อาชญากรรมคอมพิวเตอร์ ปัญหาร้ายของสังคม

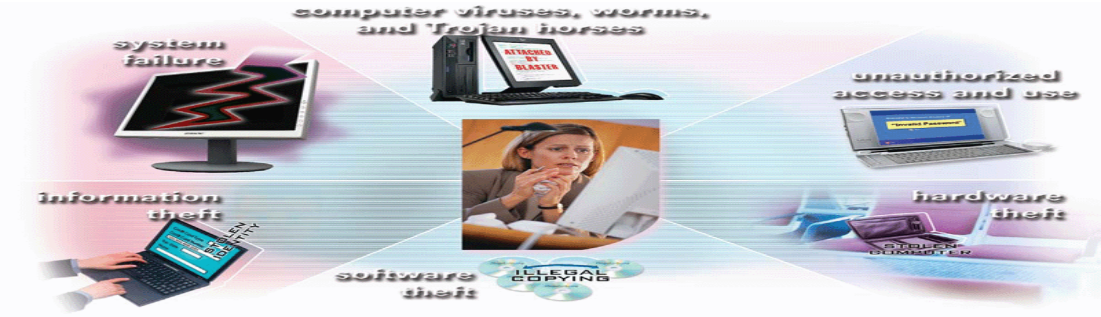
ผศ.สุพล พรหมมาพันธุ์
คณะสารสนเทศศาสตร์ มหาวิทยาลัยศรีปทุม

ลงตีพิมพ์ในหนังสือพิมพ์ไทยโพสต์ ฉบับวันพฤหัสบดีที่ 2 เมษายน พ.ศ. 2552 หน้า 4

ภัยอันฉกาจฉกรรจ์ประเภทหนึ่ง ซึ่งอยู่ใกล้ชิดคนที่ทำงานและใช้อินเตอร์เน็ตเป็นประจำ คือ **ภัยจากอาชญากรรมคอมพิวเตอร์** (Computer Crime) ซึ่งได้สร้างความรู้สึกหงุดหงิดรำคาญ และสร้างความเสียหายต่อเศรษฐกิจและธุรกิจอย่างมหาศาล ไม่ว่าจะเป็นการรับ-ส่งจดหมายอิเล็กทรอนิกส์, การสนทนา, การประชุม, การสืบค้นข้อมูลบนเว็บไซต์, การทำธุรกิจ หรือแม้กระทั่งการสอนหนังสือในมหาวิทยาลัย เป็นต้น ย่อมมีโอกาสประสบกับภัยดังกล่าวนี้ไม่มากก็น้อย ดังพอประมวลให้เห็นเป็นบางประเด็นต่อไปนี้ คือ

- **การขโมยฮาร์ดแวร์** (Hardware Theft) คือ การขโมยอุปกรณ์คอมพิวเตอร์ หรือทำการเปลี่ยนถ่ายอุปกรณ์คอมพิวเตอร์ ลักษณะการขโมย เช่น ตัดสายเคเบิ้ล เพื่อทำลายธุรกิจ หรือ การทำลายเครื่องคอมพิวเตอร์ในโรงเรียน หรือในมหาวิทยาลัยให้แตกหักเป็นเสี่ยงๆ เพื่อไม่ให้สามารถใช้งานได้ เพราะสถานที่เหล่านี้มีเครื่องคอมพิวเตอร์เป็นจำนวนมาก จึงอาจตกเป็นเป้าหมายในการทำลายมากกว่าที่บ้าน ส่วนคอมพิวเตอร์มือถือ และโน้ตบุ๊กคอมพิวเตอร์ มีโอกาสเสี่ยงต่อการถูกขโมยมาก เนื่องจากมีขนาดเล็ก น้ำหนักเบา คาดกันว่าในแต่ละปี มีโน้ตบุ๊กคอมพิวเตอร์ถูกขโมยมากว่า 600,000 เครื่อง เป้าหมายส่วนใหญ่เป็นโน้ตบุ๊กของผู้บริหารของบริษัท เพราะมีข้อมูลความลับต่างๆ ของบริษัทเป็นจำนวนมาก
- **การขโมยซอฟต์แวร์** (Software Theft) ได้แก่ (1). การขโมยสื่ออุปกรณ์ของซอฟต์แวร์ เช่น การขโมยแผ่น CD-ROM, DVD ของเอ็นไซค์โคลพีเดีย (Encyclopedia) ในห้องสมุด เป็นต้น , (2). การตั้งใจลบโปรแกรม เกี่ยวข้องกับโปรแกรมเมอร์ของบริษัทบางคน ไม่มีความซื่อสัตย์ต่อองค์กร ทำการลบชุดคำสั่งของโปรแกรมที่ตนเองเขียนเอาไว้ทิ้ง, (3). การคัดลอกโปรแกรม โดยผิดกฎหมาย ในกรณีนี้ เกิดจาการขโมยซอฟต์แวร์ออกมาจากโรงงานผลิต และนำไปทำการคัดลอกเพื่อทำการค้าหรือธุรกิจ
- **การขโมยสารสนเทศ** (Information Theft) ส่วนใหญ่เป็นการขโมยสารสนเทศซึ่งเป็นความลับของบุคคล หรือการทำให้สารสนเทศเกิดความเสียหายใช้งานไม่ได้ ซึ่งเกิดขึ้นได้ทั้งกับบริษัท และที่บ้าน ผู้บริหารบางคนไม่มีความซื่อสัตย์สุจริต หรือขาดจริยธรรมในการดำเนินธุรกิจ อาจมีการว่าจ้างให้บุคคลอื่นขโมย หรือจัดซื้อสารสนเทศที่ถูกขโมยมาเพื่อเป็นประโยชน์ และได้เปรียบทางการแข่งขัน และประเด็นสำคัญที่สุด คือ ต้องการรู้ความลับ และกลยุทธ์วิธีการดำเนินธุรกิจของคู่แข่งขัน ตลอดจนถึง การแอบขโมยข้อมูลหมายเลขบัตรเครดิตของลูกค้า ในขณะที่ลูกค้าเข้ามาซื้อสินค้า หรือประเภทหนึ่งคือ การส่งสารสนเทศไปบนเครือข่ายคอมพิวเตอร์นั้น อาจมีผู้ไม่หวังดีทำการดักจับการส่งข้อมูลหรือสารสนเทศ ทำให้สามารถล่วงรู้ความลับต่างๆ ที่ถูกส่งผ่านไปบนเครือข่ายคอมพิวเตอร์ได้
- **การเจาะระบบ** (Hacking) คือการเข้าไปครอบงำการใช้ หรือ ผู้ที่ไม่มีสิทธิ์เข้าไปใช้ระบบเครือข่ายคอมพิวเตอร์ ผู้เจาะระบบ (Hackers) อาจจะเป็นผู้ที่อยู่นอกระบบ คือไม่ได้เป็นพนักงานของบริษัท แต่เข้ามาใช้อินเตอร์เน็ต หรือเครือข่ายคอมพิวเตอร์และทำให้ข้อมูล และโปรแกรมได้รับความเสียหาย เขาจะเข้ามาติดตามและทำลายด้วยระบบอิเล็กทรอนิกส์ โดยจะเข้าถึงระบบคอมพิวเตอร์ได้ และสามารถอ่านแฟ้มข้อมูล, หรือไม่ก็ทำให้ข้อมูลได้รับความเสียหายไม่อย่างใดก็อย่างหนึ่ง ผู้เจาะระบบสามารถจะติดตามการใช้จดหมายอิเล็กทรอนิกส์, การเข้าถึงข้อมูลบนเว็บไซต์, หรือการถ่ายโอนแฟ้มข้อมูล, การเข้าไปล่วงรู้รหัสผ่าน หรือ

แฟ้มข้อมูลซึ่งอยู่ในระบบเครือข่าย ผู้เจาะระบบนั้น อาจจะเข้าไปใช้การควบคุมการบริการบนเครื่องคอมพิวเตอร์ โดยปกติแล้วระบบคอมพิวเตอร์จะอนุญาตให้เฉพาะผู้ที่สิทธิ์เท่านั้นสามารถเข้าไปทำงานในระบบเครือข่ายได้ แต่ผู้เจาะระบบสามารถที่จะเข้าไปในระบบได้เท่าเทียมกับผู้มีสิทธิ์ใช้งาน อย่างเช่น เครื่องมือของเทลเน็ต (Telnet) และอินเตอร์เน็ต ที่ใช้ในการควบคุมการทำงานของคอมพิวเตอร์ จะช่วยให้ผู้เจาะระบบค้นพบสารสนเทศเพื่อวางแผนในการโจมตี ผู้เจาะระบบจะใช้เทลเน็ต ในการเข้าถึงช่องทางจดหมายอิเล็กทรอนิกส์ ตัวอย่าง เช่น จะสามารถติดตามการส่งข้อความทางจดหมายอิเล็กทรอนิกส์ หรือรหัสผ่าน ตลอดจนบัญชีสารสนเทศอื่นๆ ของผู้ใช้ รวมทั้งทรัพยากรสารสนเทศบางประเภทที่มีผู้ใช้งาน (Gary B. Shelly : 2007 : 557)



- **การขโมยทางอิเล็กทรอนิกส์** (Cyber Theft) ส่วนใหญ่มักเป็นการขโมยเงิน (Theft of Money)สาเหตุใหญ่ เกี่ยวกับการทำงานภายในองค์กร (Inside Jobs) โดยผู้ไม่มีสิทธิ์เข้าไปใช้ฐานข้อมูลในคอมพิวเตอร์ ตัวอย่างเช่น การขโมยเงิน $11 ล้านดอลล่าร์สหรัฐ ของธนาคารซิตี้แบ็งค์ ในปี ค.ศ.1994 ผู้เจาะระบบชาวรัสเซียชื่อ Vladimir Levin และเขาทำได้สำเร็จอย่างมากที่ St. Petersburg โดยการใช้อินเตอร์เน็ตทำลายระบบเครื่องเมนเฟรมอิเล็กทรอนิกส์ของธนาคารซิตี้แบ็งค์ในนครนิวยอร์ค โดยการโอนเงินจากบัญชีทั่วไปเข้าบัญชีธนาคารของเขา ในประเทศอิสราเอล ฟินด์แลนด์ และแคลิฟฟอร์เนีย
- **การคัดลอกซอฟต์แวร์โดยไม่ได้รับอนุญาต** (Software Piracy) เช่น ซอฟต์แวร์ที่บริษัทได้เขียนขึ้น และถูกคัดลอกไปโดยพนักงานก็เป็นเรื่องที่ไม่ถูกต้องเช่นกัน ดังนั้น จึงมีการต่อต้านกันเป็นอย่างมาก โดยเฉพาะสมาคมผู้จัดทำซอฟต์แวร์, สมาคมผู้พัฒนาซอฟต์แวร์ใช้ในโรงงานอุตสาหกรรม จึงไม่อนุญาตให้คนอื่นมาทำการคัดลอกซอฟต์แวร์ของตน การกระทำดังกล่าวผิดกฎหมาย เพราะซอฟต์แวร์เป็นทรัพย์สินทางปัญญา และทรัพย์สินทางปัญญานี้ ไม่ใช่มีแต่เพียงซอฟต์แวร์คอมพิวเตอร์เท่านั้น ยังรวมไปถึงประเภท เพลง, วีดิโอ, รูปภาพ, บทความ, หนังสือ เป็นต้น
- **ไวรัสคอมพิวเตอร์และหนอน** (Computer Viruses and Worms) ไวรัสคอมพิวเตอร์ เป็นการเขียนรหัสโปรแกรมขึ้นมา ไม่สามารถทำงานได้หากขาดการใส่โปรแกรมอื่นเข้าไป หรือเกิดขึ้นเมื่อการใช้คำสั่งคัดลอก เป็นต้น ส่วนตัวหนอน (Worm) เป็นรหัสที่เขียนขึ้นมาอย่างชัดเจน คือสามารถทำงานได้โดยไม่ต้องมีตัวช่วย แต่จะฝังตัวอยู่ในเครื่องคอมพิวเตอร์ และขยายแบ่งตัวเพิ่มจำนวนขึ้นเรื่อยๆ จนอาจทำให้แฟ้มข้อมูลในเครื่องคอมพิวเตอร์เสียหายได้ในที่สุด เหมือนกับตัวหนอนที่กัดกินภายในของผลไม้ ทั้งไวรัสคอมพิวเตอร์ และตัวหนอน ต่อมาจึงมีผู้พัฒนาโปรแกรมตรวจสอบและทำลายไวรัสและตัวหนอน (Antivirus Programs) ซึ่งสามารถตรวจสอบและทำลายไวรัสที่ติดมากับแผ่นหรือในฮาร์ดดิสก์ได้ เช่น Office Scan, RT Kill, Trend Micro, NOD32 เป็นต้น
- **การหลอกลวงทางจดหมายอิเล็กทรอนิกส์** (e-Mail Hoaxes) ข้อความที่ส่งมาทางจดหมายอิเล็กทรอนิกส์ มีทั้งเรื่องจริงและไม่จริง ลักษณะของ e-Mail Hoaxes เป็นลักษณะการกุข่าวขึ้นมา เช่น คุณถูกรางวัลได้เงิน $ 1 ล้านดอลล่าร์ หรือมีจดหมายฉบับหนึ่งส่งมาจากชายคนหนึ่งซึ่งอาศัยอยู่ในประเทศไนจีเรียบอกว่า เขาเป็นรัชทายาทของกษัตริย์ไนจีเรีย ประเทศของเขามีปัญหาทางการเมืองมาก คนในตระกูลของเขาถูกฆ่าตายเกือบหมดแล้ว เหลือเพียงเขาคนเดียว เขามี

ทรัพย์สินเงินทองมากมายหลายพันล้านดอลล่าร์สหรัฐ เขาขอร้องว่า ถ้าเราให้ความร่วมมือกับเขาคือให้เขาสามารถเดินทางเข้ามาอาศัยอยู่ในประเทศไทยได้ และให้บอกหมายเลขบัญชีธนาคารให้เขา เขาจะโอนเงินเข้าบัญชีให้ 35 % เป็นต้น

- **การสอดแนมหรือจารบุรุษ** (Spyware) เป็นลักษณะของโปรแกรมที่หลอกล่อให้ผู้ใช้ที่รู้เท่าไม่ถึงการณ์ เข้าไปดาวน์โหลดข้อมูลและติดตั้งมันลงบนเครื่องคอมพิวเตอร์ โดยผู้ใช้ที่ดาวน์โหลดข้อมูลเป็นเหมือนเข้าไปโดยไม่ได้รับอนุญาตจากผู้ที่เป็นเจ้าของ ในขณะเดียวกันโปรแกรมนี้จะทำงานโดยอัตโนมัติ มีการสอดแนมเข้าไปล่วงรู้ข้อมูลส่วนตัว เปลี่ยนแปลงการตั้งค่าของโปรแกรมเว็บบราวเซอร์ และการสืบค้นหาข้อมูลในระบบคอมพิวเตอร์ ลักษณะของ Spyware จะทำให้ประสิทธิภาพการทำงานของเครื่องคอมพิวเตอร์ทำงานได้ช้าลง และบางครั้งอาจก่อให้เกิดความหงุดหงิดรำคาญใจ ส่วนใหญ่เว็บเหล่านี้จะเห็นได้จากเว็บไซต์ลามก หรือเกมคอมพิวเตอร์ต่างๆ
- **ข้อความไร้สาระหรือเมล์ขยะ** (Spam) เป็นลักษณะของจดหมายอิเล็กทรอนิกส์ที่ถูกสร้างขึ้นเพื่อต้องการให้ผู้อื่นช่วยโฆษณาและประชาสัมพันธ์สินค้า หรือเว็บไซต์ธุรกิจของตน ส่วนใหญ่จะมาจากผู้ใช้หลงไปกรอกข้อมูลรายละเอียดของตนเองลงไปเพื่อเป็นสมาชิก โดยความไม่รู้ หรือมีข้อเสนอในการแลกเปลี่ยนประชาสัมพันธ์เว็บไซต์ของกันและกัน ในที่สุดจะมีจดหมายอิเล็กทรอนิกส์ส่งมาเป็นจำนวนมหาศาล ซึ่งผู้ที่ส่งมาจะไม่สนใจใยดีต่อผู้รับว่า จะมีปฏิกิริยาโต้ตอบอย่างไร ส่งผลให้กล่องรับข้อความ (Mail Box) เต็มไปด้วยสแปมเป็นจำนวนหลายร้อยหลายพันฉบับต่อวัน วิธีหลีกเลี่ยง Spam Mail คือ ต้องไปลบ หรือยกเลิกการเป็นสมาชิกในเว็บไซต์ที่เราเคยเข้าไปสมัครไว้ และอย่าพยายามให้ e-Mail Address ของเราไปปรากฏอยู่ในที่สาธารณะมากเกินไป

อาชญากรรรมคอมพิวเตอร์เหล่านี้ เป็นปัญหาร้ายของสังคม ซึ่งเป็นบ่อนทำลายระบบเศรษฐกิจของประเทศ และบั่นทอนสุขภาพจิตใจของสุจริตชน ถึงแม้คนส่วนใหญ่จะเข้าใจว่า “**โลกนี้ย่อมมีทั้งผู้สร้าง และผู้ทำลาย หรือฝ่ายธรรม กับฝ่ายอธรรม** ” ก็ตามแต่ถ้าเลือกได้ขออย่าให้มีผู้ทำลาย โลกคงสงบสุขร่มเย็นกว่านี้เป็นแน่ทีเดียว.

✪✪✪✪✪