอมพิวเตอร์เครือข่ายของผู้อื่น แม้ว่าจะไม่ประสงค์ร้ายก็ถือว่าไม่ดีทั้งสิ้น เพราะขาดจริยธรรมด้านคอมพิวเตอร์

ไวรัส (Viruses) คือ โปรแกรมคอมพิวเตอร์ประเภทหนึ่งที่เขียนขึ้นโดยความตั้งใจของ Programmer ถูกออกแบบมาให้แพร่กระจายตัวเองจากไฟล์หนึ่งไปยังไฟล์อื่นๆ ภายในเครื่องคอมพิวเตอร์ ไวรัสจะแพร่กระจายตัวเองอย่างรวดเร็วไปยังทุกไฟล์ภายในคอมพิวเตอร์ หรืออาจจะทำให้ไฟล์เอกสารติดเชื้ออย่างช้าๆ แต่ไวรัสจะไม่สามารถแพร่กระจายจากเครื่องหนึ่งไปยังอีกเครื่องหนึ่งได้ด้วยตัวมันเอง โดยทั่วไปแล้วจะเกิดจากการที่ผู้ใช้ใช้สื่อจัดเก็บข้อมูล เช่น Diskette คัดลอกไฟล์ข้อมูลลง Disk และติดไวรัสเมื่อนำไปใช้กับเครื่องอื่น หรือไวรัสอาจแนบมากับไฟล์เมื่อมีการส่ง E-mail ระหว่างกัน

หนอนอินเตอร์เน็ต (Worms) มีอันตรายต่อระบบมาก สามารถทำความเสียหายต่อระบบได้จากภายใน เหมือนกับหนอนที่กัดกินผลไม้จากภายใน หนอนร้ายเป็นโปรแกรมคอมพิวเตอร์ที่ถูกออกแบบมาให้สามารถแพร่กระจายตัวเองจากเครื่องคอมพิวเตอร์เครื่องหนึ่งไปยังอีกเครื่องหนึ่งโดยอาศัยระบบเน็ตเวิร์ค (ผ่านสาย Cable) ซึ่งการแพร่กระจายสามารถทำได้ด้วยตัวของมันเองอย่างรวดเร็วและรุนแรงกว่าไวรัส เมื่อไรก็ตามที่คุณสั่ง Share ไฟล์ข้อมูลผ่าน Network เมื่อนั้น Worms สามารถเดินไปกับสายสื่อสารได้

Spam mail คือ การส่งข้อความที่ไม่เป็นที่ต้องการให้กับคนจำนวนมาก ๆ จากแหล่งที่ผู้รับไม่เคยรู้จักหรือติดต่อมาก่อน โดยมากมักอยู่ในรูปของ E-mail ทำให้ผู้รับรำคาญใจและเสียเวลาในการลบข้อความเหล่านั้นแล้ว Spam mail ยังทำให้ประสิทธิภาพการขนส่งข้อมูลบนอินเทอร์เน็ตลดลงด้วย

ภัยคุกคามในการทำธุรกิจ E- Commerce

ในการทำธุรกิจบนระบบพาณิชย์อิเล็กทรอนิกส์ อาจจะเกิดภัยคุกคามต่อเว็บไซต์ได้ จึงเป็นสิ่งสำคัญที่เราทุกคนควรจะรู้ว่ามีภัยคุกคามใดบ้างที่อาจเกิดขึ้นกับระบบ เพื่อเตรียมพร้อมสำหรับการป้องกันล่วงหน้า ตัวอย่างภัยคุกคามที่ควรระวังสำหรับพาณิชย์อิเล็กทรอนิกส์ เช่น

1. การเข้าสู่เครือข่ายโดยไม่ได้รับอนุญาต เช่น มีบุคคลอื่นแอบอ้างในการใช้ชื่อ Login Name และ Password ในการเข้าไปทำธุรกรรมซื้อขายบน Web site แทนตัวเราเอง

2. การทำลายข้อมูลและเครือข่าย เช่น Cracker เจาะระบบเข้าไปทำลาย file และข้อมูลภายในเครื่อง Server ของ Web site ผู้ขาย ทำให้ข้อมูลสมาชิกหรือลูกค้าของระบบเกิดความเสียหาย

3. การเปลี่ยนแปลง การเพิ่ม หรือการดัดแปลงข้อมูล เช่น การส่ง Order หรือจดหมายอิเล็กทรอนิกส์ในการสั่งซื้อสินค้า หรือการที่จดหมายถูกเปิดอ่านระหว่างทาง ทำให้ข้อมูลไม่เป็นความลับ และผู้เปิดอ่านอาจเปลี่ยนแปลง แก้ไข หรือเพิ่มเติมข้อความในจดหมาย เช่น การแก้ไขจำนวนยอดของการสั่งซื้อสินค้า เป็นต้น

4. การเปิดเผยข้อมูลแก่ผู้ที่ไม่ได้รับอนุญาต เมื่อเราสมัครเป็นสมาชิกไว้ใน Web site ใด ๆ Server ของเจ้าของ Web site จะเก็บข้อมูลส่วนตัวของเราไว้ หากเจ้าของ Web Site ขาดจริยธรรมในการทำธุรกิจอาจนำข้อมูลส่วนตัวของเราไปขายให้องค์กรอื่น เช่น ขายข้อมูลให้กับบริษัทบัตร Credit เป็นต้น

5. การทำให้ระบบบริการของเครือข่ายหยุดชะงัก เช่น การที่ Cracker เข้ามาทำลายระบบเครือข่าย และส่งผลให้เครื่อง Server ของเจ้าของ Web site ไม่สามารถให้บริการแก่ลูกค้าของเขาได้ จนกว่าระบบนั้นจะถูกแก้ไข ดังนั้น เมื่อระบบล่มเป็นระยะเวลานานหลายชั่วโมง หรืออาจจะนานหลายวันก็จะส่งผลต่อยอดขายสินค้าบน Web ด้วย

6. การขโมยข้อมูล เมื่อตัวเราเองเป็นผู้ให้ข้อมูลไว้กับ Web site ที่เราจะซื้อขายสินค้า ข้อมูลนั้นอาจถูกขโมยจากเจ้าของ Web site จากผู้ดูแล Web หรือจาก Cracker ที่นำไปใช้ประโยชน์ต่อเขาเหล่านั้น แต่ส่งผลเสียกับตัวเรา เพราะการเปิดเผยข้อมูลส่วนตัวเขาของเราโดยไม่ได้รับอนุญาตถือเป็นการขโมย

7. การปฏิเสธการบริการที่ได้รับ เช่น ปฏิเสธว่าไม่ได้เข้าไปกรอกรายการสั่งซื้อที่ Web site โดยใช้ชื่อนี้หรืออ้างว่าสั่งซื้อสินค้าแล้วแต่ไม่ได้รับการจัดส่งสินค้าจาก web site ดังกล่าวเพื่อใช้เป็นข้ออ้างในการชำระเงินค่าสินค้าส่วนที่เหลือ

8. การอ้างว่าได้ให้บริการ หรือ อ้างว่าได้ส่งมอบสินค้าและบริการแล้ว

9. Virus ที่แอบแฝงมากับผู้ที่เข้ามาใช้บริการ ส่งผลทำให้เครื่อง Server ของเจ้าของ web site ได้รับความเสียหาจากการที่ Virus ทำลายข้อมูลและ file ต่าง ๆ ภายในระบบ

ภัยคุกคามบน Internet

อันตรายหนึ่งที่คาดไม่ถึงจากอินเทอร์เน็ตที่ส่งผลกระทบโดยตรงต่อเยาวชนไทย เพราะอินเทอร์เน็ตยังเป็นสื่อ Electronic ที่มาตรการการควบคุมสิทธิเสรีภาพของผู้ใช้ยังไม่ดีนัก ดังนั้น การกระทำใด ๆ ในห้องสนทนา (Chat) และ เว็บบอร์ด (Web board) จึงเกิดขึ้นได้อย่างไร้ขอบเขต จนกลายเป็นที่ระบายออกซึ่งอารมณ์และความรู้สึกของผู้ใช้

ในห้องสนทนา ทุกคนสามารถคุยอะไรกับใครก็ได้ รายละเอียดต่างๆไม่มีการเปิดเผย รู้เพียงแต่ชื่อที่ใช้ในการสนทนาเท่านั้น ดังนั้นจึงไม่มีทางรู้ได้เลยว่า เรากำลังพูดคุยอยู่กับใคร สิ่งที่คนนั้นพูดอยู่เป็นความจริงหรือไม่ ดังจะเห็นตามหน้าหนังสือพิมพ์ที่อาชญากรรมที่เกิดกับวัยรุ่นสมัยนี้บางครั้งมีจุดเริ่มต้นมาจากการพูดคุยกันในห้องสนทนา (Chat Room) บนอินเทอร์เน็ต

Case1: หญิงสาวผู้นี้ได้แอบอ้างว่า เธอคือ นาเดีย นิมิตรวานิช

ชายหนุ่มและหญิงสาว สนทนากันบนโลก Cyber โดยหญิงสาวผู้นี้ได้แอบอ้างว่า เธอคือ นาเดีย นิมิตรวานิช ดาราสาวและดีเจชื่อดังของรายการ Channel V Thailand ซึ่งทำให้ชายหนุ่มผู้นั้นเชื่อว่าเป็นเรื่องจริง ทั้งๆที่ยังไม่เคยเห็นหน้ามาก่อน จากนั้นจึงติดต่อกันเรื่อยมาทางโทรศัพท์ จนในที่สุดเวลาผ่านไป ฝ่ายชายที่คาดว่าน่าจะหลงไหลในหญิงสาวผู้แอบอ้างเป็นอย่างมากจึงขอฝ่ายหญิงแต่งงานโดยที่ยังไม่เคยเห็นหน้าแม้แต่ครั้งเดียว โดยตกลงกันว่าฝ่ายชายจะนำเงินค่าสินสอดไปฝากไว้กับเคาน์เตอร์ของโรงแรมชื่อดังแห่งหนึ่ง แล้วให้รอการติดต่อกลับ หลังจากนั้นแล้ว ฝ่ายหญิงก็เงียบหายเข้ากลีบเมฆไป ฝ่ายชายจึงรู้ว่าตนถูกหลอกแน่จึงเข้าแจ้งความ ในที่สุดตำรวจก็สามารถจับตัวสาวนักต้มตุ๋นผู้นี้ได้ ซึ่งพบว่าเธอมีเสียงที่เหมือนกับนาเดียตัวจริงมาก จึงทำให้ชายหนุ่มหลงเชื่อสนิทใจ

Case2: วิศวกรนายหนึ่ง เข้าไปโพสท์ในเว็บบอร์ดของ Pantip.com ว่า ตนได้ข่มขืนหญิงรับใช้ภายในบ้าน

สำหรับเว็บบอร์ดก็สามารถสร้างความปั่นป่วนให้แก่สังคมได้ ดังตัวอย่างที่เคยมีวิศวกรนายหนึ่ง เข้าไปโพสท์ในเว็บบอร์ดของ Pantip.com ว่า ตนได้ข่มขืนหญิงรับใช้ภายในบ้าน ทำให้เธอมีเลือดออกมาก แต่เขาไม่กล้าพาไปหาหมอ เพราะกลัวจะเป็นเรื่องราวใหญ่โต จึงอยากรู้ว่ามีวิธีช่วยเหลืออะไรบ้าง ปรากฏว่ามีผู้หวังดีอ่านพบจึงอีเมล์ไปบอก Webmaster ของ Pantip.com Webmaster จึงนำเรื่องไปแจ้งตำรวจ หลังจากตำรวจเช็ควันเวลาที่โพสท์และ IP Address กับทางเว็บไซต์แล้ว จึงติดต่อไปยัง ISP ที่วิศวกรผู้นั้นใช้บริการอยู่ ซึ่ง ISP ก็สามารถบอกเบอร์โทรศัพท์ของวิศวกรที่ใช้ต่ออินเทอร์เน็ตเข้ามาได้ โชคดีที่วิศวกรรายนี้ไม่ได้ใช้อินเทอร์เน็ตตามอินเทอร์เน็ตคาเฟ่แต่ใช้จากคอนโดมิเนี่ยมของเขาเอง ตำรวจจึงสามารถหาที่อยู่ได้ไม่ยาก แต่เมื่อไปถึงแล้วปรากฏว่าไม่มีอะไรเกิดขึ้นเลย เหตุการณ์ทั้งหมดเป็นเพียงเรื่องแต่งขึ้นเพื่อความสนุกเท่านั้น

คุกกี้ (Cookie)

คือการที่ Web Server จดจำข้อมูลของผู้ใช้ที่เคยกรอกไว้เมื่อเข้าไปทำธุรกรรมซื้อขายบน web site โดยเก็บรายละเอียดของข้อมูลลงในไฟล์ “คุกกี้” ซึ่งผู้ใช้เป็นผู้ให้ข้อมูลด้วยตนเอง การจดจำข้อมูลลงใน file cookie มีทั้งข้อดีและข้อเสีย ซึ่งข้อดีก็คือ ทำให้สะดวกเมื่อเราต้องการจะกรอกข้อมูลชุดเดิมซ้ำอีกครั้ง web browser จะจดจำข้อมูลเดิมที่เราเคยกรอกไว้และเรียกข้อมูลนั้นขึ้นมาให้ทำให้เราทำงานได้สะดวกและรวดเร็วขึ้น แต่ในทางกลับกันข้อมูลของเราก็ไม่เป็นความลับ หากเป็นข้อมูลที่สำคัญและมีผู้แบบนำไปใช้ในทางที่ผิดก็กระทบกับตัวเราได้

Errors

คือข้อผิดพลาดของโปรแกรม เป็นสาเหตุหลักที่ทำให้คอมพิวเตอร์เกิดความยุ่งเหยิงและทำลายข้อมูลที่ถูกเก็บไว้ ตลอดจนส่งผลต่อการทำงานของโปรแกรม

Bugs

คือชุดคำสั่ง (code) ของโปรแกรมที่มีข้อบกพร่องหรือมีข้อผิดพลาด ซึ่ง Bugs กับ Errors มีความแตกต่างกันกล่าวคือ Errors ของโปรแกรมอาจเกิดขึ้นค่อนข้างบ่อยครั้ง และสามารถแก้ไขข้อผิดพลาดนั้นได้เรื่อย ๆ แต่ Bugs ของโปรแกรมนั้นเมื่อพัฒนาโปรแกรมเสร็จ นำโปรแกรมนั้นไปใช้สักระยะ Bugs นั้นอาจโผล่ขึ้นมาภายหลัง เป็นข้อผิดพลาดที่ค่อนข้างรุนแรง อาจต้องแก้ไข (Modify) โปรแกรมใหม่

ภัยคุกคามทางกายภาพ (Physical)

ภัยจากธรรมชาติ มีหลายรูปแบบ เช่น

1. น้ำท่วม
2. แผ่นดินไหว
3. คลื่นซึนามิ
4. พายุ โคลนถล่ม
5. ฟ้าผ่า
6. ภัยธรรมชาติรูปแบบอื่น ๆ

ภัยจากการกระทำของมนุษย์ มีหลายรูปแบบ เช่น

1. การขโมยเครื่องและอุปกรณ์
2. การทำลายอุปกรณ์ Hardware
3. ไฟฟ้าดับ
4. ไฟไหม้

7.2. การรักษาความปลอดภัยบนระบบคอมพิวเตอร์

จำแนกการรักษาความปลอดภัยออกเป็น 2 ด้าน ได้แก่

1. ความปลอดภัยของข้อมูล (Information Security) ข้อมูลจัดเป็นทรัพย์สินประเภทหนึ่งขององค์กร และเป็นหัวใจหลักสำหรับการดำเนินธุรกิจ ดังนั้นจำเป็นต้องให้ความสำคัญในการรักษาความปลอดภัยของข้อมูล เช่นเดียวกับการรักษาความปลอดภัยของตัวเครื่องและอุปกรณ์ หรืออาจให้ความสำคัญมากกว่าด้วยซ้ำไป

2. ความปลอดภัยทางกายภาพ (Physical Security) ได้แก่ ทรัพย์สินหรืออุปกรณ์ต่าง ๆ

มาตรการการรักษาความปลอดภัยของข้อมูล

1. การระบุตัวบุคคลและอำนาจหน้าที่ (Authentication & Authorization) เพื่อระบุตัวบุคคลที่ติดต่อ หรือทำธุรกรรมร่วมด้วย

2.การรักษาความลับของข้อมูล (Confidentiality) เพื่อรักษาความลับในขณะส่งผ่านทางเครือข่ายไม่ให้ความลับถูกเปิดโดยบุคคลอื่นที่ไม่ใช่ผู้รับ

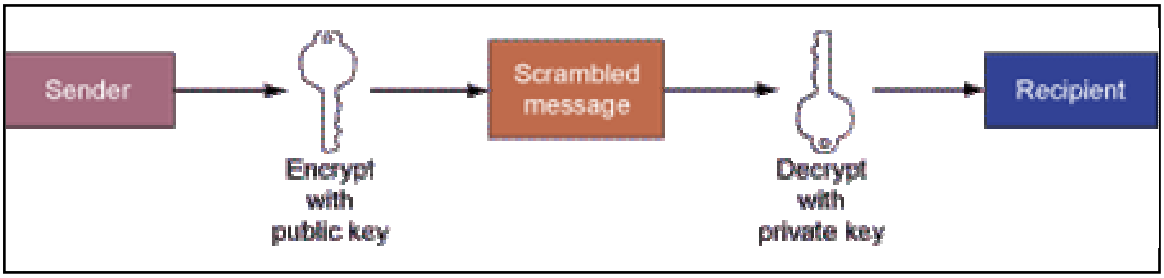
3.การรักษาความถูกต้องของข้อมูล (Integrity) เพื่อการป้องกันไม่ให้บุคคลอื่นที่ไม่ใช่ผู้รับแอบเปิดดู และแก้ไขเปลี่ยนแปลงข้อมูล

4. การป้องกันการปฏิเสธ หรือ อ้างความรับผิดชอบ (None-Repudiation) เพื่อป้องกันการปฏิเสธความรับผิดในการทำธุรกรรมระหว่างกัน เช่น การอ้างว่าไม่ได้ส่งหรือไม่ได้รับข้อมูลข่าวสาร

การรักษาความปลอดภัยของข้อมูล

การเข้ารหัส (Cryptography)

คือ การทำให้ข้อมูลที่จะส่งผ่านไปทางเครือข่ายอยู่ในรูปแบบที่ไม่สามารถอ่านออกได้ ด้วยการเข้ารหัส (Encryption) ทำให้ข้อมูลนั้นเป็นความลับ ซึ่งผู้ที่มีสิทธิ์จริงเท่านั้นจะสามารถอ่านข้อมูลนั้นได้ด้วยการถอดรหัส (Decryption)



ลายมือชื่อดิจิทัล (Digital Signature)

ลายมือชื่อดิจิตอล (Digital Signature) หรือเรียกอีกอย่างว่า ลายเซ็นดิจิตอล ใช้ในการระบุตัวบุคคลเพื่อแสดงถึงเจตนาในการยอมรับเนื้อหาในสัญญานั้น ๆ และป้องกันการปฏิเสธความรับผิดชอบ เพิ่มความน่าเชื่อถือในการทำธุรกรรมร่วมกัน

กระบวนการสร้างและลงลายมือชื่อดิจิทัล

1. นำเอาข้อมูลอิเล็กทรนอิกส์ต้นฉบับ (ในรูปแบบของ file) ที่จะส่งไปนั้น มาผ่านกระบวนการทางคณิตศาสตร์ที่เรียกว่า ฟังก์ชันย่อยข้อมูล (Hash Function) เพื่อให้ได้ข้อมูลที่สั้นเช่นเดียวกับการเข้ารหัสข้อมูลอีกชั้นหนึ่ง ซึ่งข้อมูลจะอ่านไม่รู้เรื่อง จากนั้นก็นำข้อมูลดังกล่าวมาทำการเข้ารหัส (Encryption) อีกที

2. จากนั้นทำการ “ข้ารหัสด้วยกุญแจส่วนตัวของผู้ส่ง” เรียกขั้นตอนนี้ว่า “Digital Signature”

3. ส่ง Digital Signature ไปพร้อมกับข้อมูลต้นฉบับตามที่ระบุในข้อ 1 เมื่อผู้รับ ๆ ก็จะตรวจสอบว่าข้อมูลนั้นถูกแก้ไขระหว่างทางหรือไม่ โดยนำข้อมูลต้นฉบับที่ได้รับ มาผ่านกระบวนการย่อยด้วย ฟังก์ชันย่อยข้อมูล (Hash Function) จะได้ข้อมูลที่ย่อยแล้ว เช่นเดียวกับการคลายข้อมูลที่ถูกบีบอัดอยู่ และ

4. นำ Digital Signature มาทำการถอดรหัสด้วย “กุญแจสาธารณะของผู้ส่ง (Public Key) ก็จะได้ข้อมูลที่ย่อยแล้วอีกอันหนึ่ง จากนั้นเปรียบเทียบข้อมูลที่ย่อยแล้ว ที่อยู่ในข้อ3 และข้อ 4 ถ้าข้อมูลเหมือนกันก็แสดงว่าข้อมูลไม่ได้ถูกแก้ไขระหว่างการส่ง

ใบรับรองดิจิทัล (Digital Certificate)

การขออนุญาตใช้ใบรับรองดิจิทัล (Digital Certificate) ก็เพื่อเพิ่มความน่าเชื่อถือในการทำธุรกรรมร่วมกันบนเครือข่าย Internet ซึ่งหน่วยงานที่สามารถออกใบรับรองดิจิทัล (Digital Certificate) นี้ได้จะเป็น “องค์กรกลาง” ที่มีชื่อเสียงเป็นที่น่าเชื่อถือ เรียกองค์กรกลางนี้ว่า “Certification Authority: CA”

Digital Certificate จะถูกนำมาใช้สำหรับยืนยันในการทำธุรกรรม ว่าเป็นบุคคลนั้นจริงตามที่ได้อ้างไว้ ซึ่งสามารถจำแนกประเภทของใบรับรองดิจิตอล ได้ 3 ประเภท ได้แก่

1. ใบรับรองเครื่องแม่ข่าย (Server)
2. ใบรับรองตัวบุคคล
3. ใบรับรองสำหรับองค์กรรับรองความถูกต้อง

Certification Authority (CA)

CA คือ องค์กรรับรองความถูกต้อง ในการออกใบรับรองดิจิตอล (Digital Certificate) ซึ่งมีการรับรองความถูกต้องสำหรับบริการต่อไปนี้

1. การให้บริการเทคโนโลยีการรหัส ประกอบด้วย

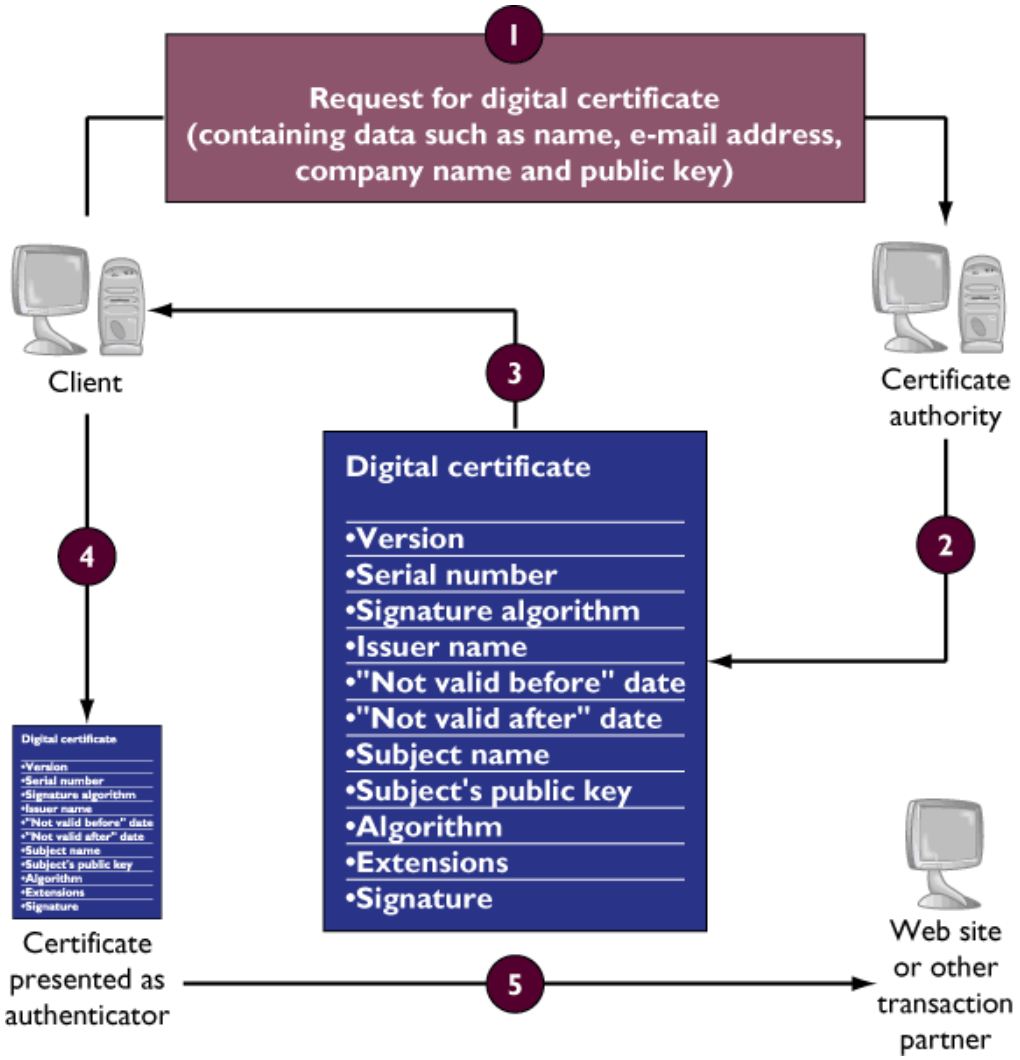
- การสร้างกุญแจสาธารณะ
- กุญแจลับสำหรับผู้จดทะเบียน
- การส่งมอบกุญแจลับ การสร้างและการรับรองลายมือชื่อดิจิตอล

2. การให้บริการเกี่ยวกับการออกใบรับรอง ประกอบด้วย

- การออก การเก็บรักษา การยกเลิก การตีพิมพ์เผยแพร่ ใบรับรองดิจิตอล
- การกำหนดนโยบายการออกและอนุมัติใบรับรอง

3. บริการเสริมอื่น เช่น การตรวจสอบสัญญาต่าง ๆ การทำทะเบียน การกู้กุญแจ

สำหรับประเทศไทย ยังไม่มีองค์กร **"CA"** ซึ่งปัจจุบันหน่วยงานที่ต้องการความน่าเชื่อถือในการทำธรรมบน Web จำเป็นต้องใช้บริการเทคโนโลยีดังที่กล่าวมาจากต่างชาติ แต่คงไม่นานคาดว่าหน่วยงานในภาครัฐอย่างเช่น NECTEC (www.nectec.or.th) คงสามารถพัฒนาเทคโนโลยีต่าง ๆ ดังกล่าวเพื่อให้ใช้บริการภายในประเทศได้



ขั้นตอนการขอ Digital Certificates

การรักษาความปลอดภัยบนระบบเครือข่าย

SSL (Secure Sockets Layer)

SSL ใช้ในการรักษาความปลอดภัยสำหรับการทำธุรกรรมต่าง ๆ ผ่านอินเทอร์เน็ต ซึ่ง SSL นั้นจะใช้ในการเข้ารหัส (encrypt) ข้อมูล ใช้ในการตรวจสอบและยืนยันฝ่ายผู้ขายว่ามีตัวตนอยู่จริง มีขั้นตอนการทำงานของ SSL ดังนี้

1. ผู้ใช้ติดต่อ ไปยัง Web Server ที่ใช้ระบบ SSL
2. จากนั้น Server จะส่งใบรับรอง (Server Certificate) กลับมาพร้อมกับเข้ารหัสด้วยกุญแจสาธารณะ (Public Key) ของเซิร์ฟเวอร์
3. คอมพิวเตอร์ฝั่งผู้รับจะทำการตรวจสอบตัวตนของฝั่งผู้ขายจากใบรับรอง (Server Certificate) จากนั้นก็จะทำการสร้างกุญแจโดยการสุ่มและทำการเข้ารหัสกุญ ด้วยกุญแจสาธารณะของเซิร์ฟเวอร์ที่ได้รับมา เพื่อส่งกลับไปยัง Server
4. เมื่อ Server ได้รับข้อมูลส่งกลับก็จะถอดรหัสด้วยกุญแจส่วนตัว (Private Key) ก็จะได้กุญแจของลูกค้ามาไว้ใช้ในการติดต่อสื่อสาร
5. จากนั้นก็สามารถติดต่อสื่อสารกัน โดยการเข้ารหัสติดต่อสื่อสาร

การป้องกัน Hacker กับ Cracker

การป้องกันที่ได้ผลดีที่สุดคือการใช้ รหัสผ่าน (Password) และใช้ Server ที่มีความปลอดภัยสูง (Secured Server) ไฟร์วอลล์ (Firewall) และเราท์เตอร์ (Router) แต่ไม่ว่าจะป้องกันด้วยวิธีใดก็แล้วแต่ ก็ไม่สามารถมั่นใจได้ว่าวิธีนั้น ๆ จะสามารถป้องกันได้ 100% ตราบใดที่เครื่องคอมพิวเตอร์นั้นยังมีการเชื่อมต่อระบบเครือข่าย

Password

เป็นการรักษาความปลอดภัยขั้นพื้นฐานในการ Login เข้าสู่ระบบ โดยการตั้งรหัสผ่าน (Password) นั้นควรมีความยาวอย่างน้อย 6 ตัวอักษร และไม่ควรง่ายต่อการเดา และควร Update รหัสผ่านอยู่บ่อย ๆ ครั้ง

Firewall

กำแพงไฟ (Firewall) เป็นได้ทั้งฮาร์ดแวร์และซอฟต์แวร์ องค์กรที่มีการเชื่อมต่อเครื่อข่ายกับภายนอก จะใช้ Firewall เพื่อกันคนนอกเข้ามาในเครือข่ายโดยไม่ได้รับอนุญาต ป้องกันการบุกรุกจาก Hacker และ Cracker ที่จะทำอันตรายให้กับเครือข่ายขององค์กร ซึ่ง Firewall จะอนุญาตให้เฉพาะข้อมูลที่มีคุณลักษณะตรงกับเงื่อนไขที่กำหนดไว้ ผ่านเข้าออกระบบเครือข่ายได้

นอกจากนี้ Firewall ยังสามารถกรอง Virus ได้ แต่ไม่ทั้งหมด และก็ไม่สามารถป้องกันอันตรายที่มาจากเครือข่ายอินเทอร์เน็ตทุกรูปแบบได้

Clipper Chip

เป็นวงจรฮาร์ดแวร์ทางอิเล็กทรอนิกส์ที่จะเข้ารหัสเพื่อใช้ในการสื่อสารกันบนอินเทอร์เน็ต คลิปเปอร์ชิปได้รับการเสนอโดยรัฐบาลสหรัฐฯ ชิปนี้ได้จัดทำขึ้นโดยที่ทางรัฐบาลสามารถถอดรหัสนี้ได้ ทำให้เกิดการโต้เถียงกันมากว่ารัฐบาลสหรัฐฯ สามารถติดตามการติดต่อสื่อสารบนอินเทอร์เน็ตได้หมด

อย่างไรก็ตามทางรัฐบาลสหรัฐฯ ก็อ้างว่า รัฐบาลจะถอดรหัสข้อมูลตามคำสั่งศาลเท่านั้น (บทความ รศ.ยืน ภู่วรวรรณ http://www.school.net.th/library/snet1/network/it11.htm)

ซอฟต์แวร์ป้องกันไวรัส (Anti-Virus Software)

Anti-Virus จำเป็นเสมอสำหรับการใช้งานคอมพิวเตอร์ถึงแม้ว่าเครื่องนั้นจะไม่มีการเชื่อมต่อเครือข่ายก็ตาม หน้าที่หลักของ Anti-Virus คือตรวจจับและทำลาย Virus แต่ก็ไม่สามารถป้องกัน Virus ตัวใหม่ ๆ ไม่ให้เข้ามาสู่เครื่องคอมพิวเตอร์ได้

ดังนั้น ซอฟต์แวร์ Anti-Virus จากค่ายใดก็ตามจะมีประสิทธิภาพสูงสุด เพียงช่วงระยะเวลาหนึ่งเท่านั้น เมื่อมี Virus ตัวใหม่เกิดขึ้นก็อาจไม่มีความสามารถเพียงพอที่จะดักจับและทำลาย Virus นั้นได้ ผู้ใช้จึงควร Update ซอฟต์แวร์ Anti-Virus ให้ทันสมัยอยู่เสมอ และปัจจุบันมีซอฟต์แวร์ Anti-Virus ที่มีชื่อเสียงและเป็นที่นิยมในอันดับต้นๆ ของโลกได้แก่

1. Norton Antivirus ของบริษัท Symantec (http://www.symantec.com)
2. McAfee ของบริษัท Network Associates, Inc. (http://www.macafee.com)

แสดงข้อมูล Anti-Virus อื่น ๆ ดังนี้

(http://www.download.com/3120-20_4-0.html?tg=dl-20&qt=Anti%20virus&tag=srch)

Anti- Virus (แบบมีค่าใช้จ่าย)

ลำดับที่	ชื่อ	ความสามารถ
1	SpyWall Anti-Spyware 1.3.9.26	ลบ spyware
2	XoftSpy SE Anti-Spyware 4.22	ตรวจจับและลบ spyware , adware,Trojans
3	XoftSpy SE Anti-Spyware 4.22	ลบ spyware, adware, Trojan horses
4	Spyware Doctor 4	ลบ spyware, adware, Trojan horses, keyloggers
5	McAfee VirusScan Plus 2007	ลบ spyware และ virus ที่คุกคามเครื่องและป้องกันโปรแกรมอื่นที่มุ่งร้ายต่อเครื่อง
6	AVG Anti-Virus Free Edition 7.5.4	ป้องกันเครื่องจาก Virus และโปรแกรมอื่นที่มุ่งร้ายต่อเครื่อง

Free AntiVirus

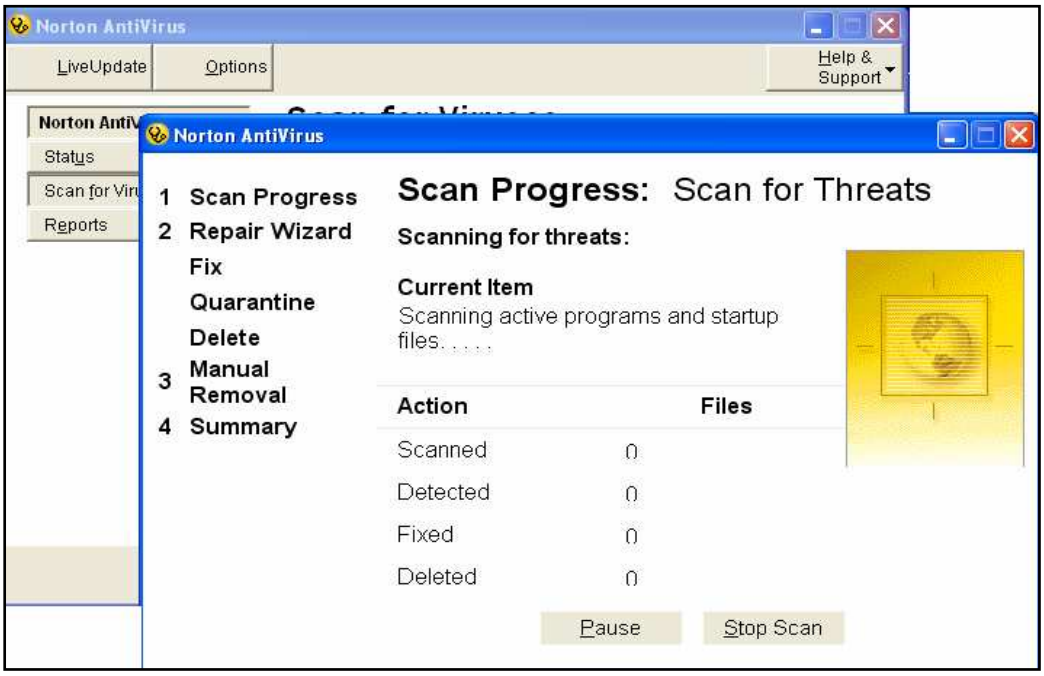
(http://www.pctools.com/free-antivirus/?ref=google_antivirus)

ลำดับที่	ชื่อ	ความสามารถ
1	PC Tools AntiVirus™ 3.1 Free Edition	ป้องกันและต่อต้านสิ่งชั่วร้ายต่าง ๆ ที่มาจากการคุกคามของโลก Cyber ไม่ให้เข้าถึงและทำลายข้อมูลในเครื่อง PC
2.	Avira AntiVir PersonalEdition Classic	มีความน่าเชื่อถือในการต่อต้านและป้องกันอันตรายที่มาจาก Virus, worms, Trojans

Norton Antivirus

Norton เป็น Software ที่ได้รับความนิยมมาก สามารถป้องกัน Virus ได้เกือบ 90% อีกทั้งยังใช้งานง่ายและมี Update Center ในการปรับปรุง Software ให้สามารถดักจับ Virus ตัวใหม่ ๆ ให้ทันสมัยอยู่เสมอ

นอกจากนี้ Norton Antivirus ยังสามารถสร้างตารางเวลาในการสแกนไวรัสอัตโนมัติ การทำแผ่นดิสก์ฉุกเฉินกรณีที่ไม่สามารถเข้าสู่โปรแกรมวินโดวส์ได้



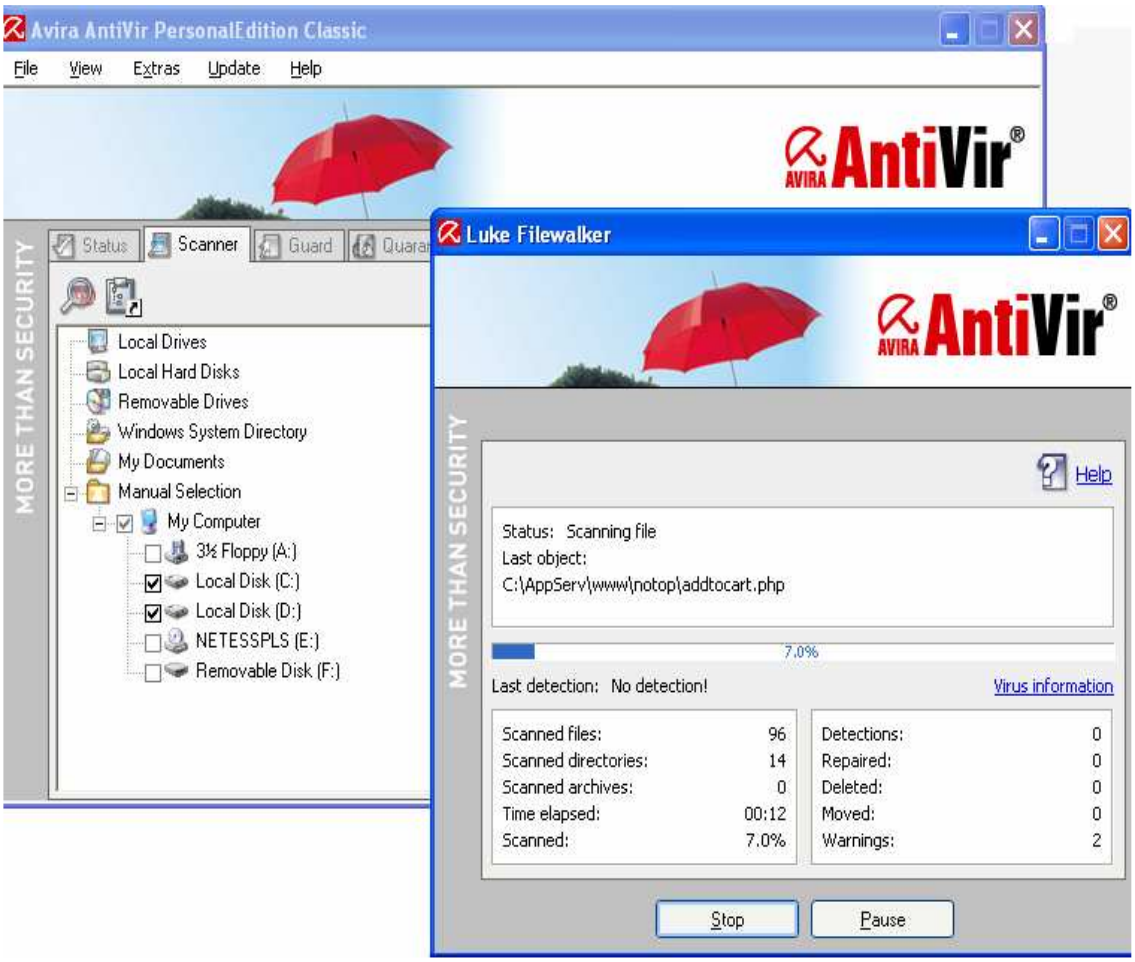
แสดงภาพตัวอย่างการทำงานของโปรแกรม Norton Anti-Virus

McAfee Anti-Virus

เป็นอีกหนึ่งในโปรแกรมที่ได้รับความนิยมรองจาก Norton Antivirus มีความแม่นยำในการตรวจจับ Virus สแกน E-mail ที่ได้รับ มี Update Center เพื่อปรับปรุงความสามารถของโปรแกรมให้ใหม่อยู่เสมอ และมีรูปแบบที่ง่ายต่อการใช้งาน (http://it-info.tu.ac.th/program.html)

Avira Anti-Virus

เป็นอีกโปรแกรมหนึ่งที่มีประสิทธิภาพในการดักจับ Virus ใช้งานง่ายและ Vision สำหรับใช้งานฟรีโดยไม่ต้องเสียค่าใช้จ่าย



สามารถ Download Avira Anti- Virus รุ่น Classic เพื่อใช้งานฟรีได้ที่ www.avira.com ซึ่งเมื่อเข้าไปใน web site แล้วสามารถศึกษาข้อมูลเกี่ยวกับรายชื่อ และความรุนแรงของ Virus ได้ดังตัวอย่าง


AVIRA
English
Home » Virus Info » Virus Search
Search
Home
Support
Solutions
Products
Downloads
Virus Info
Statistics
VDF History
Virus Science
Security News
Viruses In the Wild
Company
Press
Partners
Newsletter
Virus Search
Search by name:
Statistics
Virus Science
A · B · C · D · E · F · G · H · I · J · K · L · M · N · O · P · Q · R · S · T · U · V · W · X · Y · Z
Latest descriptions
RSS
No. Name Type Danger Added on
1. Worm/Braban.H Worm 05 Sep 2006
2. Sierra Central Credit Union 1 Phishing 01 Sep 2006
3. Worm/Rbot.180736.7 Worm 01 Sep 2006
4. Federal Deposit Insurance Corporation 2 Phishing 31 Aug 2006
5. Worm/Brontok.a Worm 30 Aug 2006
6. MidAmerica Bank 1 Phishing 30 Aug 2006
7. TR/Dldr.Ba.any.88.C Trojan 29 Aug 2006
8. Worm/Womble.A Worm 29 Aug 2006
9. Listerhill Credit Union 1 Phishing 29 Aug 2006
10. TR/Dldr.EbayBill.H Trojan 29 Aug 2006
11. Worm/Scano.W.1 Worm 29 Aug 2006
TopThreats
Worm/Bagz.D.3
Worm/NetSky.P
Worm/Bagz.C.2
Worm/Mytob.NT
Worm/NetSky.Z
Latest Thre
Worm/Braban.H
Sierra Central Credit Union 1
Worm/Rbot.180736.7
Federal Deposit Insuran Corporation 2
Worm/Brontok.a
RSS Fee
Get comfortable up to th info from Avira as
RSS

12.	Worm/Scano.Q.3	Worm		29 Aug 2006
13.	TR/Spy.Banker.550548	Trojan		29 Aug 2006
14.	Elizabethton Federal Savings Bank 3	Phishing		28 Aug 2006
15.	Worm/Scano.Q.1	Worm		28 Aug 2006
16.	TDECU 3	Phishing		28 Aug 2006
17.	TR/Spy.Banker.anv.1891	Trojan		25 Aug 2006
18.	Worm/Sdbot.664576.B	Worm		25 Aug 2006
19.	TR/Dldr.Malwar.AG	Trojan		25 Aug 2006
20.	TR/Spy.Banker.819156	Trojan		24 Aug 2006
21.	Nationwide 7	Phishing		24 Aug 2006
22.	Nationwide 6	Phishing		24 Aug 2006
23.	TR/Spy.Small.GI	Trojan		24 Aug 2006
24.	TR/Dldr.Small.GL1	Trojan		24 Aug 2006
25.	TR/PSW.WOW.CR	Trojan		24 Aug 2006
26.	TR/PSW.Sinowal.V.5	Trojan		24 Aug 2006
27.	National Credit Union Administration 16	Phishing		23 Aug 2006
28.	BDS/Hupigon.E.201	Backdoor Server		23 Aug 2006
29.	TR/Spy.Banker.bhq.3	Trojan		23 Aug 2006
30.	TR/Proxy.Small.DU.8	Trojan		23 Aug 2006
31.	TR/Dldr.Ba.any.79.A	Trojan		23 Aug 2006
32.	Air Academy Federal Credit Union 1	Phishing		23 Aug 2006
33.	TR/Spy.Banker.533556	Trojan		23 Aug 2006
34.	TR/Dldr.VB.alb.2	Trojan		23 Aug 2006
35.	TR/Dldr.EbayBill.G.1	Trojan		23 Aug 2006
36.	TR/Spy.Banker.551280	Trojan		22 Aug 2006
37.	TR/Dldr.Goldun.CW	Trojan		22 Aug 2006
38.	Citizens National Bank of Texas 2	Phishing		22 Aug 2006
39.	Paypal 114	Phishing		22 Aug 2006

ความปลอดภัยในการชำระเงินด้วยบัตรเครดิตผ่านเครือข่าย Internet

การชำระเงินค่าสินค้าและบริการ ด้วยบัตรเครดิตบนระบบ Internet นั้นอาจมีความเสี่ยงอยู่บ้าง เพราะเป็นช่องทางใหม่ที่เรายังไม่คุ้นเคยนัก ยังไม่อาจมอบความไว้วางใจกับ Web Site ที่เข้าไปชำระเงิน

แต่ถ้าเปรียบเทียบกันแล้วระหว่างการชำระเงินด้วยบัตร Credit บนระบบ Internet กับการชำระด้วยบัตร Credit ตามร้านค้าหรือปั๊มน้ำมันทั่วไปที่เราเข้าไปใช้บริการ คิดว่าความเสี่ยงบนระบบ Internet น่าจะน้อยกว่าเนื่องจากเราเป็นผู้กรอกหมายเลขบัตร Credit ด้วยตนเอง และทำรายการทุก

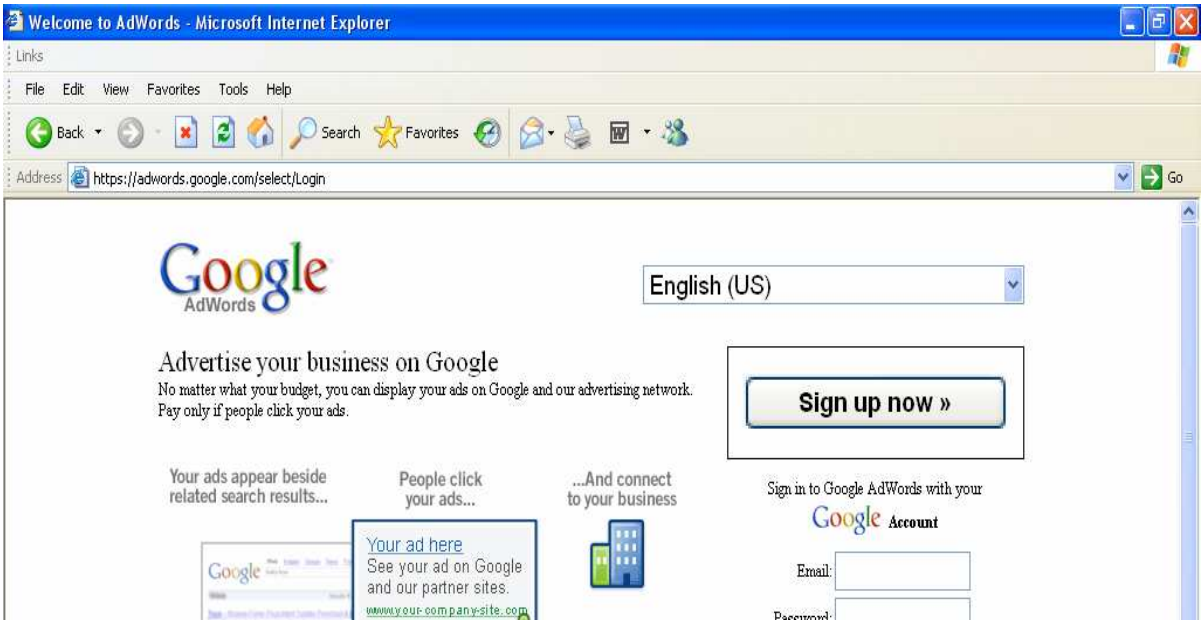
อย่างด้วยตนเองและเราก็ควรเลือกทำ ธุรกรรมซื้อขายกับ Web site ที่มีชื่อเสียงเป็นที่น่าเชื่อถือที่เปิดให้บริการมานาน เช่น Amazon.com Dell.com หรือ Thailand.com เนื่องจาก Web เหล่านี้จะมีภาพลักษณ์ที่ดี และอยู่ในธุรกิจมานาน ดังนั้นน่าจะมีระบบรักษาความปลอดภัยและป้องกันการบุกรุกได้ดี แต่ถ้าหากเป็นร้านค้าอาจมีความเสี่ยงที่เราอาจคาดไม่ถึงเนื่องจากเราไม่ได้ทำรายการของบัตร Credit ด้วยตัวเอง หากแต่เป็นพนักงานในร้านที่เป็นคนรูดบัตรแล้วจะมั่นใจได้อย่างไรว่าพนักงานจะไม่แอบจดหมายเลขบัตรและคัดลอกบัตรไว้

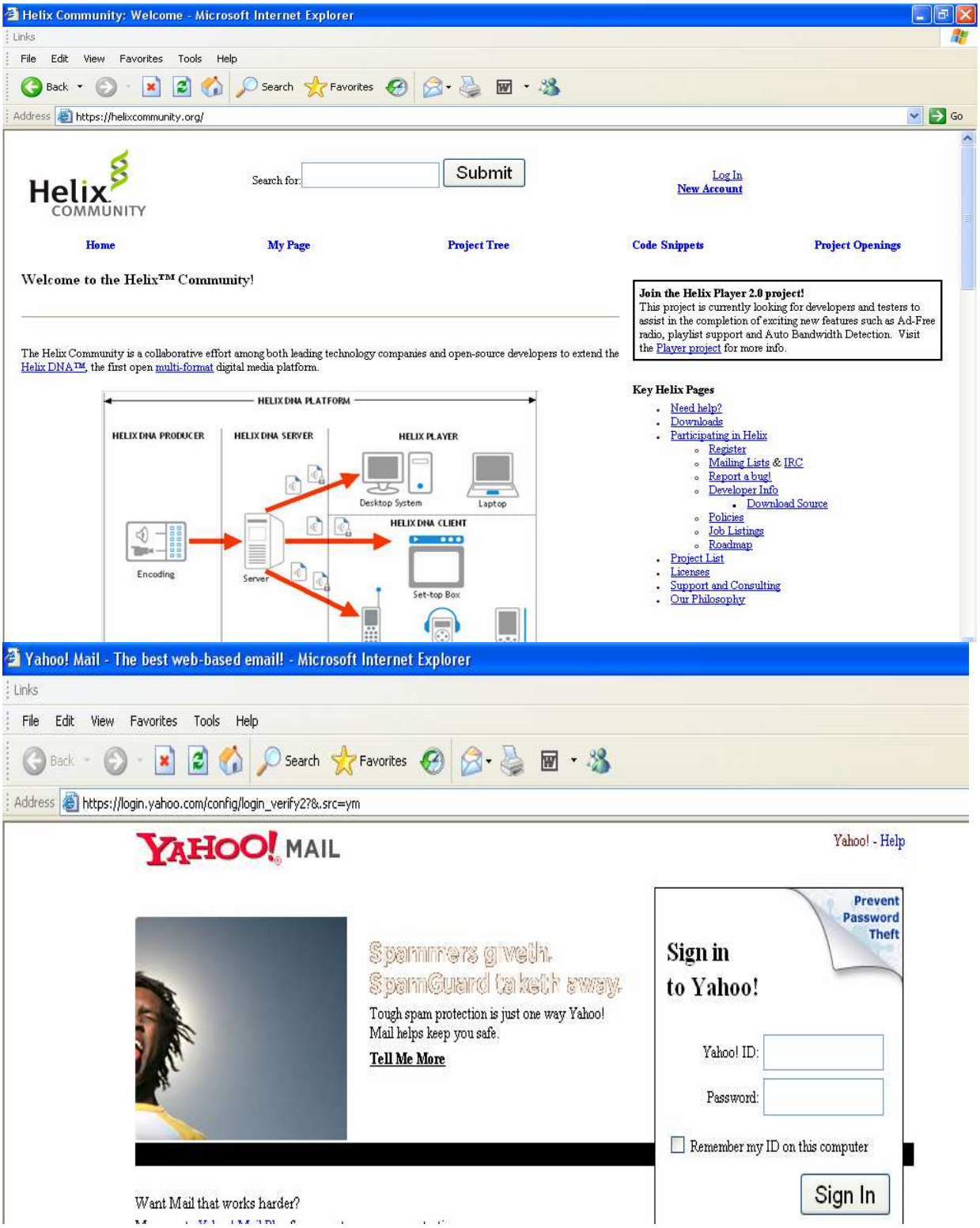
การสังเกตความปลอดภัยในการซื้อขายบน Web Sit

สังเกตุได้จากปัจจัยหลัก ๆ ดังต่อไปนี้

1.ชื่อเสียงของเว็บไซต์ ดูได้จากความนิยมของเว็บไซต์ ระยะเวลาที่เปิดดำเนินการมา หรือดูจากบริษัทที่เป็นเจ้าของเว็บไซต์นั้นว่าเป็นอย่างไร เช่น Thailand.com เป็นไซเบอร์มอลล์ที่ดำเนินธุรกิจโดยบริษัท Internet Thailand จำกัด (มหาชน) ซึ่งเป็นผู้ให้บริการอินเทอร์เน็ตที่อยู่ในธุรกิจมาอย่างยาวนาน หรือ amazon.com เป็น web site ขายหนังสือที่มีชื่อเสียงโด่งดังไปทั่วโลก

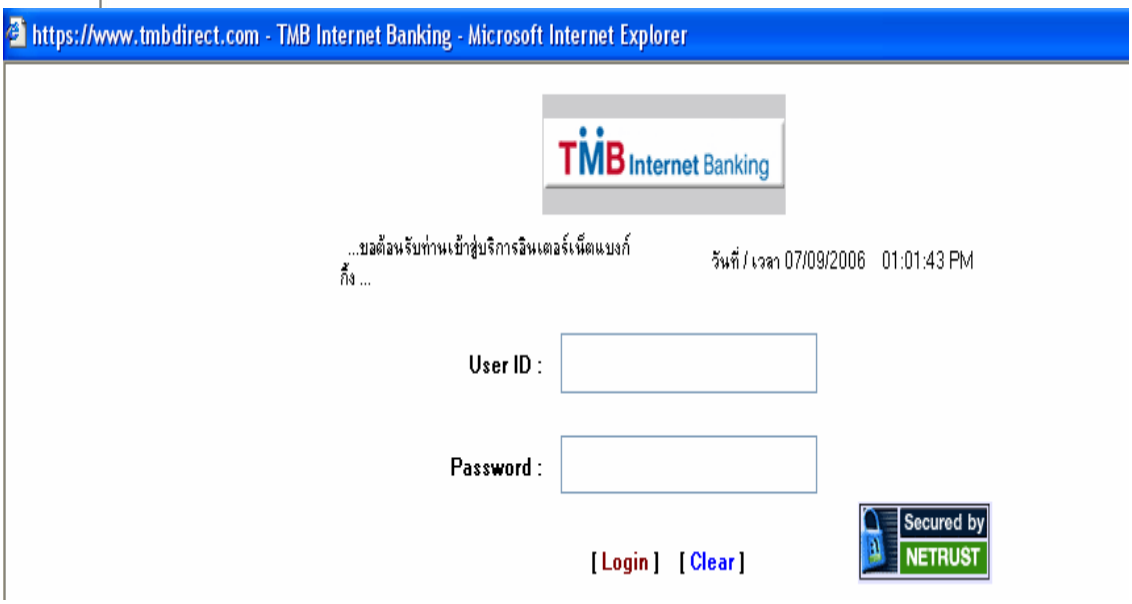
2. เว็บไซต์จะต้องสนับสนุนระบบ SSL (Secure Socket Layer) URL โดยปกติของการเข้าถึงเว็บไซต์ใด ๆ จะขึ้นต้นด้วย HTTP (HyperText Transmission Protocol) เป็นมาตรฐาน แต่หากว่ากำลังเข้าสู่โหมด(Mode) รักษาความปลอดภัยของ SSL URL จะเปลี่ยนเป็น HTTPS (Hyper Text Transmission Protocol Secure) ตัวอย่าง ดังเช่น web site ต่อไปนี้

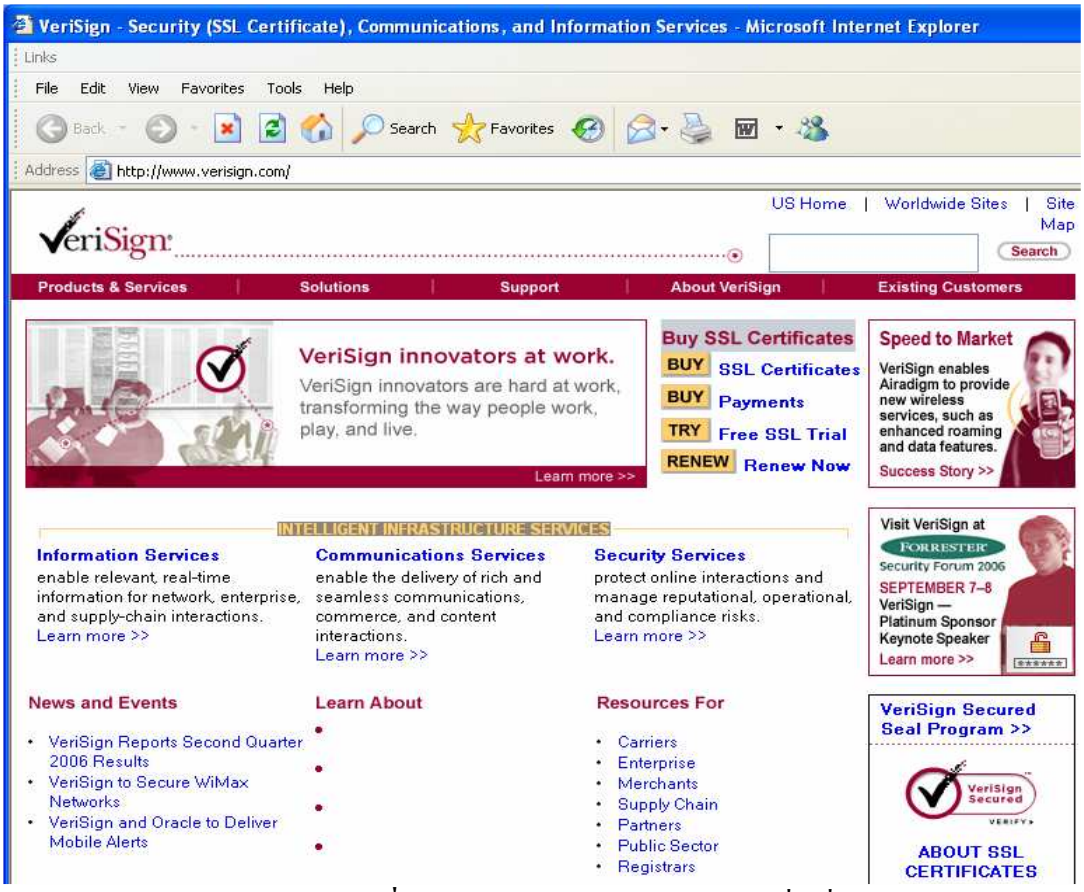




3. เว็บไซต์ควรจะได้รับการรับรองเรื่องความปลอดภัย โดยมีเครื่องหมาย Verisign's Secure Site ปรากฏอยู่


https://order.tmbam.com - FundLink OnLine - TMB Asset Management Co., Ltd. - Microsoft Internet Explorer
TMBAM
TMB Asset Management
FUNDLINK ONLINE
Customer Login
โปรดใส่รหัสผู้ใช้ รหัสผ่าน เพื่อเข้าสู่ระบบ
Please enter your username and password to sign in.
รหัสผู้ใช้ (Username)
รหัสผ่าน (Password)
เข้าสู่ระบบ
VeriSign Secured
VERIFY


https://www.tmbdirect.com - TMB Internet Banking - Microsoft Internet Explorer
TMB Internet Banking
...ขอต้อนรับท่านเข้าสู่บริการอินเตอร์เน็ตแบงก์กิ้ง ...
วันที่ / เวลา 07/09/2006 01:01:43 PM
User ID :
Password :
[Login] [Clear]
Secured by NETRUST



4. นโยบายส่งเสริมความมั่นใจหลังการขาย เว็บไซต์ที่ดีเชื่อถือได้จะต้องระบุนโยบายหลังการขายอย่างละเอียดไว้บนเว็บไซต์เพื่อให้ลูกค้าทราบนโยบายหลังการขาย เช่น นโยบายตรวจสอบข้อมูลสินค้าที่สั่งซื้อ นโยบายการส่งคืนสินค้าและคืนเงินที่ชำระไปแล้ว เช่น กรณีที่สั่งซื้อหนังสือที่ web site ของ amazon.com หนังสือนั้นจะถูกขนส่งข้ามประเทศโดยเรือขนส่งสินค้า หากสินค้าที่ได้รับเกิดการชำรุดระหว่างทาง แล้วเราต้องการคืนสินค้านั้น จะต้องดูนโยบายการรับคืนสินค้าและการคืนเงินด้วย

สมาร์ตการ์ด (Smart Card)

Smart Card เป็นบัตรพลาสติกที่มี “ชิบขนาดเล็ก (Microchip)” สำหรับเก็บข้อมูล โดยจะเก็บข้อมูลส่วนตัวของเจ้าของบัตรซึ่งประกอบด้วย ข้อมูลเงินสดในบัญชี เบอร์บัญชีเงินฝากหมายเลขบัตรหรือรายละเอียดเกี่ยวกับการเงินต่างๆ สามารถใช้ในการจ่ายเงินค่าสินค้าผ่านอินเทอร์เน็ตและมีความปลอดภัยสูงกว่าการใช้บัตร Credit อีกทั้งยังพกพาได้สะดวกและมีความเป็นส่วนตัว

การรักษาความปลอดภัยทางกายภาพ

มีหลายวิธีที่จะใช้สำหรับการรักษาความปลอดภัยให้กับตัวเครื่องและอุปกรณ์คอมพิวเตอร์ เช่น

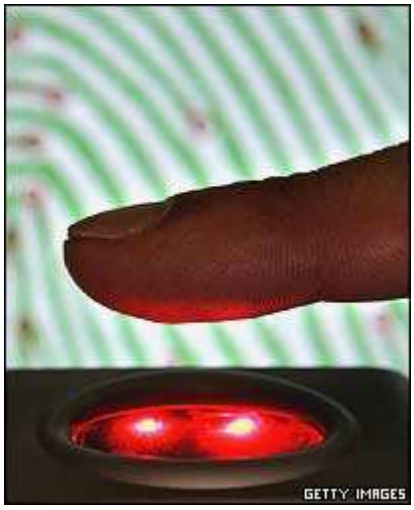
1. การใช้พนักงานรักษาความปลอดภัย อาจใช้ รปภ. จับขโมยและผู้บุกรุก

2. ใช้ระบบรักษาความปลอดภัยในการเข้า - ออก จากห้องคอมพิวเตอร์ เช่น

- ล๊อคห้องคอมพิวเตอร์ด้วยกุญแจ

- เข้าและออกจากห้องด้วยระบบ Key Card

- ใช้ระบบเข้าออกจากห้องโดยการสแกนลายนิ้วมือ (Finger Scan)



- ใช้ระบบสแกนม่านตา (Eye Scan)

3. ใช้กุญแจล็อคเครื่องและอุปกรณ์คอมพิวเตอร์

http://www.locdown.com/images/BMSe-MacCBLKit2004.jpg

http://www.csiro.au/files/images/p46.jpg

4. ใช้ระบบสำรองไฟ เช่น ใช้เครื่อง UPS ในการสำรองไฟ เมื่อไฟดับเพื่อป้องการการเสียหายของ Hardware และข้อมูลภายใน

5. ใช้สารเคมีในการดับไฟเมื่อเกิดไฟไหม้ เมื่อเกิดไฟไหม้ในห้องคอมพิวเตอร์จะไม่สามารถใช้น้ำในการดับไฟ เนื่องจากเมื่อดับไฟได้แล้วก็จะทำให้เครื่องและอุปกรณ์เกิดความเสียหาย ดังนั้นจึงจำเป็นต้องใช้สารเคมีชนิดพิเศษในการดับไฟ

6. การออกแบบห้องคอมพิวเตอร์ศูนย์กลางให้อยู่ในชั้นที่สูงขึ้นเพื่อป้องกันน้ำท่วม

การป้องกันภัยที่อาจเกิดกับเครื่อง (Hardware) และข้อมูล (Data)

1. เลือกใช้ระบบคอมพิวเตอร์ที่มีความทนทานสูง (Fault-tolerant computer systems) ซึ่ง Fault-tolerant ระบบที่ใช้ hardware คุณสมบัติพิเศษ หรือใช้ Hardware software และ power supply เพิ่มเติมจากที่มีอยู่ เพื่อให้อุปกรณ์สามารถทำงานได้อย่างต่อเนื่อง ไม่ให้การให้บริการนั้นถูกขัดจังเหวะ
2. เลือกใช้ระบบคอมพิวเตอร์ที่มีขีดความสามารถในการประมวลผลสูง (High-availability computing) โดยอาจเลือกใช้เครื่องมือและเทคโนโลยีภายในระบบที่มีคุณภาพสูง ในการกู้คืนระบบได้อย่างรวดเร็วเมื่อระบบถูกระทบหรือถูกทำลาย
3. การวางแผนการกู้คืนระบบ (Disaster recovery plan) เป็นการวางแผนสำหรับกู้คืนระบบหากระบบล่ม ธุรกิจนั้นต้องสามารถดำเนินต่อไปได้ เมื่อเกิดเหตุการณ์ใดเข้ามาขัดจังหวะการให้บริการ
4. การกระจายงานที่เหมาะสม (Load balancing) เป็นการกระจายจำนวนงานที่มีการร้องขอจากเครื่องคอมพิวเตอร์ลูกข่าย ไปยัง servers ตัวอื่น ๆ ให้เกิดความสมดุลระหว่างเครื่อง อย่าให้เครื่อง Server เครื่องใดเครื่องหนึ่งทำงานหนักจนเกินไป
5. การทำซ้ำระบบ (Mirroring) คือ การทำซ้ำทุกโปรแกรม ทุกงาน และทุก transactions ที่อยู่บน server เพื่อ backup ข้อมูลและป้องกันการถูกขัดจังหวะการให้บริการ
6. การทำงานสองระบบ (Clustering) งานควรจะถูกกระทำลงในเครื่องคอมพิวเตอร์ 2 เครื่องทุกครั้ง โดยใช้คอมพิวเตอร์เครื่องที่ เป็นตัว backup ข้อมูลของเครื่องหลัก (ซึ่งเครื่องต้องมีความเร็วในการประมวลผลสูง)
7. มีระบบตรวจจับผู้บุกรุก (Intrusion Detection System) โดยตรวจสอบจุดที่ทำให้ถูกโจมตีได้ง่าย ภายในระบบเครือข่าย ป้องกันและขัดขวางไม่ให้ผู้ที่ไม่มีสิทธิ์แอบเข้ามาในระบบ

นโยบายภาครัฐกับมาตรการรักษาความปลอดภัย

1. จัดเตรียมบุคลากรที่สามารถจับผู้กระทำความผิด ตรวจตราดูแลความสงบสุขในการใช้เทคโนโลยีสารสนเทศ

2. NECTEC จัดตั้ง Computer Emergency Response Team (CERT) เพื่อเป็นหน่วยงานที่คอยประสานงานในเรื่องการละเมิดความปลอดภัยบนเครือข่าย

การรักษาความปลอดภัยของคอมพิวเตอร์

การรักษาความปลอดภัย(security) คืออะไร

การรักษาความปลอดภัยไม่ใช่การขัดขวางไม่ให้มีคนใช้ระบบของคุณ คุณอาจจะทำอย่างนั้นได้ง่าย ๆ โดยการ ถอดปลั๊กคอมพิวเตอร์และใช้ค้อนทุบลงบนฮาร์ดไดรฟ์ของคุณ แน่นอนว่าไม่มีใครสามารถเข้าถึงมันได้อีก

อีกทั้งการรักษาความปลอดภัยไม่ใช่การขัดขวางไม่ให้คนดูว่ามีอะไรในระบบคุณ ถ้าสิ่งนี้เป็นการรักษาความปลอดภัย ดังนั้นจึงไม่มีความจำเป็นที่ต้องใช้ระบบคอมพิวเตอร์ถ้ายูสเซอร์ไม่สามารถหาไฟล์ได้ แล้วระบบจะมีไว้ทำอะไร ?

จริง ๆ แล้วการรักษาความปลอดภัยเกี่ยวข้องกับการนำยูสเซอร์ให้เข้ามาในระบบและให้พวกเขาเข้าถึงไฟล์ได้ รวมถึงการจำกัดผู้ใช้ที่ได้รับการอนุญาตให้เข้ามาได้และจำกัดในสิ่งที่พวกเขาสามารถเห็นและทำได้เมื่อเข้ามาในระบบ ในเวลาเดียวกันจุดประสงค์ของการรักษาความปลอดภัยก็เพื่อทำสิ่งต่าง ๆ ให้ง่ายที่สุดเท่าที่จะเป็นไปได้ เพื่อให้ยูสเซอร์สามารถทำงานได้สำเร็จตามสภาพที่ควบคุมไว้ แต่ถ้ายากเกินไปสำหรับพวกเขาที่จะทำงาน เน็ตเวิร์คจะกลายเป็นอุปสรรคและไม่มีประโยชน์

หนังสือเกี่ยวกับการรักษาความปลอดภัยของคอมพิวเตอร์หลายเล่มให้คำจำกัดความของการรักษาความปลอดภัยไว้ดังนี้

คอมพิวเตอร์ปลอดภัยถ้าคุณสามารถใช้มันและซอฟท์แวร์ของมันให้ทำงานอย่างที่คุณหวังให้มันเป็น กระทรวงกลาโหมสหรัฐ ฯ (DoD) ชี้ว่าคอมพิวเตอร์ไม่มีวันปลอดภัยอย่างสิ้นเชิง ดังนั้นพวกเขาจึงได้พัฒนา แนวความคิดของระดับความเชื่อถือ(trustedness) เพื่อให้คำจำกัดความของสถานะที่เป็นไปได้ระหว่าง การไม่มีการรักษาความปลอดภัยในระบบนั้นและการรักษาความปลอดภัยที่ไม่มีข้อบกพร่องจนไม่มีใครสามารถเข้าถึงได้ ความเชื่อถือที่ให้นิยามโดย DoD มี 7 ระดับ ระดับความปลอดภัยนี้แบ่งโดยใช้ตัวอักษร D, C, B และ A ตามด้วยตัวเลข 1,2 หรือมากกว่า ในที่นี้ตัวอักษรถูกเรียงจากข้างหลังไปข้างหน้าเพราะระบบที่มีระดับ D มีการรักษาความปลอดภัยที่ต่ำกว่าระบบที่เป็นระดับ C ตัวเลข 1 และ 2 ใช้เพื่อบอกถึงการรักษาปลอดภัยในระดับย่อยในระดับนั้น ระดับเจ็ดระดับจากต่ำสุดไปสูงสุดดังนี้:

* D

* C1

* C2

* B1

* B2

* B3

* A1

การรักษาความปลอดภัยระดับ D

ระบบปฏิบัติการที่มีระดับ D มีการรักษาความปลอดภัยที่น้อยที่สุด(ไม่มีการรักษาความปลอดภัยโดยพื้นฐาน) ขาดวิธีที่จะระบุว่าใครที่กำลังใช้งาน ระบบที่มีระดับ D มีการควบคุมการเข้าถึงไฟล์เพียงเล็กน้อยหรือไม่มีเลย

ระบบปฏิบัติการที่พยายามใช้มาตรการรักษาความปลอดภัยที่ล้มเหลวหรือต้องการการเปิดใช้งานลักษณะเด่น (ไม่เปิดการใช้งานโดยค่าเริ่มต้น) จัดเป็นระบบระดับ D ด้วย ตัวอย่างของระบบปฏิบัติการระดับ D คือ MS-DOS, NetWare หลายเวอร์ชันก็จัดอยู่ในประเภทนี้ด้วยเพราะลักษณะเด่นด้านการรักษาความปลอดภัย ไม่ได้เปิดใช้งานโดยค่าเริ่มต้นในระหว่างการลงซอฟท์แวร์

การรักษาความปลอดภัยระดับ C1

ระบบปฏิบัติการที่มีการรักษาความปลอดภัยระดับ C1 หรือ Discretionary Security Protection มีการรักษาความปลอดภัยมากกว่าระบบปฏิบัติการระดับ D การรักษาความปลอดภัยที่เพิ่มขึ้นมามีวิธีการ พิสูจน์ตัวผู้ใช้และการควบคุมการเข้าถึงไฟล์

อีกนัยหนึ่ง ยูสเซอร์ต้องแสดงตัวเองต่อระบบปฏิบัติการเพื่อ log in เข้าสู่ระบบ หลังจาก log in วิธีที่ พวกเขาใช้แสดงตัวจะกำหนดว่าไฟล์ใดที่พวกเขาสามารถเข้าถึงได้

คำว่า "Discretionary" หมายถึงการเข้าถึงที่ถูกกำหนดอยู่ในเกณฑ์ของ "need-to-know" ตัวอย่างของระบบปฏิบัติการระดับ C1 โดยทั่วไปได้แก่ ยูนิกซ์และเน็ตแวร์

Discretionary Access Control ทำให้เจ้าของไฟล์สามารถเปลี่ยนสิทธิ์และความเป็นเจ้าของต่อไฟล์ จำกัดว่าใครสามารถอ่าน ใช้งานและลบไฟล์ บ่อยมากที่คำว่า Trusted Computing Base (TCB) ถูกใช้ในความหมายเดียวกับการรักษาความปลอดภัย ระดับ C1 แต่จริง ๆ แล้ว TCB เป็นวิธีการหนึ่งเพื่อให้ความปลอดภัยระดับ C TCB มีการแบ่งยูสเซอร์และ ข้อมูลและทำให้ยูสเซอร์สามารถป้องกันผู้อื่นจากการอ่าน เปลี่ยนแปลงหรือทำลายข้อมูล โดยผ่านสิทธิ์(rights) คุณสมบัติ(attribute) และการอนุญาต (permission)

การรักษาความปลอดภัยระดับ C2

การรักษาความปลอดภัยระดับ C2 หรือ Controlled Access Protection ระบบปฏิบัติการมีองค์ประกอบ ของระบบปฏิบัติการระดับ C1 และมีการบันทึก(auditing)เหตุการณ์ที่เกี่ยวข้องกับการรักษาความปลอดภัยเข้ามาด้วย สิ่งนี้สามารถช่วยให้จำกัดผู้ใช้จากการรันคำสั่งโดยขึ้นอยู่กับระดับของการอนุญาตที่พวกเขาได้รับ และมีการบันทึกเหตุการณ์ที่เกิดขึ้นในระบบ การบันทึกนี้ใช้เพื่อบันทึกเหตุการณ์ที่เกี่ยวข้องกับการรักษาความปลอดภัย เช่น กิจกรรมที่ทำโดยผู้บริหารระบบ การบันทึกนี้ต้องใช้การพิสูจน์เพิ่มเติม

Controlled Access Protection หมายถึง การบันทึกและเพิ่มการพิสูจน์ตัวที่เพิ่มมาจากการรักษาความปลอดภัยระดับ C1

การรักษาความปลอดภัยระดับ B

การรักษาความปลอดภัยระดับ B ระบบปฏิบัติการจะสูญเสียความง่ายในการใช้งาน ในระดับนี้ลักษณะเด่นด้าน การรักษาความปลอดภัยที่กล่าวมาแล้วก่อนหน้านี้ต้องใช้ทั้งหมดรวมกับ mandatory access control ต่อ name subject และ object ยูสเซอร์ ไฟล์และโปรแกรมต้องได้รับการระบุและกำหนดระดับความปลอดภัยที่เฉพาะเจาะจง กระบวนการนี้เรียกว่า labeling ข้อมูลที่นำเข้าและส่งออกต้องมีชื่อ (label) นอกจากนี้ ระบบบันทึก(audit) ต้องบันทึกหลาย ๆ อย่างอันประกอบด้วย:

* การลบทุกอย่าง
* การกระทำทุกอย่างที่ทำโดยโอเปอร์เรเตอร์
* การกระทำทุกอย่างที่ทำโดยผู้บริหารระบบ
* การเข้าสู่ระบบที่ล้มเหลว
* การใช้ระบบช่วยเหลือใด ๆ ก็ตาม
* การเปิดไฟล์ทุกอย่าง

ระดับความปลอดภัยที่เพิ่มขึ้นจาก B1 ถึง B3 มาตรการป้องกันมีความเข้มงวดมากยิ่งขึ้น การรักษาความ ปลอดภัยระดับ C2 เกี่ยวข้องกับ Controlled Access Protection ระดับ B เกี่ยวข้องกับ:

* B1 - Labeled Security Protection
* B2 - Structured Protection
* B3 - Security Domain

ระดับ B1 เป็นระดับแรกที่สนับสนุนการรักษาความปลอดภัยหลายระดับ เช่น "secret" และ "top secret" ระดับนี้ object ภายใต้ mandatory access control ไม่ได้รับการอนุญาตให้เปลี่ยนการอนุญาตในการเข้าถึงไฟล์โดยเจ้าของไฟล์

ระดับ B2 เพิ่มความสามารถในการบอกถึงปัญหาของ object ที่อยู่ในระดับสูงกว่าของการสื่อสารที่มีการรักษาความปลอดภัยกับ object ในระดับที่มีการรักษาความปลอดภัยในระดับที่ต่ำกว่า

ระดับ B3 บังคับให้เทอร์มินัลของยูสเซอร์ต้องต่อกับระบบ ผ่านเส้นทางที่เชื่อถือได้

การรักษาความปลอดภัยระดับ A

ระดับสุดท้ายจากคำนิยามของกระทรวงกลาโหมสหรัฐ ฯ (จาก Orange Book) คือ A1 หรือระดับการ ออกแบบที่ได้รับการตรวจสอบความถูกต้อง ระดับนี้ต้องการการออกแบบที่ได้รับการตรวจสอบความถูกต้องทางคณิตศาสตร์ การวิเคราะห์อย่างละเอียดของแต่ละ channel ที่ซ่อนอยู่และ trusted distribution ซึ่งจำเป็นที่ฮาร์ดแวร์และซอฟทแวร์ต้องมีการป้องกันในระหว่างการขนส่งสินค้าเพื่อป้องกันการเข้าไปเปลี่ยน แปลงระบบรักษาความปลอดภัย

การรักษาความปลอดภัยระดับ A1 เป็นระบบที่อยู่ในห้องลับที่ไม่มีใครสามารถเข้าถึงได้ และเป็นสิ่งที่ปฏิบัติไม่ได้ในการทำการค้า ไม่เพียงแต่มาตรการและการอารักขาที่สูงเท่านั้น แต่ค่าใช้จ่ายในการดำเนินการและการ ดูแลรักษาเป็นอุปสรรคในทัศนะทางด้านการเงินอีกด้วย

ตารางต่อไปนี้ดัดแปลงมาจาก Orange Book เปรียบเทียบลักษณะเด่นหลาย ๆ อย่างของการรักษาความปลอดภัยระดับต่าง ๆ สังเกตได้ว่าแต่ละระดับที่สูงกว่าจะรวมเอาลักษณะเด่นในระดับที่ต่ำกว่าด้วย

NetWare Security

เน็ตแวร์เสนอลักษณะเด่นทางด้านการรักษาความปลอดภัย 2 ชุดคือ ชุดหนึ่งที่เปิดการใช้งานอยู่แล้วโดยที่คุณไม่ต้องทำอะไรอีก และชุดที่มีอยู่แต่คุณจำเป็นต้องเปิดการใช้งาน โดยการรวมเข้าด้วยกันลักษณะเด่นด้าน การรักษาความปลอดภัยของเน็ตแวร์สามารถจัดอยู่ในระดับ D, C หรือแม้แต่ B ลักษณะเด่นด้านการรักษาความปลอดภัยของเน็ตแวร์เสนอสิ่งต่อไปนี้:

* การระบุชื่อยูสเซอร์ (User login identification)
* การระบุกลุ่มยูสเซอร์ (Group identification)
* การจัดการเกี่ยวกับรหัสผ่านและการเข้ารหัส (สามารถเลือกได้)
* การควบคุมทรัพยากร โดยผ่านทางสิทธิ์(rights) และคุณสมบัติ(attributes)
* การรักษาความปลอดภัยของ Server console

ส่วนประกอบที่สำคัญที่สุดในการรักษาความปลอดภัยของเน็ตแวร์คือผู้บริหารระบบ ต้องรู้ว่าอะไรที่ต้องดำเนินการ ดำเนินการอย่างถูกต้องและดูแลรักษา เน็ตแวร์มีสิ่งที่จำเป็นสำหรับการรันเน็ตเวิร์ตไซต์ที่ปลอดภัย ผู้บริหารระบบมีหน้าที่ที่จะต้องใช้อย่างฉลาด

ในเน็ตแวร์การระบุตัว(identification)และการพิสูจน์ตัว(authentication)เกิดขึ้นในเวลาเดียวกันโดยผ่านขั้นตอน login การระบุตัวผู้ใช้ทำโดยการใส่ login ID ที่ถูกลงไป การพิสูจน์ผู้ใช้เกิดขึ้นเมื่อมีการใส่รหัสผ่านที่ถูกต้อง

เมื่อมีการระบุและพิสูจน์ตัวผู้ใช้แล้ว ยูสเซอร์จะอยู่หนึ่งในห้าประเภท ดังต่อไปนี้:

* supervisor
* ยูสเซอร์ที่เทียบเท่ากับ supervisor

* workgroup manager

* account manager

* ยูสเซอร์

สิทธิ์และการเข้าถึงข้อมูลของยูสเซอร์แต่ละประเภทถูกจำกัดโดยคำจำกัดความของแต่ละยูสเซอร์ สิ่งที่ควรสังเกตคือ supervisor สามารถเข้าถึงได้ทั้งระบบ ยูสเซอร์ธรรมดามีการเข้าถึงที่จำกัดมากในสิ่งที่ได้เฉพาะเจาะจงไว้เท่านั้น ส่วนยูสเซอร์ระดับอื่นจะอยู่ระหว่าง supervisor และยูสเซอร์ธรรมดา supervisor มีเพียงยูซเซอร์เดียวเท่านั้น จำนวนของยูสเซอร์ที่เทียบเท่ากับ supervisor ควรมีจำนวนจำกัด แต่ยูสเซอร์ธรรมดาไม่จำกัดจำนวน

Supervisor

เมื่อลงเน็ตแวร์เรียบร้อยแล้ว account supervisor ที่มีเพียงหนึ่งเดียวถูกสร้างขึ้นมาสำหรับเซิร์ฟเวอร์ ยูสเซอร์มีสิทธิ์ต่อ utility และไฟล์ทุกไฟล์ในเน็ตเวิร์ค มีความสามารถที่จะลบยูสเซอร์อื่นที่อยู่ในเน็ตเวิร์ค เพิ่มยูสเซอร์และทำทุกอย่างที่เกี่ยวข้องกับการบริหารระบบ แปลกที่ว่าสิ่งที่เดียวที่ยูสเซอร์นี้ทำไม่ได้คือ การลบ account ของ supervisor เอง

ยูสเซอร์ที่เทียบเท่ากับ supervisor

อีกยูสเซอร์หนึ่งที่มีสิทธิ์เทียบเท่ากับ supervisor สามารถสร้างและลบยูสเซอร์อื่น (และยูสเซอร์ที่เทียบเท่ากับ supervisor ด้วย) สามารถเปลี่ยนรหัสผ่านของตนเอง รวมทั้งรหัสผ่านของ supervisor ด้วย

Workgroup Managers

workgroup manager เป็นยูสเซอร์หรือกลุ่มยูสเซอร์ที่มีอำนาจจำกัดในการสร้างและจัดการเกี่ยวกับยูสเซอร์ และกลุ่มของยูสเซอร์ ลบยูสเซอร์และกลุ่มของยูสเซอร์ที่พวกเขาได้สร้างขึ้น กำหนดการเข้าถึงไฟล์และจำกัด ปริมาณและเนื้อที่ของดิสก์

อย่างไรก็ตาม workgroup manager ไม่สามารถสร้างยูสเซอร์หรือกลุ่มยูสเซอร์ที่เทียบเท่ากับ supervisor หรือจัดการเกี่ยวกับยูสเซอร์หรือกลุ่มยูสเซอร์ที่พวกเขาไม่ได้สร้างขึ้น หรือลบยูสเซอร์นี้ ไม่สามารถสร้างหรือ ลบลำดับในการพิมพ์ หรือเปลี่ยนแปลงการจำกัดสิทธิ์ของ login ของใครก็ตาม

Account Managers

account manager มีสิทธิ์เช่นเดียวกับ workgroup manager ยกเว้นแต่พวกเขาสามารถทำได้เพียงแต่ การจัดการยูสเซอร์ที่ได้รับการกำหนดไว้เท่านั้น พวกเขาไม่สามารถเพิ่มยูสเซอร์หรือกลุ่มยูสเซอร์ขึ้นมาใหม่

ยูสเซอร์

เป็นผู้ที่ log in เข้ามาในเน็ตเวิร์คและไม่อยู่ในประเภทอื่น เป็นยูสเซอร์ส่วนใหญ่ของระบบ

supervisor และยูสเซอร์ที่เทียบเท่าสามารถใช้คำสั่ง FCONSOLE ได้โดยไม่จำกัด แต่ workgroup manager และ account manager สามารถใช้ได้อย่างจำกัด

FCONSOLE เป็น utility อันทรงพลัง สามารถทำสิ่งต่าง ๆ ได้ดังต่อไปนี้:

* ส่ง broadcast message
* เปลี่ยนไปใช้เซิร์ฟเวอร์อื่น
* ดูรายละเอียดการติดต่อของยูสเซอร์
* ปิดไฟล์เซิร์ฟเวอร์จากการใช้งานของ workstation
* ดูและเปลี่ยนสถานะของไฟล์เซิร์ฟเวอร์
* ดูเวอร์ชันของเน็ตแวร์ที่เซิร์ฟเวอร์ใช้อยู่

ถ้าต้องการเปลี่ยนไปที่เซิร์ฟเวอร์อื่น เลือกที่เมนู Change Current File Server จากเมนูหลักของ FCONSOLE รายชื่อเซิร์ฟเวอร์อื่นจะปรากฏขึ้น แล้วเลือกเซิร์ฟเวอร์ที่คุณต้องการติดต่อ กด Enter ถ้าต้องการออกจากระบบ เลือกที่เมนู Server แล้วกดปุ่ม Del ถ้าต้องการเปลี่ยนยูสเซอร์ที่ใช้ log in อยู่ ให้กดปุ่ม F3

เมนู Connection Information แสดงถึงการติดต่อทุกชนิดที่เข้ามายังเซิร์ฟเวอร์ อัปเดททุก ๆ 2 วินาที โดยค่าเริ่มต้น

ข้อสังเกต: คุณสามารถส่งข้อความไปยังยูสเซอร์แบบเจาะจงโดยเลือกยูสเซอร์จากหน้าจอ Current Connection แล้วกด Enter แล้วจึงเลือก Broadcast Console Message จากเมนู Connection Information ซึ่งปรากฏขึ้นแล้วจึงพิมพ์ข้อความของคุณ (ความยาวไม่เกิน 55 ตัวอักษร)
ถ้าเลือกเมนู Down File Server จากเมนูหลักของ FCONSOLE เพื่อปิด File Server จากเครื่อง workstation เมื่อเลือกเมนูนี้แล้วจะปรากฏกล่องข้อความให้เลือก Yes สำหรับยืนยันการปิดและ No สำหรับกลับไปเมนูก่อนหน้านี้

ถ้าเลือกเมนู Status จากเมนูหลักของ FCONSOLE จะเห็นสิ่งต่อไปนี้:

* Server date
* Server time
* Login restriction status
* Transaction tracking status

ถ้าต้องการเปลี่ยนค่าต่าง ๆ ข้างบนนี้ให้ใช้ arrow key เพื่อให้ปรากฏแถบสีที่ส่วนนั้นแล้วจึงกด Enter แล้วพิมพ์ค่าใหม่ลงไป แล้วกด ESC เพื่อ save สิ่งที่ได้เปลี่ยนแปลงไป
เมนูสุดท้ายใน FCONSOLE คือ Version Information แสดงถึงข้อมูลโดยทั่วไปเกี่ยวกับเน็ตแวร์ที่กำลังทำงานอยู่ คุณจะเห็นได้ว่าทำไมความสามารถเหล่านี้จึงทำให้ FCONSOLE เป็น utility ที่ทรงพลังและเป็นสิ่งหนึ่งที่ ควรปกป้องจากยูสเซอร์ให้มากเท่าที่จะเป็นไปได้