Digital Harm

ตอนที่ 1

ผศ.สุพล พรหมมาพันธุ์

ภาควิชาคอมพิวเตอร์ธุรกิจ คณะสารสนเทศศาสตร์ มหาวิทยาลัยศรีปทุม

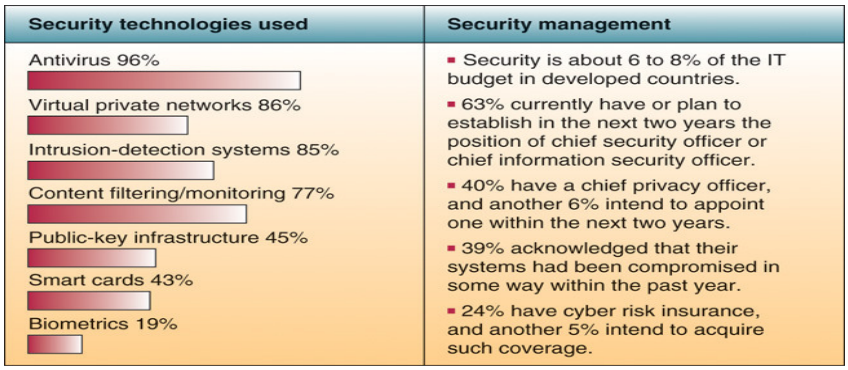
(ลงตีพิมพ์ในวารสาร ส่งเสริมเทคโนโลยี ฉบับที่197 เดือนกุมภาพันธ์ – มีนาคม พ.ศ. 2551 หน้า 84)

ภัยคุกคามมนุษยชาติในปัจจุบันอีกแนวทางหนึ่ง นอกเหนือจากภัยธรรมชาติต่างๆ แล้ว ยังมีภัยอีกประเภทหนึ่ง ซึ่งอยู่ใกล้ตัวมาก ได้แก่ ภัยที่เกิดจากการใช้เครื่องคอมพิวเตอร์ไม่ว่าจะเป็นที่บ้าน หรือที่ทำงาน ตลอดจนถึงการใช้อินเตอร์เน็ตเพื่อการสื่อสารทั้งหลาย เช่น การส่งจดหมายอิเล็กทรอนิกส์, การสนทนา, การประชุม, การสืบค้นข้อมูล, การทำธุรกิจ เป็นต้น ย่อมมีโอกาสประสบกับภัยอันตรายที่กล่าวนี้ เรียกโดยรวมว่า **ภัยยุคดิจิตอล หรืออาชญากรรมคอมพิวเตอร์** (Computer Crime) อาชญากรรมทางคอมพิวเตอร์นี้ สมาคมผู้เป็นมืออาชีพทางเทคโนโลยีสารสนเทศ (Association of Information Technology Professional : AITP) ได้ใคร่ครวญร่วมกันพิจารณาและได้ให้แนวทางเป็นเครื่องชี้นำว่า ผู้ใช้คอมพิวเตอร์ หรือ ผู้เป็นมืออาชีพในทางธุรกิจ และเทคโนโลยีสารสนเทศ จำต้องมีเครื่องชี้นำด้านจริยธรรมความประพฤติเข้ามาช่วย เพื่อลดปัญหาอาชญากรรมที่เกิดขึ้น คือ (1) ต้องมีความซื่อสัตย์ (Acting with integrity), (2) เพิ่มสมรรถนะความเป็นมืออาชีพของตนเอง (Increasing your professional competence), (3) ตั้งเกณฑ์การทำงานไว้ให้สูง (Setting high standards of personal performance), (4) มีความรับผิดชอบในการทำงาน (Accepting responsibility for your work) และ (5) รักษาสุขภาพ, รักษาความเป็นส่วนตัว และ (5) ดูแลสวัสดิการสาธารณะทั่วไป (Advancing the health, privacy, and general welfare of the public) ดังนั้น นอกจากหลักความประพฤติเหล่านี้แล้ว ยังต้องพยายามหลีกเลี่ยงจากปัญหาอาชญากรรมคอมพิวเตอร์ และเพิ่มการพัฒนาระบบความปลอดภัยทางด้านระบบสารสนเทศให้มากขึ้นด้วย สำหรับปัญหาด้านอาชญากรรมทางคอมพิวเตอร์ในปัจจุบันนับวันยิ่งเป็นภัยคุกคามต่อมนุษย์และสังคมมากขึ้นทุกขณะ โดยเฉพาะการใช้คอมพิวเตอร์ อินเตอร์เน็ต และเครือข่ายคอมพิวเตอร์ประเภทอื่นๆ แบบไร้ความสำนักรับผิดชอบ ดังนั้น จึงเป็นเรื่องที่ท้าทายสำหรับผู้ที่ทำงานอยู่ในด้านเทคโนโลยีสารสนเทศที่จะต้องร่วมกันใช้เทคโนโลยีอย่างมีจิตสำนึก และจะต้องมีการพัฒนาทฤษฎีของการรักษาความปลอดภัยก่อนเป็นอันดับแรก สำหรับปัญหาทางอาชญากรรมทางคอมพิวเตอร์ที่ถูกกำหนดโดยสมาคมผู้เป็นมืออาชีพทางด้านเทคโนโลยีสารสนเทศ (AITP) นั้น หมายรวมถึงในเรื่องเหล่านี้ คือ (1) การใช้งานโดยไม่ได้รับอนุญาต, การเข้าถึง, การแก้ไข, และการทำลายฮาร์ดแวร์, ซอฟท์แวร์, ข้อมูล, หรือทรัพยากรเครือข่าย (2) ผู้ที่ไม่มีสิทธิ์เข้ามาแก้ไขสารสนเทศ (3) การคัดลอกซอฟท์แวร์โดยไม่ได้รับอนุญาต (4) การปฏิเสธผู้ใช้ในการเข้าถึงฮาร์ดแวร์, ซอฟท์แวร์, ข้อมูล หรือเครือข่ายอื่นๆ และ (5) การใช้ หรือการสมรู้ร่วมคิดในการใช้คอมพิวเตอร์ หรือทรัพยากรเครือข่าย หรือใช้สารสนเทศไม่ถูกต้องตามกฎหมาย หรือละเมิดทรัพย์สินทางปัญญา ตัวแบบของอาชญากรรมทางคอมพิวเตอร์ที่มีผลกระทบหรือไม่ถูกต้องตามกฎหมายมีหลายประการ คือ

- **การขโมยฮาร์ดแวร์** (Hardware Theft) การขโมยฮาร์ดแวร์ และการทำลายทรัพย์สินของอุปกรณ์คอมพิวเตอร์ต่างๆ มีโอกาสเสี่ยงสูงมากที่จะถูกขโมยหรือถูกทำลาย การขโมยฮาร์ดแวร์ คือ การขโมยอุปกรณ์คอมพิวเตอร์ หรือทำการเปลี่ยนถ่ายอุปกรณ์คอมพิวเตอร์ ลักษณะการขโมย หรือทำลายมีหลายลักษณะ บาง

คนอาจทำการตัดสายเคเบิ้ล โดยมีจุดหมายเพื่อทำลายธุรกิจ หรือ การทำลายเครื่องคอมพิวเตอร์ในโรงเรียน หรือในมหาวิทยาลัยให้แตกหักเป็นเสี่ยงๆ เพื่อไม่ให้สามารถใช้งานได้ เนื่องจากในโรงเรียน หรือในมหาวิทยาลัย มีเครื่องคอมพิวเตอร์เป็นจำนวนมาก จึงอาจตกเป็นเป้าหมายในการทำลายมากกว่าเครื่องคอมพิวเตอร์ที่บ้านผู้ใช้เครื่องคอมพิวเตอร์มือถือ และโน๊ตบุ๊คคอมพิวเตอร์ มีโอกาสเสี่ยงต่อการถูกขโมยมีมาก เนื่องจากมีขนาดเล็ก จากการคาดหมายทำให้ทราบว่าในแต่ละปี มีโน๊ตบุ๊คคอมพิวเตอร์ถูกขโมยมากกว่า 600,000 เครื่อง ด้วยขนาดของโน๊ตบุ๊คที่มีขนาดเล็กและน้ำหนักเบา ทำให้ถูกขโมยได้อย่างง่ายดาย โจรขโมยได้เล็งหาเป้าหมายโน๊ตบุ๊คคอมพิวเตอร์ของผู้บริหารของบริษัทเป็นหลัก นอกจากขโมยได้ง่ายแล้ว ยังสามารถเข้าถึงข้อมูลความลับต่างๆ ของบริษัทได้อีกด้วย นอกจากนี้การขโมยฮาร์ดแวร์ ยังหมายรวมไปถึงซอฟท์แวร์ และระบบสารสนเทศด้วย

วิธีป้องกันการขโมยฮาร์ดแวร์ และการทำลายทรัพย์สินนั้น บางโรงเรียน บางมหาวิทยาลัย และบางบริษัทมีการตรวจวัดระดับความปลอดภัย เพื่อลดความเสี่ยงต่ออันตรายเหล่านี้ การควบคุมความปลอดภัยที่เห็นเป็นรูปธรรม ได้แก่ การปิดประตูและหน้าต่าง ซึ่งเป็นระบบป้องกันที่สามารถทำได้โดยง่าย นอกจากนั้น ในส่วนของบริษัท หรือที่บ้าน ควรมีการติดตั้งสัญญาณกันขโมย เพื่อเพิ่มระดับความปลอดภัย ในส่วนของโรงเรียน และมหาวิทยาลัย อาจใช้วิธีล็อกกุญแจสายอุปกรณ์คอมพิวเตอร์ทั้งหมดเข้าด้วยกัน ไม่ว่าจะเป็นสายเมาส์ คีย์บอร์ด ลำโพง รวมทั้งสายเครื่องพิมพ์ด้วย. หรืออาจมีการล็อกตู้หรือโต๊ะสำหรับวางคอมพิวเตอร์ด้วย ในส่วนของโน๊ตบุ๊คคอมพิวเตอร์ ในกรณีที่เป็นแขกเข้าพักตามโรงแรม ควรล็อกโน๊ตบุ๊ตคอมพิวเตอร์ไว้กับโต๊ะหรือเตียง หรือเมื่อออกจากห้องพักไปแล้ว ควรปิดล็อกประตูให้แน่นหนาด้วย หรือมีการติดตั้งสัญญาณกันขโมยด้วย เมื่อโน๊ตบุ๊คคอมพิวเตอร์ถูกเคลื่อนย้าย ก็จะมีสัญญาณดัง เป็นต้น ในส่วนของอุปกรณ์มือถือขนาดเล็ก เช่น Palmtop หรือ PDA ควรมีการติดตั้งอุปกรณ์กันขโมยขนาดเล็ก เมื่อถูกขโมยไปก็สามารถติดตามได้โดยสะดวกว่าตอนนี้ไปอยู่ ณ จุดใด นอกจากนี้ ยังมีวิธีอื่นๆ อีก เช่น การตั้งรหัสลับ, การใช้เครื่องรูดบัตร, หรือการใช้การสแกนลายพิมพ์นิ้วมือเอาไว้ เพื่อใช้เข้ารหัสผ่านเข้าสู่เครื่องคอมพิวเตอร์ ทำให้การโจรกรรมทำได้ยากขึ้น เป็นต้น



ภาพที่ 1 แสดงการักษาความปลอดภัยทางคอมพิวเตอร์ ที่มีการใช้โปรแกรมตรวจสอบและทำลายไวรัสถึง 96 % มากกว่าวิธีการอื่นๆ (James A.O'Brien : 2006 : 440)

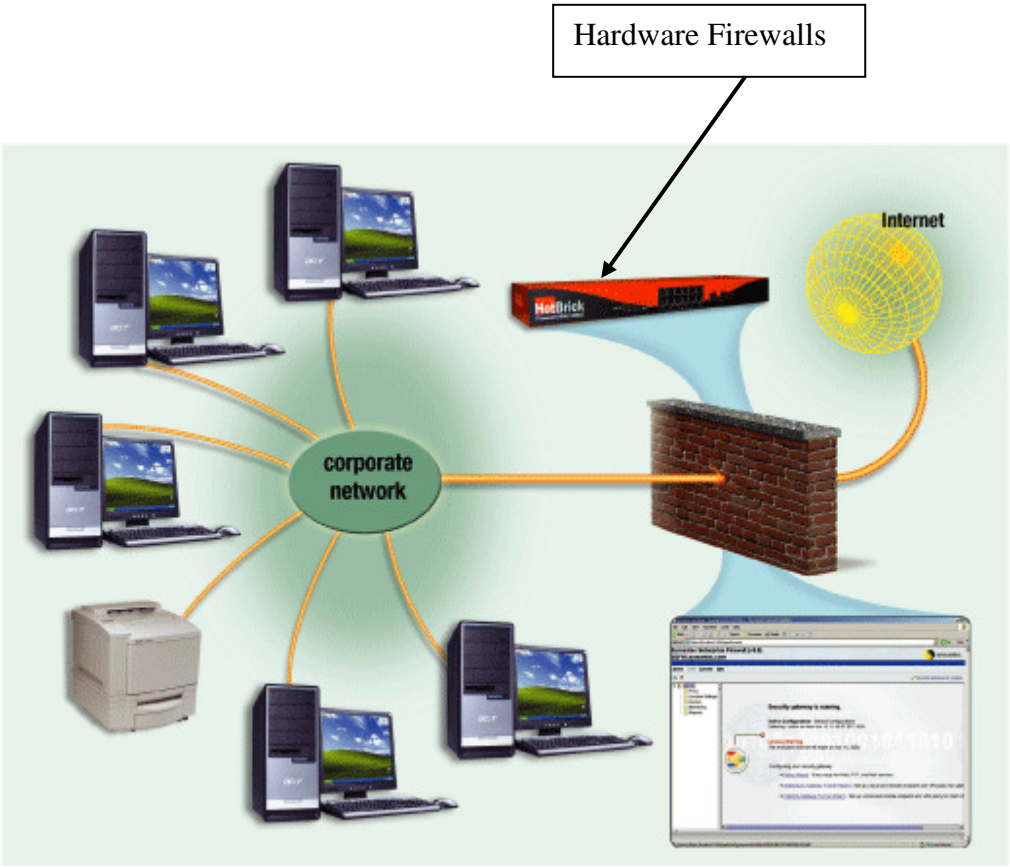
- **การขโมยซอฟต์แวร์** (Software Theft) เกิดขึ้นจากสาเหตุของกลุ่มบุคคลกระทำการอันเป็นเหตุอันตรายทำให้บุคคลอื่นได้รับความเสียหาย คือ (1). การขโมยสื่ออุปกรณ์ของซอฟต์แวร์ เกี่ยวข้องกับการขโมยสื่อที่บรรจุซอฟต์แวร์หรือโปรแกรม เช่น การขโมยแผ่น CD-ROM ของเอ็นไซค์โคลพีเดีย (Encyclopedia) ในห้องสมุด เป็นต้น , (2). การตั้งใจลบโปรแกรม เกี่ยวข้องกับโปรแกรมเมอร์ของบริษัทบางคน ไม่มีความซื่อสัตย์

ต่อองค์กร ทำการลบชุดคำสั่งของโปรแกรมที่ตนเองเขียนเอาไว้ทิ้ง, (3). การคัดลอกโปรแกรม โดยผิดกฎหมาย ในกรณีนี้ เกิดจาการขโมยซอฟต์แวร์ออกมาจากโรงงานผลิต และนำไปทำการคัดลอกเพื่อทำการค้าหรือธุรกิจ ซึ่งกระบวนการเรียกว่า **การละเมิดทรัพย์สินทางปัญญา**

วิธีการป้องกัน การขโมยซอฟต์แวร์ ได้แก่ การทำการตกลงกันระหว่างผู้ซื้อและผู้ขายในการใช้ซอฟต์แวร์ที่เรียกว่า License Agreement **เช่น** การอนุญาตให้คัดลอกได้ไม่เกิน 3 ครั้ง, การอนุญาตให้ติดตั้งซอฟต์แวร์ได้บนเครื่องคอมพิวเตอร์เครื่องเดียว, การอนุญาตให้ติดตั้งซอฟต์แวร์บนเครื่องคอมพิวเตอร์แบบตั้งโต๊ะได้หนึ่งเครื่อง การอนุญาตให้ติดตั้งซอฟต์แวร์บนโน๊ตบุ๊คคอมพิวเตอร์ได้หนึ่งเครื่อง, เช่า หรือเช่าซื้อซอฟต์แวร์ เป็นต้น

- **การขโมยสารสนเทศ** (Information Theft) ส่วนใหญ่เป็นการขโมยสารสนเทศซึ่งเป็นความลับของแต่ละบุคคล หรือการทำให้สารสนเทศเกิดความเสียหายใช้งานไม่ได้ การขโมยสารสนเทศนี้ สามารถเกิดขึ้นได้ทั้งกับบริษัท และที่บ้าน ผู้บริหารระดับสูงของบางบริษัทอาจไม่มีความซื่อสัตย์สุจริต หรือขาดจริยธรรมในการดำเนินธุรกิจ อาจมีการว่าจ้างให้บุคคลอื่นขโมย หรือทำการจัดซื้อสารสนเทศที่ถูกขโมยมาเพื่อประโยชน์ หรือก่อให้เกิดข้อได้เปรียบกับธุรกิจของตนเอง และประเด็นสำคัญที่สุด คือต้องการรู้ความลับ และกลยุทธ์วิธีการดำเนินธุรกิจของคู่แข่งขัน เช่น การแอบขโมยข้อมูลหมายเลขบัตรเครดิตของลูกค้า ในขณะที่ลูกค้าเข้ามาซื้อสินค้า การขโมยสารสนเทศในลักษณะนี้ จัดเป็นอาชญากรรมคอมพิวเตอร์ที่กำลังระบาด หรือในอีกกรณีหนึ่ง คือ ในการส่งสารสนเทศไปบนเครือข่ายคอมพิวเตอร์นั้น อาจมีผู้ไม่หวังดีทำการดักจับการส่งข้อมูลหรือสารสนเทศ ทำให้สามารถล่วงรู้ความลับต่างๆ ที่ถูกส่งผ่านไปบนเครือข่ายคอมพิวเตอร์ ส่วนใหญ่จะเรียกกลุ่มบุคคลผู้กระทำการเหล่านี้ว่า ผู้เจาะระบบ (Hacker) วิธีการป้องกันการขโมยสารสนเทศที่เกิดขึ้นในลักษณะนี้ หลายบริษัทได้ทำการพัฒนาระบบใหม่ๆ ขึ้นมา เช่น การป้องกันโดยให้ผู้ใช้สามารถเทคนิคการสร้างรหัสลับ หรือรหัสผ่านของตนเองขึ้นมาใหม่ได้ เพื่อเก็บรักษาข้อมูลความลับของตน และความเป็นส่วนตัวของตนเอง โดยปกติแล้วเทคนิคการสร้างรหัสลับขึ้นมานั้นจะเป็นหน้าที่ของซอฟต์แวร์ เช่น **ซอฟต์แวร์กำแพงเพลิง** (Firewalls) เป็นซอฟต์แวร์รักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์ หรือซอฟต์แวร์รักษาความปลอดภัยของทรัพยากรของเครือข่ายคอมพิวเตอร์จากผู้บุกรุกหรือผู้ที่ไม่หวังดี โดยทำหน้าที่ในการป้องกัน แจ้งเตือนผู้บุกรุกเข้ามาทำลายระบบเครือข่าย โดยซอฟต์แวร์ Firewalls นี้จะมีการรับรู้ที่รวดเร็วมาก จะทำการแจ้งเตือนได้อย่างรวดเร็ว เช่น มีบุคคลรุกล้ำเข้ามาในระบบบัญชีเงินเดือน หรือระเบียนของบุคคลที่มีการจัดเก็บเอาไว้เป็นความลับ องค์กรธุรกิจ หรือบริษัทสามารถที่จะทำการพัฒนาซอฟต์แวร์ Firewalls ของตนเองขึ้นมาได้ เพื่อให้มีความเหมาะสมกับธุรกิจของตนเอง หรืออาจจะมีการว่าจ้างบริษัทภายนอก (Outsourcing) ให้ทำการพัฒนาให้ก็ได้เช่นกัน หากเป็นธุรกิจขนาดเล็กก็สามารถพัฒนาซอฟต์แวร์ Firewalls ของตนเองขึ้นมาใช้ได้เหมือนกันเพื่อรักษาความปลอดภัยคอมพิวเตอร์ของเขา โดยมีชื่อเรียกว่า ซอฟต์แวร์กำแพงเพลิงส่วนบุคคล (Personal Firewalls) โปรแกรมระบบปฏิบัติการบางชนิดที่ทันสมัยในปัจจุบัน เช่น Windows XP จะมีโปรแกรม Firewalls ติดมาด้วย เพื่อส่งเสริมสนับสนุนการรักษาป้องกันความปลอดภัยบนเครื่องคอมพิวเตอร์ส่วนบุคคล ผู้ใช้บางคนอาจจัดหาจัดซื้อซอฟต์แวร์ Firewalls มาใช้กับเครื่องส่วนตัวเครื่องเดียวของตนเองได้ โดยราคาประมาณ $50 ดอลล่าร์ หรือประมาณ 1,663 บาท มีบริษัทขนาดเล็ก หรือคนที่ใช้บ้านทำเป็นสำนักงาน มีการจัดซื้อ Hardware Firewalls เช่น Router หรืออุปกรณ์คอมพิวเตอร์อื่นๆ ซึ่งจะมีซอฟต์แวร์ Firewalls ติดมาด้วย ซึ่งเป็นเสมือนใช้ทำหน้าที่

แทนซอฟต์แวร์ Firewalls ไปในตัว ในส่วนของ Hardware Firewalls นี้ จะหยุดการทำงานก็ต่อเมื่อมีการปิดเครื่องคอมพิวเตอร์เท่านั้น



ภาพที่ 2 แสดงการทำงานของ Hardware Firewalls สำหรับเครือข่ายคอมพิวเตอร์ที่ใช้งานในองค์กร (Gary B.Shelly : 2007 : 563)

ส่วนซอฟต์แวร์ตัวใหม่ล่าสุดชื่อ **Firefox** ซึ่งพัฒนาขึ้นมาโดย Mozilla Corporation กำลังได้รับความนิยมเป็นอย่างมาก เป็นซอฟต์แวร์ประเภทการติดต่อสื่อสารบนเครือข่ายคอมพิวเตอร์หรืออินเตอร์เน็ต (Web Browser)และมีระบบดูแลรักษาความปลอดภัยสูงมาก คล้ายกับ Internet Explorer (IE) ของ Microsoft โปรแกรม Firefox มีส่วนแบ่งทางการตลาด ซึ่งสำรวจเมื่อเดือนพฤศจิกายน พ.ศ.2550 ที่ผ่านมาปรากฏว่า มีส่วนแบ่งทางการตลาดประเภท Web Browsers ถึง 16.01% เป็นซอฟต์แวร์ที่ได้รับความนิยมมากที่สุดเป็นอันดับสองที่มีการใช้งานกันอยู่ทั่วโลกในปัจจุบัน เป็นซอฟต์แวร์ที่ได้มาตรฐานและเปิดเผยรหัสเขียนโปรแกรม (Open Source) สำหรับคุณสมบัติโดยรวมของโปรแกรม Firefox คือ (1). มีปุ่มสำหรับเลือกรายการบนคอมพิวเตอร์ (Tabbed Browsing), (2). เป็นผู้ตรวจสอบคำผิด (Spell Checker), (3). เพิ่มการค้นหาได้มากขึ้น (Incremental Find), (4). สามารถคั่นรายการที่ชื่นชอบไว้ได้ทันที (Live Bookmarking), (5). ทำหน้าที่ในการจัดการดาวน์โหลดแฟ้มข้อมูล (Download Manager), (6). มีระบบสืบค้นข้อมูลได้รวดเร็วทันใจรวมทั้งบน Google ด้วย นอกจากนี้ ในส่วนของหน้าที่การทำงานหรือ Function การทำงานต่างๆ นั้นองค์กรหรือบริษัทสามารถพัฒนา

เพิ่มขึ้นเองได้อีกมากกว่า 2,000 ชนิดการทำงาน และที่ได้รับความนิยมมากที่สุด คือ (1). Foxy Tunes (คือ ส่วนที่ช่วยควบคุมการเล่นเพลง), (2). Adblock Plus (คือ ส่วนที่ทำหน้ากันหรือบล็อกส่วนที่ไม่ต้องการได้), (3). StumbelUpon (คือ ส่วนที่ทำหน้าที่ในการทำให้สามารถค้นหาเว็บไซต์ได้อย่างรวดเร็ว), (4). Down ThemAll (คือ ส่วนที่ทำหน้าที่ในการดาวน์โหลดข้อมูล), และ (5). Web Developer (คือ ส่วนที่ใช้เป็นเครื่องมือในการพัฒนาเว็บไซต์) โปรแกรม Firefox สามารถทำงานได้บนระบบปฏิบัติการของ Microsoft Windows, Mac OS X, and Linux โปรแกรม Firefox ปัจจุบันเป็นเวอร์ชั่น 2.0.0.11, ซึ่งเวอร์ชั่นนี้ เพิ่งเปิดตัวเมื่อวันที่ 30 พฤศจิกายน พ.ศ.2550 ส่วนเงื่อนไขของรหัสโปรแกรมของ Firefox ส่วนใหญ่เปิดเผยและให้บริการฟรี ภายใต้เงื่อนไขของ Mozilla (http://en.wikipedia.org) ผู้ใดสนใจอยากได้โปรแกรม Firefox นี้สามารถหาดาวน์โหลดได้ฟรีไม่มีค่าใช้จ่าย หรือสามารถเข้าไปดาวน์โหลดได้ที่เว็บไซต์ http://bangkoktravel-bangkoksmile.blogspot.com ซึ่งมีซอฟต์แวร์ตรวจสอบทำลายไวรัสคอมพิวเตอร์ ซอฟต์แวร์ประยุกต์อื่นๆ อีกมากกว่า 3,5000 ชนิดให้ดาวน์โหลดได้ฟรี

ภาพที่ 3 ตัวอย่างเว็บไซต์ http://bangkoktravel-bangkoksmile.blogspot.com ซึ่งนอกเหนือจากเป็นเว็บไซต์ที่บริการเกี่ยวกับการจองห้องพักโรงแรม รีสอร์ท ตั๋วเครื่องบินแล้ว ยังมีบริการให้ดาวน์โหลดซอฟต์แวร์ฟรีด้วย

- **การเจาะระบบ** (Hacking)

การเจาะระบบในคอมพิวเตอร์คือการเข้าไปครอบงำการใช้เครื่องคอมพิวเตอร์ หรือ ผู้ที่ไม่มีสิทธิ์เข้าไปใช้ระบบเครือข่ายคอมพิวเตอร์ ผู้เจาะระบบ (Hackers) อาจจะเป็นผู้ที่อยู่นอกระบบ คือไม่ได้เป็นพนักงานของบริษัท แต่เข้ามาใช้อินเตอร์เน็ต หรือเครือข่ายคอมพิวเตอร์และทำให้ข้อมูล และโปรแกรมได้รับความเสียหาย เรื่องที่ควรทราบไว้อย่างหนึ่งก็คือ หากเราจะทำอะไร นักเจาะระบบจะเข้ามาติดตามและทำลายด้วยระบบอิเล็กทรอนิกส์ (Electronic Breaking and Entering) นั่นก็คือ เขาสามารถจะเข้าถึงระบบคอมพิวเตอร์ได้ และสามารถอ่านแฟ้มข้อมูล, หรือไม่ก็ทำให้ข้อมูลได้รับความเสียหายไม่อย่างใดก็อย่างหนึ่ง ด้วยสถานการณ์เป็นอย่างนี้ จึงจำเป็นต้องสร้างระบบความปลอดภัยขึ้นมาก่อน

ผู้เจาะระบบสามารถจะติดตามการใช้จดหมายอิเล็กทรอนิกส์, การเข้าถึงข้อมูลบนเว็บไซต์, หรือการถ่ายโอนแฟ้มข้อมูล, การเข้าไปล่วงรู้รหัสผ่าน หรือแฟ้มข้อมูลซึ่งอยู่ในระบบเครือข่าย ผู้เจาะระบบนั้น อาจจะเข้าไปใช้การควบคุมการบริการบนเครื่องคอมพิวเตอร์ โดยปกติแล้วระบบคอมพิวเตอร์ที่มีโปรแกรมทำงานอยู่นั้น จะอนุญาตให้เฉพาะผู้ที่สิทธิ์เท่านั้นสามารถเข้าไปทำงานได้ภายในระบบเครืออข่าย แต่ผู้เจาะระบบสามารถที่จะ

เข้าไปในระบบได้เท่าเทียมกับผู้มีสิทธิ์ใช้งาน อย่างเช่น เครื่องมือของเทลเน็ต (Telnet) และอินเตอร์เน็ต ที่ใช้ในการควบคุมการทำงานของคอมพิวเตอร์ จะช่วยให้ผู้เจาะระบบค้นพบสารสนเทศเพื่อวางแผนในการโจมตี ผู้เจาะระบบจะใช้เทลเน็ต ในการเข้าถึงช่องทางจดหมายอิเล็กทรอนิกส์ ตัวอย่าง เช่น จะสามารถติดตามการส่งข้อความทางจดหมายอิเล็กทรอนิกส์ หรือรหัสผ่าน ตลอดจนบัญชีสารสนเทศอื่นๆ ของผู้ใช้ รวมทั้งทรัพยากรสารสนเทศบางประเภทที่มีผู้ใช้งาน ดังนั้น ปัญหาหลักอย่างหนึ่งของอาชญากรรรมทางคอมพิวเตอร์ก็คือ ผู้เจาะระบบบนอินเตอร์เน็ต

ภาพที่ 4 แสดงถึงอาชญากรรมคอมพิวเตอร์ประเภทต่างๆ (Gary B. Shelly : 2007 : 557)

- **การขโมยทางอิเล็กทรอนิกส์** (Cyber Theft)

อาชญากรรมทางคอมพิวเตอร์หลายชนิดเกี่ยวข้องกับการขโมยเงิน (Theft of Money)สาเหตุเรื่องหลักใหญ่เกี่ยวกับการทำงานภายใน (Inside Jobs) ซึ่งเกี่ยวกับผู้ไม่มีสิทธิ์เข้าไปใช้ฐานข้อมูลในคอมพิวเตอร์ ควรมีการติดตามการทำงานของพนักงานอย่างใกล้ชิด แท้จริงแล้ว อาชญากรรรมทางคอมพิวเตอร์หลายชนิดเกี่ยวข้องกับการใช้อินเตอร์เน็ต ตัวอย่างเช่น การขโมยเงิน $11 ล้านดอลล่าร์สหรัฐ ของธนาคารซิตี้แบ็งค์ ในปี ค.ศ.1994 ผู้เจาะระบบชาวรัสเซียชื่อ Vladimir Levin และการกระทำของเขาได้รับความสำเร็จที่ St. Petersburg โดยการใช้อินเตอร์เน็ตทำลายระบบเครื่องเมนเฟรมอิเล็กทรอนิกส์ของธนาคารซิตี้แบ็งค์ในนครนิวยอร์ค เขาทำสำเร็จโดยการโอนเงินจากบัญชีทั่วไปเข้าบัญชีธนาคารของเขา ในประเทศอิสราเอล ฟินด์แลนด์ และแคลิฟฟอร์เนีย

- **การใช้เครื่องคอมพิวเตอร์ในที่ทำงานในทางที่ไม่ถูกต้อง** (Unauthorized Use at Work)

การใช้เครื่องคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ในที่ทำงานโดยมู่กต้องหรือไม่ได้รับอนุญาตจะถูกเรียกว่า **การขโมยเวลาและทรัพยากร** (Time and Resource Theft) ตัวอย่างหนึ่งที่เห็นกันอยู่บ่อยๆ คือ พนักงานของบริษัทใช้เครื่องคอมพิวเตอร์ของบริษัทเพื่อทำงานส่วนของตนเอง อัตราสูงจากคำให้การของที่ปรึกษาเกี่ยวกับเรื่องเหล่านี้ คือ การใช้เครื่องทำงานด้านการเงินส่วนบุคคล, การเล่นวีดิโอเกมส์, การเล่นอินเตอร์เน็ต เป็นต้น จากการใช้ซอฟท์แวร์ติดตามดักจับข้อมูลการทำงานของพนักงานที่เรียกว่า สนิฟเฟอร์ (Sniffers) มีทั้งการส่งจดหมายอิเล็กทรอนิกส์, การคัดลอกโปรแกรมโดยผิดกฎหมาย, การโพสข้อความกลุ่ม, การเข้ามาใช้งานโดยไม่ถูกต้อง,การซื้อสินค้า การส่งการ์ดอิเล็กทรอนิกส์, การเล่นเกมส์, การสนทนา,การประมูล, การแลกเปลี่ยน, หรือกิจกรรมส่วนตัวด้านอื่นๆ จากการสำรวจในสหรัฐอเมริกาพบว่า พนักงานกว่า 90 % ใช้เครื่องคอมพิวเตอร์ทำงานโดยไม่ถูกต้องในเวลาทำงาน, และพบว่า 84% ส่งอีเมล์ส่วนตัวในเวลาการทำงาน และจากการรายงานของบริษัทซีร็อกส์ (Xerox Corporation) ทำให้ทราบว่า พนักงานมากกว่า 40% ใช้เวลามากถึง 8 ชั่วโมงต่อวันเข้าไปดูเว็บไซต์เกี่ยวกับหนังและภาพลามก พนักงานบางคนมีการดาวน์โหลดภาพลามก, วีดิโอลามก,หรือมีการรับส่งผ่านจดหมายอิเล็กทรอนิกส์ มีกลุ่มของคนทำงานที่ติดตามการทำงานของพนักงานโดยใช้ซอฟท์แวร์เปิดดูการเคลื่อนไหวของเว็บไซต์ที่เรียกว่า Surf Watch (SWAT) พบว่ามีเว็บไซต์เกี่ยวกับเรื่องลามากนี้กว่า 40,000 เว็บไซต์ ที่มีพนักงานเข้าไปดู และโปรแกรมชนิดนี้สามารถที่จะบล็อกหรือปิดเว็บไซต์เหล่านี้ทำให้พนักงานภายในองค์ไม่สามารถเข้าไปใช้ได้

- **การคัดลอกซอฟท์แวร์โดยไม่ได้รับอนุญาต** (Software Piracy)

ซอฟท์แวร์หรือโปรแกรมคอมพิวเตอร์ที่ถูกเขียนขึ้นนั้นถือว่า เป็นทรัพย์สินทางปัญญา ดังนั้น เมื่อมีการคัดลอกซอฟท์แวร์โดยที่เจ้าของไม่ได้อนุญาต จึงเรียกว่า Software Piracy มีหลายกรณีที่เกิดขึ้น เช่น ซอฟท์แวร์ที่บริษัทได้เขียนขึ้น และถูกคัดลอกไปโดยพนักงานก็เป็นเรื่องที่ไม่ถูกต้องเช่นกัน ดังนั้น จึงมีการต่อต้านกันเป็นอย่างมาก โดยเฉพาะสมาคมผู้จัดทำซอฟท์แวร์, สมาคมผู้พัฒนาซอฟท์แวร์ใช้ในโรงงานอุตสาหกรรม จึงไม่อนุญาตให้คนอื่นมาทำการคัดลอกซอฟท์แวร์ของตน การคัดลอกซอฟท์แวร์เป็นการกระทำที่ผิดกฎหมายดังที่ทราบกันแล้ว เนื่องจากเป็นทรัพย์สินทางปัญญา ดังนั้น จึงมีการดำเนินการในเรื่องต่างๆ ขึ้นมา เช่น ความเห็นชอบในการคัดลอกซอฟท์แวร์ หรือที่เรียกกันว่า ***ข้อตกลงระหว่างผู้และผู้ขาย*** *(Site Licenses)* มีการกำหนดตกลงกันว่า ให้สามารถคัดลอกสำเนาได้กี่ชุด เพื่ออำนวยความสะดวกในการทำงานให้กับพนักงานของพวกเขา หรือมีอีกหลายแนวทาง คือ **การอนุญาตให้คัดลอกได้แต่มีลิขสิทธิ์** (Shareware) หมายถึง อาจคัดลอกไปเพื่อการศึกษาหรือเรียนรู้ได้ แต่ไม่อนุญาตให้คัดลอกไปเพื่อทำการค้า เป็นต้น ส่วนอีกชนิดหนึ่งคือ **การอนุญาตให้คัดลอกได้ โดยไม่สงวนลิขสิทธิ์** (Public Domain Software) ลักษณะนี้เป็นซอฟท์แวร์ที่โปรแกรมเมอร์มือสมัครเล่น เขียนโปรแกรมขึ้นมาและอยากทดสอบความรู้ของตนเอง จึงอนุญาตให้คนอื่นคัดลอกได้ เพื่อแบ่งปันความรู้กัน หรือต้องการคำแนะนำจากลูกค้า

- **การไม่อนุญาตให้คัดลอกทรัพย์สินทางปัญญา** (Piracy of Intellectual Property) ไม่ใช่แต่เพียงซอฟท์แวร์คอมพิวเตอร์เท่านั้นที่เป็นทรัพย์สินทางปัญญา ยังรวมไปถึงการคัดลอกสิ่งที่เป็นวัตถุประเภทอื่นๆ คือ เพลง, วีดิโอ, รูปภาพ, บทความ, หนังสือ หรือ การเขียนงานในลักษณะอื่นๆ อย่าง**กรณีของการพัฒนาเทคโนโลยีเครือข่ายคอมพิวเตอร์ที่เป็นได้ทั้งตัวรับและตัวส่งในเวลาเดียวกัน** (Peer-to-Peer : P2P) ขึ้นมาก็นับว่าเป็นทรัพย์สินทางปัญญาเช่นกัน ลักษณะการทำงานของ P2P ก็จะเป็นซอฟท์แวร์ที่สามารถใช้แฟ้มข้อมูลร่วมกัน หรือการที่สามารถถ่ายโอนแฟ้มข้อมูลเสียงเพลงจากเครื่องคอมพิวเตอร์ส่วนบุคคลไปยังเครื่องเล่นเอ็มพี3 (MP3) ได้โดยตรง ซึ่งผู้ใช้มีการใช้งานผ่านอินเตอร์เน็ต

- **ไวรัสคอมพิวเตอร์และหนอน** (Computer Viruses and Worms) จัดเป็นภัยอันตรายอยู่ในประเภทของอาชญากรรมทางคอมพิวเตอร์อย่างหนึ่ง ไวรัสคอมพิวเตอร์ เป็นการเขียนรหัสโปรแกรมขึ้นมา ไม่สามารถทำงานได้หากขาดการใส่โปรแกรมอื่นเข้าไป หรือเกิดขึ้นเมื่อการใช้คำสั่งคัดลอก เป็นต้น ส่วนตัวหนอน (Worm) เป็นรหัสที่เขียนขึ้นมาอย่างชัดเจน คือสามารถทำงานได้โดยไม่ต้องมีตัวช่วย แต่จะฝังตัวอยู่ในเครื่องคอมพิวเตอร์ และขยายแบ่งตัวเพิ่มจำนวนขึ้นเรื่อยๆ จนอาจทำให้แฟ้มข้อมูลในเครื่องคอมพิวเตอร์เสียหายได้ในที่สุด เหมือนกับตัวหนอนที่กัดกินภายในของผลไม้ ทั้งไวรัสคอมพิวเตอร์ และตัวหนอน เมื่อติดเชื้อแล้วจะขยายไปยังผู้ใช้เครื่องคอมพิวเตอร์รายอื่นๆ ต่อไปเรื่อยๆ เมื่อมีการคัดลอกโปรแกรม จึงมีผู้พัฒนาโปรแกรมตรวจสอบและทำลายไวรัสและตัวหนอน (Antivirus Programs) ซึ่งสามารถตรวจสอบและทำลายไวรัสที่ติดมากับแผ่น หรือในฮาร์ดดิสก์ได้ เช่น Office Scan, RT Kill, NOD32 เป็นต้น
- **การหลอกลวงทางจดหมายอิเล็กทรอนิกส์** (e-Mail Hoaxes) ข้อความที่ส่งมาทางจดหมายอิเล็กทรอนิกส์ มีทั้งเรื่องจริงและไม่จริง ลักษณะของ e-Mail Hoaxes เป็นลักษณะการกุข่าวขึ้นมา เช่น มีจดหมายฉบับหนึ่งส่งมาจากชายคนหนึ่งซึ่งอาศัยอยู่ในประเทศไนจีเรียบอกว่า เขาเป็นรัชทายาทของกษัตริย์ไนจีเรีย ประเทศของเขามีปัญหาทางการเมืองมาก คนในตระกูลของเขาถูกฆ่าตายเกือบหมดแล้ว เหลือเพียงเขาคนเดียว เขามีทรัพย์สินเงินทองมากมายหลายพันล้านดอลล่าร์สหรัฐ เขาขอร้องว่า ถ้าเราให้ความร่วมมือกับเขาคือให้เขาสามารถเดินทางเข้ามาอาศัยอยู่ในประเทศไทยได้ และให้บอกหมายเลขบัญชีธนาคารให้เขา เขาจะโอนเงินเข้าบัญชีให้ 35 % เป็นต้น นอกจากนี้ ยังมีการหลอกลวงในลักษณะอื่นอีกเช่น การทำงานผ่านอินเตอร์เน็ต (Work at Home), การสะสมแต้มคลิกเพื่อแลกเงินสด, การหลอกให้เป็นสมาชิกและช่วยประชาสัมพันธ์เว็บไซต์ให้กับตนเอง ที่กล่าวมานี้ บางคนอาจได้เงินจริงก็มี แต่จำนวนน้อยมาก เพราะต้องรู้กลวิธีเชิงลึก แต่คนที่เข้าใจเพียงผิวเผิน ทำการสะสมแต้มอยู่เป็นเดือนก็ยังไม่ได้เงิน เป็นต้น เว็บไซต์เหล่านี้ ส่วนใหญ่เป็นเว็บไซต์ของฝรั่ง แต่เว็บของไทยเองก็เริ่มมีมากขึ้นในระยะหลัง
- **การสอดแนมหรือจารบุรุษ** (Spyware) เป็นลักษณะของโปรแกรมที่หลอกล่อให้ผู้ใช้ซึ่งรู้เท่าไม่ถึงการณ์ เข้าไปดาวน์โหลดข้อมูลและติดตั้งมันลงบนเครื่องคอมพิวเตอร์ โดยผู้ใช้ที่ดาวน์โหลดข้อมูลเป็นเหมือนเข้าไปโดยไม่ได้รับอนุญาตจากผู้ที่เป็นเจ้าของ ในขณะเดียวกันโปรแกรมนี้จะทำงานโดยอัตโนมัติ มีการสอดแนมเข้าไปล่วงรู้ข้อมูลส่วนตัว เปลี่ยนแปลงการตั้งค่าของโปรแกรมเว็บเบราเซอร์ และการสืบค้นหาข้อมูลในระบบคอมพิวเตอร์ ลักษณะของ Spyware จะทำให้ประสิทธิภาพการทำงานของเครื่องคอมพิวเตอร์ทำงานได้ช้าลง และบางครั้งอาจก่อให้เกิดความรำคาญใจ ส่วนใหญ่เว็บเหล่านี้จะเห็นได้จากเว็บไซต์ลามก หรือเกมส์คอมพิวเตอร์ และอื่นๆ (สัญญา คล่องในวัย : 2547 : 60)
- **ข้อความไร้สาระหรือเมล์ขยะ** (Spam) เป็นลักษณะของจดหมายอิเล็กทรอนิกส์ที่ถูกสร้างขึ้นเพื่อต้องการให้ผู้อื่นช่วยโฆษณาและประชาสัมพันธ์สินค้า หรือเว็บไซต์ธุรกิจของตน ส่วนใหญ่จะมาจากผู้ใช้หลงไปกรอกข้อมูลรายละเอียดของตนเองลงไปเพื่อเป็นสมาชิก โดยความไม่รู้ หรือมีข้อเสนอในการแลกเปลี่ยนประชาสัมพันธ์เว็บไซต์ของกันและกัน ในที่สุดจะมีจดหมายอิเล็กทรอนิกส์ส่งมาเป็นจำนวนมหาศาล ซึ่งผู้ที่ส่งมาจะไม่สนใจใยดีต่อผู้รับว่า จะมีปฏิกิริยาโต้ตอบอย่างไร ส่งผลให้กล่องรับข้อความ (Mail Box) เต็มไปด้วยสแปมเป็นจำนวนหลายร้อยหลายพันฉบับต่อวัน ต้องมานั่ง ลบทิ้งข้อความจดหมายเหล่านั้นเป็นหลายๆ ชั่วโมงจึงจะหมด วิธีหลีกเลี่ยง Spam Mail คือ ต้องไปลบ หรือยกเลิกการเป็นสมาชิกในเว็บไซต์ที่เราเคยเข้าไปสมัครไว้ และอย่าพยายามให้ e-Mail Address ของเราไปปรากฏอยู่ในที่สาธารณะมากเกินไป เช่น ตามหน้าหนังสือพิมพ์ เพราะเดี๋ยวจะมีจดหมายจากคนที่เราไม่รู้จักส่งกลับมามากมาย ส่วนใหญ่เป็นโฆษณาสินค้า และเรื่องไร้สาระต่างๆ
- **การเลือกซื้อสินค้าออนไลน์** (Online Shopping) การเลือกซื้อสินค้าออนไลน์ หรือบนเว็บไซต์พาณิชย์

อิเล็กทรอนิกส์ (e-Commerce) สิ่งที่ต้องระวังมากที่สุด คือ อย่าหลงกลกรอกหมายเลขบัตรเครดิตของตนลงไปง่ายๆ เพราะบางเว็บไซต์เชื่อถือได้ และบางเว็บไซต์เชื่อถือไม่ได้ ต้องอ่านกฎระเบียบข้อตกลงในการซื้อสินค้าให้ดี โดยเฉพาะภาษาอังกฤษต้องดี ถ้าภาษาอังกฤษไม่ดี อาจทำให้เข้าใจความหมายคลาดเคลื่อนและจะเป็นอันตรายต่อตนเอง ตัวอย่างเว็บที่น่าเชื่อได้ เช่น www.amazon.com, www.ebay.com, www.walmart.com เป็นต้น

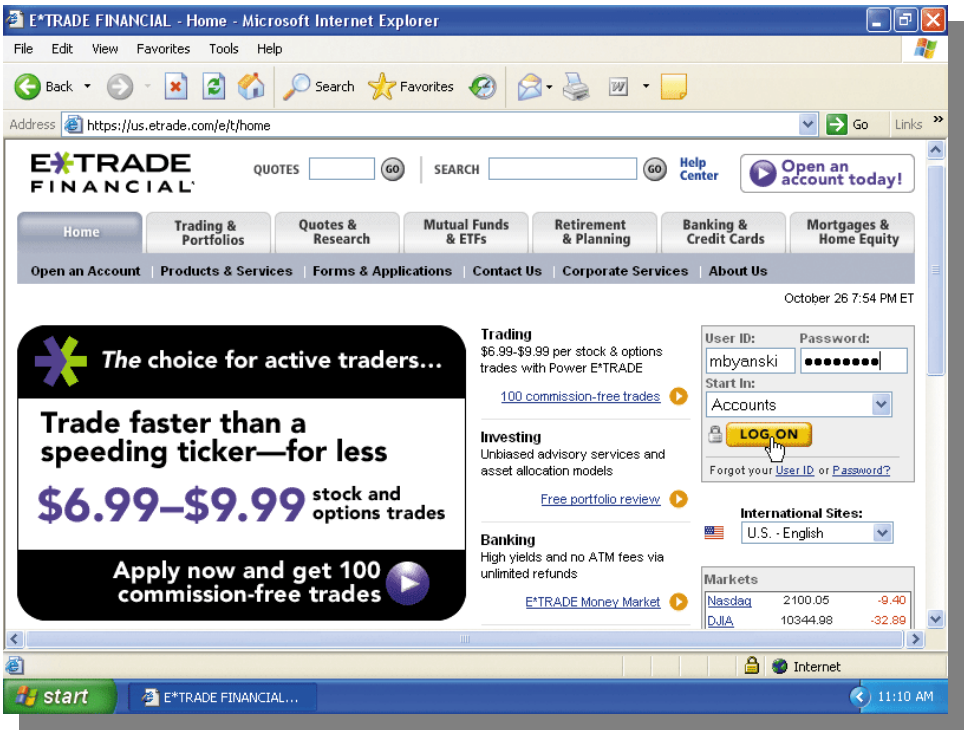
- **การรักษาความปลอดภัยของข้อมูล** (Data Security) ข้อมูลถือเป็นส่วนหนึ่งในสินทรัพย์ขององค์กรที่สำคัญที่สุดอย่างหนึ่ง จึงต้องมีการวางแผนสำหรับการรักษาความปลอดภัยของข้อมูล มีหลายเทคนิคในการป้องกันข้อมูล แต่ไม่มีเทคนิคใดร้อยเปอร์เซ็นว่าจะรักษาความปลอดภัยของข้อมูลได้ แต่มีอยู่หลายเทคนิคที่นิยมใช้กันมากได้แก่

(1). **การรักษาความปลอดภัยของขยะข้อมูล** (Secured Waste) ขยะข้อมูลได้แก่ เอกสารการพิมพ์ต่างๆ สำเนากระดาษคาร์บอน แถบผ้าหมึก และอะไรก็ตามที่สามารถเป็นแหล่งข้อมูลให้กับบุคคลที่ไม่ได้รับอนุญาต ดังนั้น ควรทำลายทิ้งอย่างถาวรโดยอาจใช้เครื่องทำลายเอกสาร

(2). **การควบคุมในระบบคอมพิวเตอร์** (Internal Controls) เป็นการควบคุมที่ถูกกำหนดให้เป็นส่วนหนึ่งของระบบคอมพิวเตอร์ เช่น การจัดทำ Transaction Log File ซึ่งเป็นแฟ้มข้อมูลที่ใช้เก็บรายละเอียดของผู้ที่เข้าถึงหรือพยายามเข้าไปทำการอย่างใดอย่างหนึ่งในแฟ้มข้อมูลแต่ละครั้ง

(3). **การตรวจสอบ** (Auditor Checks) เป็นการให้เจ้าหน้าที่ตรวจสอบ (Auditor) ตรวจสอบโปรแกรมและข้อมูลว่ามีการทำงานถูกต้องหรือไม่อย่างไร การตรวจสอบจะใช้การสุ่มตรวจสอบเป็นระยะโดยไม่บอกให้ผู้ปฏิบัติงานทราบ ผู้ตรวจสอบจะมีข้อมูลที่ใช้ตรวจสอบและตรวจจับข้อผิดพลาดของการทำงาน และอาจตรวจสอบการเข้าใช้ระบบนอกเวลาทำการด้วย ปัจจุบันสามารถใช้ซอฟต์แวร์สำเร็จรูปตรวจสอบความถูกต้องแม่นยำของการปฏิบัติการและการแสดงผลของระบบ

(4). **การตรวจสอบประวัติผู้สมัครงาน** (Applicant Screening) เป็นการตรวจสอบประวัติของผู้สมัครงาน เพื่อการคัดบุคคลที่อาจไม่ประสงค์ดีต่อองค์กรก่อนทำการว่าจ้าง



ภาพที่ 5 เว็บไซต์จำนวนมากใช้วิธีรักษาความปลอดภัยโดยมีการกำหนดการเข้าใช้ข้อมูลส่วนบุคคล และรหัสผ่าน (User Name and Password) (Gary B. Shelly : 2007 : 566)

(5). **การใช้รหัสผ่าน** (Password) ซึ่งเป็นข้อความและ/หรือตัวเลขที่เป็นความลับ ซึ่งต้องพิมพ์ด้วยคีย์บอร์ดเพื่อการเข้าใช้ระบบคอมพิวเตอร์ รหัสควรเป็นความลับ และต้องยากแก่การเดา อย่างไรก็ตามก็ยังมีการแตกรหัส (Cracking) ซึ่งเป็นวิธีการทั่วไปที่ใช้เข้าระบบอย่างผิดกฎหมาย

(6). **ตัวป้องกันในซอฟต์แวร์** (Built-in Software Protection) เป็นซอฟต์แวร์ที่ติดตั้งไว้ในระบบ หรือระบบปฏิบัติการ เพื่อเพิ่มความเข้มงวดในการเข้าใช้ระบบคอมพิวเตอร์ โดยอาจใช้วิธีการเปรียบเทียบเลขหรือรหัสประจำตัวของผู้ที่เข้าใช้ระบบกับเลขหรือรหัสที่กำหนดให้เข้าใช้ระบบได้ ถ้าบุคคลนั้นเข้าระบบไม่ได้ก็จะถูกบันทึกลงไปว่าบุคคลนั้นกำลังพยายามเข้าใช้ระบบที่บุคคลนั้นไม่ได้รับอนุญาตให้ใช้ ส่วนอีกวิธีหนึ่งคือการใช้ User Profile เป็นแฟ้มข้อมูลที่ใช้เก็บข้อมูลของผู้ใช้แต่ละคน รวมทั้งแฟ้มข้อมูลต่างๆ ได้รับอนุญาตให้เข้าไปได้ นอกจากนี้ยังรวมถึงหน้าที่การทำงาน ทักษะ ความรู้ความสามารถ สิทธิพิเศษในการเข้าใช้ระบบ เป็นต้น ในกรณีที่ระบบมีปัญหา ข้อมูลเหล่านี้จะถูกตรวจสอบโดยผู้บริหาร หรือผู้มีอำนาจในหน่วยงาน (สรรรัตน์ ห่อไพศาล : 2543 : 149)

ภัยยุคดิจิตอล หรืออาชญากรรมทางคอมพิวเตอร์ดังที่ได้กล่าวมาแล้วเบื้องต้น จะเห็นว่าเรื่องหลัก คือ การขโมยฮาร์ดแวร์ ซอฟต์แวร์ และสารสนเทศ การละเมิดทรัพย์สินทางปัญญา การคัดลอกซอฟต์แวร์โดยผิดกฎหมาย หรือการให้ร้ายป้ายสีด่าทอกรรโชกผู้อื่นให้ได้รับความเสียหาย ซึ่งเป็นอันตรายและก่อให้เกิดความเสียหายอย่างยิ่งสำหรับผู้ใช้คอมพิวเตอร์ไม่ว่าจะอยู่ที่บ้าน หรือที่ทำงาน หรือแม้กระทั่งการถูกรุกล้ำความเป็นส่วนตัว ปัจจุบันในประเทศไทยได้มีพระราชบัญญัติว่าด้วยการกระทำความผิด เกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ได้ประกาศใช้ออกมาอย่างเป็นทางการแล้ว ซึ่งนับว่าเป็นกฎหมายส่วนหนึ่งที่ช่วยป้องกันอาชญากรรมทางคอมพิวเตอร์ที่กำลังระบาดหนักขึ้นทุกวัน อย่างน้อยก็ช่วยปกป้อง คุ้มกันความปลอดภัยให้กับผู้ใช้คอมพิวเตอร์และอินเตอร์เน็ตในยุคดิจิตอลนี้เกิดความอุ่นใจได้ในระดับหนึ่ง โดยจะขอยกตัวอย่าง กฎหมายนี้ ซึ่งมีการประกาศใช้ในพระราชกิจจานุเบกษาเรียบร้อยแล้ว ลงวันที่ 18 มิถุนายน พ.ศ. 2550 และขอยกตัวอย่างกฎหมายที่ว่านี้มาให้ทราบเป็นบางข้อ คือ **มาตราที่** 5 ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ, **มาตราที่** 8 ผู้ใดกระทำด้วยประการใด โดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะ หรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ, **มาตราที่** 9 ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมด หรือบางส่วนซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ, **มาตราที่** 10 ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวน จนไม่สามารถทำงานตามปกติได้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ, **มาตราที่** 11 ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท เป็นต้น ซึ่งการที่กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ได้ออกกฎหมายเหล่านี้มา ถือได้

ว่าช่วยป้องปรามอาชญากรรมคอมพิวเตอร์ให้ลดลง หรืออย่างน้อยก็ทำให้ผู้คิดจะกระทำในสิ่งที่ไม่ถูกต้อง จะได้ลด ละ เลิก การกระทำ ในสิ่งที่ไม่สมควร ไม่ถูกต้องเหมาะสมในโอกาสต่อไป.

✪✪✪✪✪

บรรณานุกรม

ประสงค์ ปราณีตพลกรัง, ผศ. ดร., และคณะ, ***ระบบสารสนเทศเพื่อการจัดการ,*** กรุงเทพฯ : บริษัท ธีระฟิล์ม และไซเท็กซ์ จำกัด, 2541.

สรรรัชต์ ห่อไพศาล, ผศ.ดร., ***คอมพิวเตอร์และวิทยาการสารสนเทศเบื้องต้น,*** กรุงเทพฯ : มหาวิทยาลัยศรีปทุม, 2543.

สุพล พรหมมาพันธุ์, ผศ., ***ภัยจากอินเตอร์เน็ต***, หนังสือพิมพ์สยามธุรกิจ ราย 3 วัน, ฉบับที่ 790 วันที่ 5-8 พฤษภาคม พ.ศ.2550

College of Education, ***Desktop Video Conferencing,*** http://tiger.coe.missouri.edu~cjw/video/overview.htm, (February 10, 2004)

David M. Kroenke, ***Management Information Systems,*** Pearson International Edition, Pearson Prentice Hall TM, 2008.

Ephraim Schwartz, ***Social networking targets the enterprise,*** http://www.infoworld.com/article/03/12/15/49Nnsocial_1.html, (February, 2004)

Gary B. Shelly, ***Discovering Computers,*** Thomson Course Technology, 2005.

_____, ***Discovering Computers,*** Sripatum University Edition, Thomson Course Technology, 2008.

James A. O'Brien, ***Management Information Systems,*** Fourth Edition, McGraw-Hill, Inc., 1999.

_____, ***Management Information Systems,*** Eighth Edition, McGraw-Hill, Inc., 2008.

Timothy J. O'Leary, *Computing Essential*, McGraw-Hill International Edition, 2007.

http://en.wikipedia.org

✪✪✪✪✪