Digital Harm

ตอนจบ

ผศ.สุพล พรหมมาพันธุ์

ภาควิชาคอมพิวเตอร์ธุรกิจ คณะสารสนเทศศาสตร์ มหาวิทยาลัยศรีปทุม

(ลงตีพิมพ์ในวารสาร ส่งเสริมเทคโนโลยี ฉบับที่198 เดือนเมษายน - พฤษภาคม พ.ศ. 2551 หน้า 90)

- **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 จึงมีการต่อต้านกันเป็น

อย่างมาก 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) ลักษณะนี้
เป็นซอฟท์แวร์ที่โปรแกรมเมอร์มือสมัครเล่น 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 เข้าไป

ดาวน์โหลดข้อมูลและติดตั้งมันลงบนเครื่องคอมพิวเตอร์ โดยผู้ใช้ที่ดาวน์โหลดข้อมูลเป็นเหมือนเข้าไปโดยไม่ได้รับอนุญาตจากผู้ที่เป็นเจ้าของ ในขณะเดียวกันโปรแกรมนี้จะทำงานโดยอัตโนมัติ มีการสอดแนมเข้าไปล่วงรู้ข้อมูลส่วนตัว เปลี่ยนแปลงการตั้งค่าของโปรแกรมเว็บเบราเซอร์ และการสืบค้นหาข้อมูลในระบบคอมพิวเตอร์ ลักษณะของ Spyware จะทำให้ประสิทธิภาพการทำงานของเครื่องคอมพิวเตอร์ทำงานได้ช้าลง และบางครั้งอาจก่อให้เกิดความรำคาญใจ ส่วนใหญ่เว็บเหล่านี้จะเห็นได้จากเว็บไซต์ลามก หรือเกมส์คอมพิวเตอร์ และอื่นๆ (สัญญา คล่องในวัย : 2547 : 60)

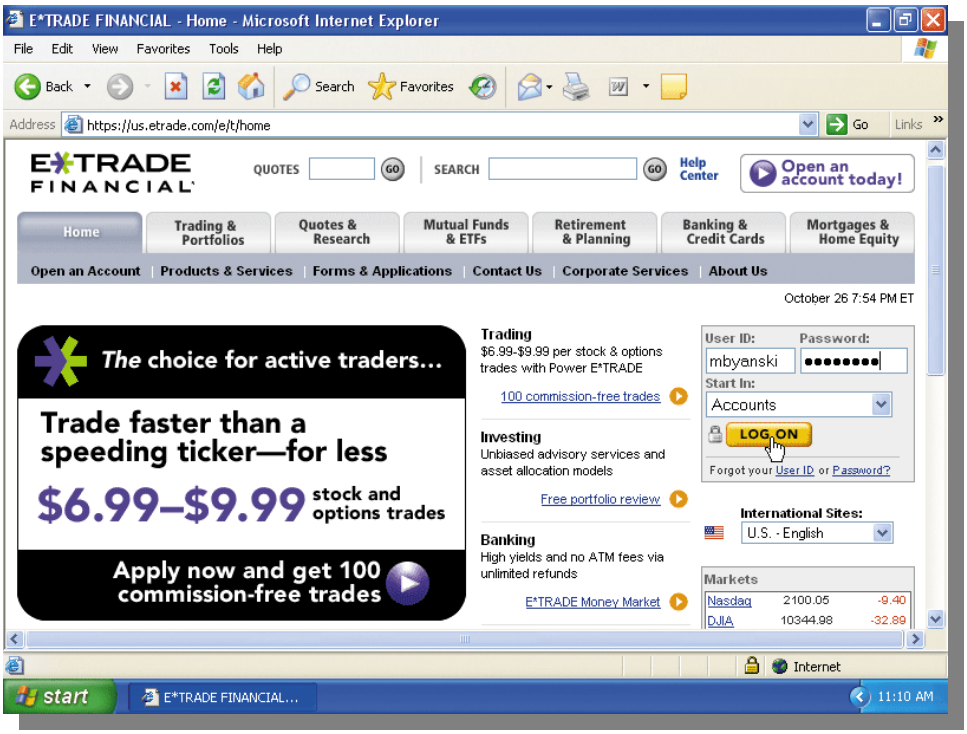
- **ข้อความไร้สาระหรือเมล์ขยะ** (Spam) เป็นลักษณะของจดหมายอิเล็กทรอนิกส์ที่ถูกสร้างขึ้นเพื่อต้องการให้ผู้อื่นช่วยโฆษณาและประชาสัมพันธ์สินค้า หรือเว็บไซต์ธุรกิจของตน ส่วนใหญ่จะมาจากผู้ใช้หลงไปกรอกข้อมูลรายละเอียดของตนเองลงไปเพื่อเป็นสมาชิก โดยความไม่รู้ หรือมีข้อเสนอในการแลกเปลี่ยนประชาสัมพันธ์เว็บไซต์ของกันและกัน 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 หรือบนเว็บไซต์พาณิชย์อิเล็กทรอนิกส์ (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 ถือได้ว่าช่วยป้องปรามอาชญากรรมคอมพิวเตอร์ให้ลดลง 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