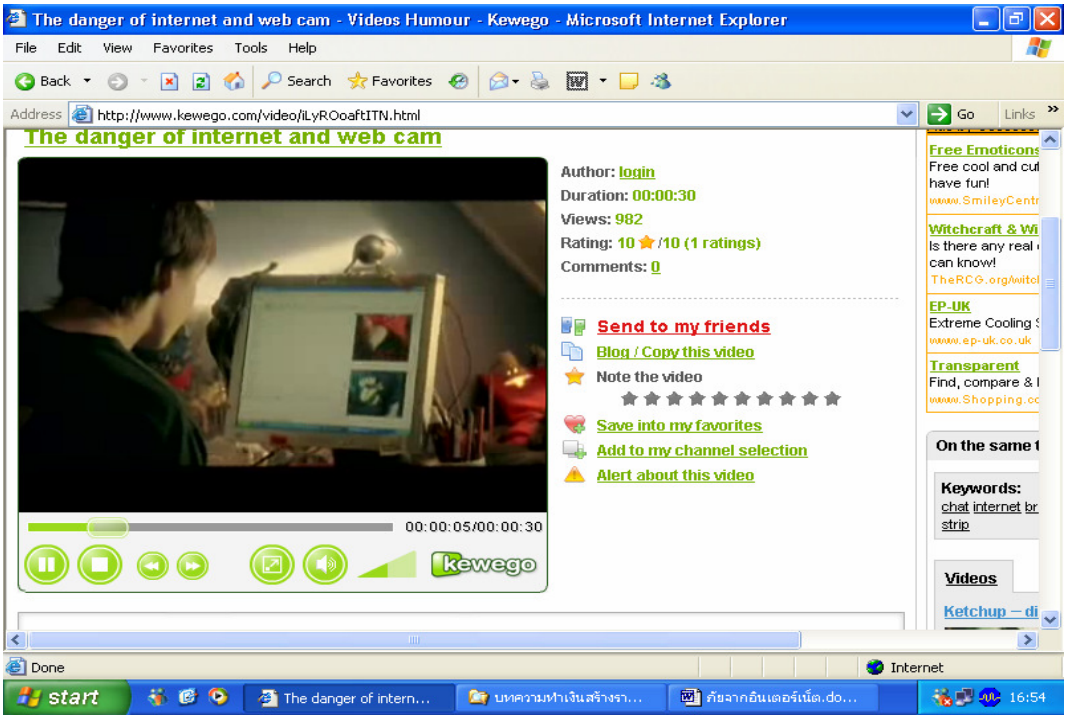
ภัยจากอินเตอร์เน็ต

ผศ.สุพล พรหมมาพันธุ์
คณะสารสนเทศศาสตร์ มหาวิทยาลัยศรีปทุม

(ลงตีพิมพ์ในหนังสือพิมพ์สยามธุรกิจ ราย 3 วัน ฉบับที่ 790 วันที่ 5-8 พฤษภาคม พ.ศ.2550 หน้า 8)

ยุคปัจจุบัน อินเตอร์เน็ตเข้ามามีบทบาทในชีวิตประจำวันมากขึ้น คนใช้เวลาส่วนใหญ่อยู่กับเครื่องคอมพิวเตอร์และอินเตอร์เน็ต เนื่องจากได้รับความสะดวกรวดเร็วสามารถติดต่อสื่อสารกับคนได้ทั่วโลก เพียงใช้นิ้วมือคลิกที่ปุ่มเมาส์ไม่กี่อึดใจเท่านั้น ในสหรัฐอมริกาเองมีรายงานว่า เด็กใช้เวลาส่วนใหญ่อยู่กับอินเตอร์เน็ตมากกว่าทีวีเสียอีก ในประเทศไทยคงไม่ต่างอะไรกันมากนัก เด็กส่วนใหญ่ใช้อินเตอร์เน็ตในการสนทนา เล่นเกมส์ ส่งข้อความ ค้นคว้าหาความรู้ และด้านบันเทิง อินเตอร์เน็ตจึงเปรียบเสมือนเป็นดาบสองคม คือ มีทั้งคุณและโทษ สำหรับโทษหรือหรือภัยจากอินเตอร์เน็ตพอประมวลได้ดังต่อไปนี้ คือ

- **การสนทนาและส่งข้อความเร่งด่วนบนอินเตอร์เน็ต** (Internet Chat & Instant messages) ในปัจจุบันการสนทนาสามารถมองเห็นหน้าคู่สนทนาได้โดยผ่านกล้องวิดีโอ (Video Camera) เรียกกันว่า Web Cam เมื่อสนทนากันแล้วอาจมีการพูดคุยชักชวนให้เกิดอาการคล้อยตามเช่น มีการเปลื้องผ้า เต้นระบำ หรืออาจมีการนัดพบเจอกัน ซึ่งเป็นคนที่เพิ่งรู้จักกัน ไม่ทราบนิสัยใจคอว่า เป็นคนอย่างไร อาจเป็นภัยนำไปสู่ปัญหาอาชญากรรม เช่น การฆ่าข่มขืน การหลอกลวงต้มตุ๋น เป็นต้น โปรแกรมที่นิยมใช้กันอย่างแพร่หลาย เช่น Microsoft Messenger, Yahoo Messenger สำหรับปัญหาใหญ่บนอินเตอร์เน็ตในปัจจุบันที่เกิดขึ้นกับเด็กและเยาวชน หลายฝ่ายต่างสรุปว่า ส่วนใหญ่เป็นปัญหาเกี่ยวกับเรื่องเซ็กส์ เนื่องจากบางครั้งเด็กอยู่คนเดียวทำให้เกิดความเปลี่ยวเหงา ซึ่งต้องอาศัยอินเตอร์เน็ตเป็นช่องให้คลายเหงาเรื่องนี้ ผู้ปกครองควรใส่ใจกับบุตรหลานของตนอย่างใกล้ชิด ทั้งนี้ รวมไปถึงเกมส์คอมพิวเตอร์ออนไลน์ด้วย ซึ่งเคยมีเด็กชาวเกาหลี และจีน เสียชีวิตคาหน้าจอคอมพิวเตอร์มาแล้ว เพราะเล่นเกมส์จนไม่ยอมกินข้าว และไม่ยอมหลับนอน



ภาพแสดงเว็บไซต์ที่เด็กชายและเด็กหญิงสนทนากันผ่าน Web Cam (www.kewego.com)

- **การเจาะระบบ (Hacking)** หมายถึงการเข้าไปครอบงำการใช้เครื่องคอมพิวเตอร์ หรือ ผู้ที่ไม่มีสิทธิ์เข้าไปใช้ระบบเครือข่ายคอมพิวเตอร์ ผู้เจาะระบบ (Hackers) อาจจะเป็นผู้ที่อยู่นอกระบบ คือไม่ได้เป็นพนักงานของบริษัท แต่เข้ามาใช้อินเตอร์เน็ต หรือเครือข่ายคอมพิวเตอร์และทำให้ข้อมูล และโปรแกรมได้รับความเสียหาย เรื่องที่ควรทราบไว้อย่างหนึ่งก็คือ หากเราจะทำอะไร นักเจาะระบบจะเข้ามาติดตามและทำลายด้วยระบบอิเล็กทรอนิกส์ (Electronic Breaking and Entering) นั่นคือ เขาสามารถจะเข้าถึงระบบคอมพิวเตอร์ได้ และสามารถอ่านแฟ้มข้อมูล, หรือไม่ก็ทำให้ข้อมูลได้รับความเสียหายไม่อย่างใดก็อย่างหนึ่ง ด้วยสถานการณ์เป็นอย่างนี้ จึงจำเป็นต้องสร้างระบบความปลอดภัยขึ้นมาก่อนผู้เจาะระบบสามารถจะติดตามการใช้จดหมายอิเล็กทรอนิกส์, การเข้าถึงข้อมูลบนเว็บไซต์, หรือการถ่ายโอนแฟ้มข้อมูล, การเข้าไปล่วงรู้รหัสผ่าน หรือแฟ้มข้อมูลซึ่งอยู่ในระบบเครือข่าย โดยปกติแล้วระบบคอมพิวเตอร์ที่มีโปรแกรมทำงานอยู่นั้น จะอนุญาตให้เฉพาะผู้ที่สิทธิ์เท่านั้นสามารถเข้าไปทำงานได้ แต่ผู้เจาะระบบสามารถที่จะเข้าไปในระบบได้เท่าเทียมกับผู้มีสิทธิ์ใช้งาน อย่างเช่น เครื่องมือของเทลเน็ต (Telnet) และอินเตอร์เน็ต ที่ใช้ในการควบคุมการทำงานของคอมพิวเตอร์ จะช่วยให้ผู้เจาะระบบค้นพบสารสนเทศเพื่อวางแผนในการโจมตี ผู้เจาะระบบจะใช้เทลเน็ต ในการเข้าถึงช่องทางจดหมายอิเล็กทรอนิกส์ ตัวอย่าง เช่น จะสามารถติดตามการส่งข้อความทางจดหมายอิเล็กทรอนิกส์ หรือรหัสผ่าน ตลอดจนบัญชีสารสนเทศอื่นๆ ของผู้ใช้ รวมทั้งทรัพยากรสารสนเทศบางประเภทที่มีผู้ใช้งาน

- **การขโมยทางอิเล็กทรอนิกส์ (Cyber Theft)** ส่วนใหญ่มักเกี่ยวข้องกับการขโมยเงิน (Theft of Money) สาเหตุเรื่องหลักเกี่ยวกับการทำงานภายใน (Inside Jobs) ซึ่งเกี่ยวกับผู้ไม่มีสิทธิ์เข้าไปใช้ฐานข้อมูลในคอมพิวเตอร์ ควรมีการติดตามการทำงานของพนักงานอย่างใกล้ชิด แท้จริงแล้ว ตัวอย่างการขโมยทางอิเล็กทรอนิกส์เช่น การขโมยเงิน $11 ล้านดอลล่าร์สหรัฐ ของธนาคารซิตี้แบ็งค์ ในปี ค.ศ.1994 ผู้เจาะระบบชาวรัสเซียชื่อ Vladimir Levin และการกระทำของเขาได้รับความสำเร็จที่ St. Petersburg โดยการใช้อินเตอร์เน็ตทำลายระบบเครื่องเมนเฟรมอิเล็กทรอนิกส์ของธนาคารซิตี้แบ็งค์ในนครนิวยอร์ค เขาทำการสำเร็จโดยการโอนเงินจากบัญชีทั่วไปเข้าบัญชีธนาคารของเขา ในประเทศอิสราเอล ฟินด์แลนด์ และแคลิฟฟอร์เนีย (James A. O'Brien, 2006 : 442)

- **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, การหลอกให้เป็น

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

ดังนั้น เมื่อทราบถึงภัยจากอินเตอร์เน็ตเหล่านี้แล้ว ควรต้องระมัดระวังการใช้คอมพิวเตอร์และอินเตอร์เน็ตให้มากขึ้นกว่าเดิม อย่าหลงกลผู้มีเจตนาร้ายทั้งหลาย เพราะคนเหล่านี้เขาจะมองว่า “**คนอื่นเป็นเสมือนปลาที่เขาจะใช้เหยื่อหลอกล่อให้มาติดเบ็ดของเขาเมื่อไหร่ก็ได้**” หากคนเหล่านั้นรู้เท่าไม่ถึงการณ์.

✪✪✪✪✪