“การบำรุงรักษาคอมพิวเตอร์เบื้องต้น,การสืบค้นข้อมูล และการใช้งาน Social Network”

สารบัญ

หน้า

บำรุงรักษาคอมพิวเตอร์เบื้องต้น

ลักษณะของคอมพิวเตอร์

คอมพิวเตอร์ คืออุปกรณ์อิเล็กทรอนิกส์ที่ทำงานตามชุดคำสั่งอย่างอัตโนมัติ โดยจะทำการคำนวณเปรียบเทียบทางตรรกกับข้อมูล และให้ผลลัพธ์ออกมาตามต้องการโดยมนุษย์ไม่ต้องเข้าไปเกี่ยวข้องในการประมวลผล

คุณสมบัติของคอมพิวเตอร์

ปัจจุบันนี้คนส่วนใหญ่นิยมนำคอมพิวเตอร์มาใช้งานต่าง ๆ มากมายซึ่งผู้ใช้ส่วนใหญ่มักจะคิดว่าคอมพิวเตอร์เป็นเครื่องมือที่สามารถทำงานได้สารพัดแต่ผู้ที่มีความรู้ทางคอมพิวเตอร์จะทราบว่างานที่เหมาะกับการนำคอมพิวเตอร์มาใช้อย่างยิ่งคือการสร้างสารสนเทศซึ่งสารสนเทศเหล่านั้นสามารถนำมาพิมพ์ออกทางเครื่องพิมพ์ส่งผ่านเครือข่ายคอมพิวเตอร์หรือจัดเก็บไว้ใช้ในอนาคตก็ได้เนื่องจากคอมพิวเตอร์จะมีคุณสมบัติต่าง ๆ คือ

ความเป็นอัตโนมัติ (Self Acting)การทำงานของคอมพิวเตอร์จะทำงานแบบอัตโนมัติภายใต้คำสั่งที่ได้ถูกกำหนดไว้ ทำงานดังกล่าวจะเริ่มตั้งแต่การนำข้อมูลเข้าสู่ระบบ การประมวลผลและแปลงผลลัพธ์ออกมาให้อยู่ในรูปแบบที่มนุษย์เข้าใจได้

ความเร็ว (Speed)คอมพิวเตอร์ในปัจจุบันนี้สามารถทำงานได้ถึงร้อยล้านคำสั่งในหนึ่งวินาที

ความเชื่อถือ (Reliable)คอมพิวเตอร์ทุกวันนี้จะทำงานได้ทั้งกลางวันและกลางคืนอย่างไม่มีข้อผิดพลาดและไม่รู้จักเหน็ดเหนื่อย

ความถูกต้องแม่นยำ (Accurate)วงจรคอมพิวเตอร์นั้นจะให้ผลของการคำนวณที่ถูกต้องเสมอหากผลของการคำนวณผิดจากที่ควรจะเป็นมักเกิดจากความผิดพลาดของโปรแกรมหรือข้อมูลที่เข้าสู่โปรแกรม

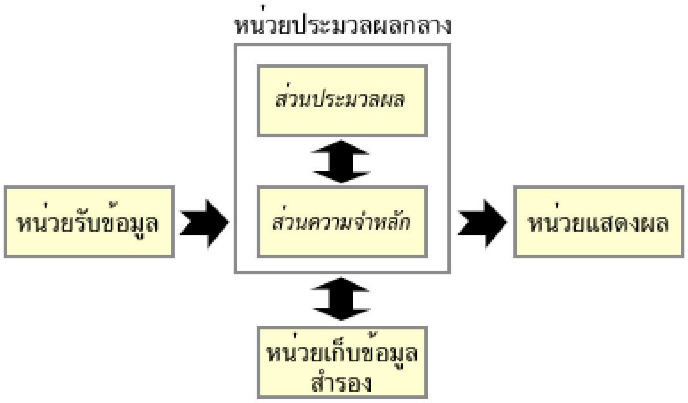
เก็บข้อมูลจำนวนมากๆ ได้ (Store massive amounts of information)ไมโครคอมพิวเตอร์ในปัจจุบันจะมีที่เก็บข้อมูลสำรองที่มีความสูงมากกว่าหนึ่งพันล้านตัวอักษรและสำหรับระบบคอมพิวเตอร์ขนาดใหญ่จะสามารถเก็บข้อมูลได้มากกว่าหนึ่งล้าน ๆ ตัวอักษร

ย้ายข้อมูลจากที่หนึ่งไปยังอีกทีหนึ่งได้อย่างรวดเร็ว (Move information)โดยใช้การติดต่อสื่อสารผ่านระบบเครือข่ายคอมพิวเตอร์ซึ่งสามารถส่งพจนานุกรมหนึ่งเล่มในรูปของข้อมูลอิเล็กทรอนิกส์ไปยังเครื่องคอมพิวเตอร์ที่อยู่ไกลคนซีกโลกได้ในเวลาเพียงไม่ถึงหนึ่งวินาทีทำให้มีการเรียกเครือข่ายคอมพิวเตอร์ที่เชื่อมกันทั่วโลกในปัจจุบันว่าทางด่วนสารสนเทศ (Information Superhighway)

ทำงานซ้ำๆได้ (Repeatability)ช่วยลดปัญหาเรื่องความอ่อนล้าจากการทำงานของแรงงานคน นอกจากนี้ยังลดความผิดพลาดต่างๆได้ดีกว่าด้วย ข้อมูลที่ประมวลผลแม้จะยุ่งยากหรือซับซ้อนเพียงใดก็ตาม จะสามารถคำนวณและหาผลลัพธ์ได้อย่างรวดเร็ว

ส่วนประกอบของคอมพิวเตอร์

จำแนกหน้าที่ของฮาร์ดแวร์ต่างๆ สามารถแบ่งเป็นส่วนสำคัญ 4 ประเภทคือ อุปกรณ์นำข้อมูลเข้า (Input Device) อุปกรณ์ประมวลผล(Processing Device) หน่วยเก็บข้อมูลสำรอง(Secondary Storage Device) อุปกรณ์แสดงผล (Output Device)



รูปที่ 1 แสดงวงจรการทำงานของคอมพิวเตอร์

อุปกรณ์นำข้อมูลเข้า (Input Device)

รูปที่ 2 อุปกรณ์นำเข้าแบบต่างๆ ที่พ

เป็นอุปกรณ์ที่เกี่ยวข้องก์ ประมวลผลต่อไปได้ ซึ่งอาจจะเป็น ตัวเลข ตัวอักษร ภาพนิง ภาพเคลือนไหว เสียง เป็นต้น

อุปกรณ์ประมวลผล (Processing Device)

อุปกรณ์ประมวลผลหลักๆ มีดังนี้

ซีพียู (CPU-Central Processing Unit)หน่วยประมวลผลกลางหรือซีพียู เรียกอีกชื่อหนึ่งว่า

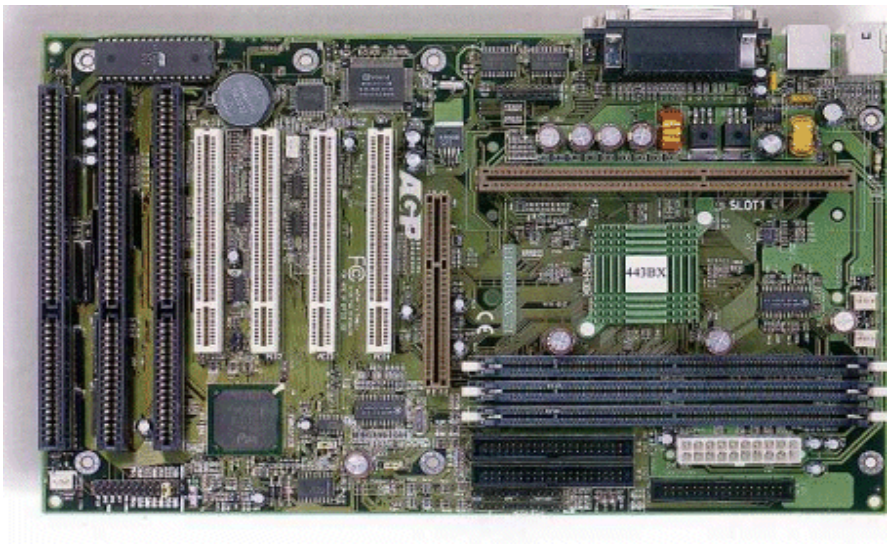
โปรเซสเซอร์ (Processor) หรือ ชิป (Chip) นับเป็นอุปกรณ์ที่มีความสำคัญมากที่สุดของฮาร์ดแวร์เพราะมีหน้าที่ในการประมวลผลข้อมูลที่ผู้ใช้ป้อนเข้ามาทางอุปกรณ์นำเข้าข้อมูลตามชุดคำสั่งหรือโปรแกรมที่ผู้ใช้ต้องการใช้งาน หน่วยประมวลผลกลาง

หน่วยความจำหลัก (Main Memory)หรือเรียกว่า หน่วยความจำภายใน (Internal Memory) สามารถแบ่งออกเป็น 2 ประเภท ได้แก่

- รอม (Read Only Memory - ROM) เป็นหน่วยความจำที่มีโปรแกรมหรือข้อมูลอยู่แล้ว สามารถเรียกออกมาใช้งานได้แต่จะไม่สามารถเขียนเพิ่มเติมได้และแม้ว่าจะไม่มีกระแสไฟฟ้าไปเลี้ยงให้แก่ระบบข้อมูลก็ไม่สูญหายไป

- แรม (Random Access Memory)เป็นหน่วยความจำที่สามารถเก็บข้อมูลได้เมื่อมีกระแสไฟฟ้าหล่อเลี้ยงเท่านั้นเมื่อใดไม่มีกระแสไฟฟ้ามาเลี้ยงข้อมูลที่อยู่ในหน่วยความจำชนิดนี้จะหายไปทันที

เมนบอร์ด (Main board) เป็นแผงวงจรต่อเชื่อมอุปกรณ์ที่เกี่ยวข้องกับการทำงานของคอมพิวเตอร์ทั้งหมด ถือได้ว่าเป็นหัวใจหลักของ พีซีทุกเครื่อง เพราะจะบอกความสามารถของเครื่องว่าจะใช้ซีพียูอะไรได้บ้าง มีประสิทธิภาพเพียงใด สามารถรองรับกับอุปกรณ์ใหม่ได้หรือไม่



ชิปเซ็ต (Chip Set)ชิปเซ็ตเป็นชิปจำนวนหนึ่งหรือหลายตัวที่บรรจุวงจรสำคัญๆ ที่ช่วยการทำงานของซีพียู และติดตั้งตายตัวบนเมนบอร์ดถอดเปลี่ยนไม่ได้ ทำหน้าที่เป็นตัวกลางประสานงานและควบคุมการทำงานของหน่วยความจำรวมถึงอุปกรณ์ต่อพ่วงต่างทั้งแบบภายในหรือภายนอกทุกชนิดตามคำสั่งของซีพียู เช่น SiS, Intel, VIA, AMD เป็นต้น

หน่วยเก็บข้อมูลสำรอง (Secondary Storage Device)

เนื่องจากหน่วยความจำหลักมีพื้นที่ไม่เพียงพอในการเก็บข้อมูลจำนวนมากๆ อีกทั้งข้อมูลจะหายไปเมื่อปิดเครื่อง ดังนั้นจำเป็นต้องหาอุปกรณ์เก็บข้อมูลที่มีขนาดใหญ่ขึ้น เช่น

ฮาร์ดดิสก์ (Hard Disk)เป็นฮาร์ดแวร์ที่ทำหน้าที่เก็บข้อมูลในเครื่องคอมพิวเตอร์ทั้งโปรแกรมใช้งานต่างๆ ไฟล์เอกสารรวมทั้งเป็นที่เก็บระบบปฏิบัติการที่เป็นโปรแกรมควบคุมการทำงานของเครื่องคอมพิวเตอร์ด้วย

ฟล็อบปี้ดิสก์ (Floppy Disk)เป็นอุปกรณ์บันทึกข้อมูลที่มีขนาด 3.5 นิ้วมีลักษณะเป็นแผ่นกลมบางทำจากไมลาร์ (Mylar) สามารถบรรจุข้อมูลได้เพียง 1.44 เมกะไบต์ เท่านั้น

ซีดี (Compact Disk - CD)เป็นอุปกรณ์บันทึกข้อมูลแบบดิจิทัล เป็นสื่อที่มีขนาดความจุสูงเหมาะสำหรับบันทึกข้อมูลแบบมัลติมีเดียซีดีรอมทำมาจากแผ่นพลาสติกกลมบางที่เคลือบด้วยสารโพลีคาร์บอเนต (Poly Carbonate) ทำให้ผิวหน้าเป็นมันสะท้อนแสง โดยมีการบันทึกข้อมูลเป็นสายเดียว (Single Track) มีขนาดเส้นผ่าศูนย์กลางประมาณ 120 มิลลิเมตร ปัจจุบันมีซีดีอยู่หลายประเภท ได้แก่ซีดีเพลง (Audio CD) วีซีดี (Video CD - VCD) ซีดี- อาร์ (CD Recordable - CD-R) ซีดี-อาร์ดับบลิว (CD-Rewritable - CD-RW) และ ดีวีดี (Digital Video Disk - DVD)

สื่อเก็บข้อมูลอื่นๆ

1)รีมูฟเอเบิลไดร์ฟ (Removable Drive)เป็นอุปกรณ์เก็บข้อมูลที่ไม่ต้องมีตัวขับเคลื่อน (Drive) สามารถพกพาไปไหนได้โดยต่อเข้ากับเครื่องคอมพิวเตอร์ด้วย Port USB ปัจจุบันความจุของรีมูฟเอเบิลไดร์ฟมีตั้งแต่ 8 , 16 , 32 , 64 , 128 จนถึง 1024 เมกะไบต์ ทั้งนี้ยังมีไดร์ฟลักษณะเดียวกัน เรียกในชื่ออื่นๆ ได้แก่ Pen Drive , Thump Drive , Flash Drive

2) ซิบไดร์ฟ (Zip Drive)เป็นสื่อบันทึกข้อมูลที่จะมาแทนแผ่นฟล็อปปี้ดิสก์มีขนาดความจุ 100 เมกะไบต์ ซึ่งการใช้งานซิปไดร์ฟจะต้องใช้งานกับซิปดิสก์ (Zip Disk) ความสามารถในการเก็บข้อมูลของซิปดิสก์จะเก็บข้อมูลได้มากกว่าฟล็อปปี้ดิสก์

3)Magnetic optical Disk Driveเป็นสื่อเก็บข้อมูลขนาด 3.5 นิ้วซึ่งมีขนาดพอๆ กับฟล็อบปี้ดิสก์ แต่ขนาดความจุมากกว่า เพราะว่า MO Disk drive 1 แผ่นสามารถบันทึกข้อมูลได้ตั้งแต่ 128 เมกะไบต์ จนถึงระดับ 5.2 กิกะไบต์

4)เทปแบ็คอัพ (Tape Backup)เป็นอุปกรณ์สำหรับการสำรองข้อมูลซึ่งเหมาะกับการสำรองข้อมูลขนาดใหญ่มากๆ ขนาดระดับ 10-100 กิกะไบต์

5)การ์ดเมมโมรี (Memory Card)เป็นอุปกรณ์บันทึกข้อมูลที่มีขนาดเล็กพัฒนาขึ้น เพื่อนำไปใช้กับอุปกรณ์เทคโนโลยีแบบต่างๆ เช่น กล้องดิจิทัลคอมพิวเตอร์มือถือ (Personal Data Assistant - PDA) โทรศัพท์มือถือ

อุปกรณ์แสดงผล (Output Device)

คืออุปกรณ์สำหรับแสดงผลลัพธ์ที่ได้จากการประมวลผลของคอมพิวเตอร์ และเป็นอุปกรณ์ส่งออก (Output device) ทำหน้าที่แสดงผลลัพธ์เมื่อซีพียูทำการประมวลผล

รูปที่ 4 แสดงอุปกรณ์แสดงผลข้อมูลแบบต่างๆ

จอภาพ (Monitor)เป็นอุปกรณ์แสดงผลลัพธ์ที่เป็นภาพ ปัจจุบันแบ่งออกเป็น 2 ชนิดคือ จอภาพแบบ CRT (Cathode Ray Tube) และ จอภาพแบบ LCD (Liquid Crystal Display)

เครื่องพิมพ์ (Printer)เป็นอุปกรณ์ที่ทำหน้าที่แสดงผลลัพธ์ในรูปของอักขระหรือรูปภาพที่จะไปปรากฏอยู่บนกระดาษแบ่งออกเป็น 4 ประเภท ได้แก่ เครื่องพิมพ์ดอตเมตริกซ์(Dot Matrix Printer) เครื่องพิมพ์แบบพ่นหมึก (Ink-Jet Printer) เครื่องพิมพ์แบบเลเซอร์ (Laser Printer) และพล็อตสเตอร์(Plotter)

ลำโพง (Speaker)เป็นอุปกรณ์แสดงผลลัพธ์ที่อยู่ในรูปของเสียงสามารถเชื่อมต่อกับคอมพิวเตอร์ผ่านแผงวงจรเกี่ยวกับเสียง (Sound card) ซึ่งมีหน้าที่แปลงข้อมูลดิจิตอลไปเป็นเสียง

ประโยชน์ของคอมพิวเตอร์

จากการที่คอมพิวเตอร์มีลักษณะเด่นหลายประการทำให้ถูกนำมาใช้ประโยชน์ต่อการดำเนินชีวิตประจำวันในสังคมเป็นอย่างมาก ที่พบเห็นได้บ่อยที่สุดก็คือ การใช้ในการพิมพ์เอกสารต่างๆ เช่น พิมพ์จดหมาย รายงานเอกสารต่างๆ ซึ่งเรียกว่างานประมวลผล (Wordprocessing)นอกจากนี้ยังมีการประยุกต์ใช้คอมพิวเตอร์ในด้านต่างๆ อีกหลายด้านดังต่อไปนี้

งานธุรกิจเช่น บริษัท ร้านค้า ห้างสรรพสินค้าตลอดจนโรงงานต่างๆ ใช้คอมพิวเตอร์ในการทำบัญชี งานประมวลคำและติดต่อกับหน่วยงานภายนอกผ่านระบบโทรคมนาคม นอกจากนี้งานอุตสาหกรรมส่วนใหญ่ก็ใช้คอมพิวเตอร์มาช่วยในการควบคุมการผลิตและการประกอบชิ้นส่วนของอุปกรณ์ต่างๆ เช่น โรงงานประกอบรถยนต์ซึ่งทำให้การผลิตมีคุณภาพดีขึ้นบริษัทยังสามารถรับ หรืองานธนาคารที่ให้บริการถอนเงินผ่านตู้ฝากถอนเงินอัตโนมัติ (ATM)และใช้คอมพิวเตอร์คิดดอกเบี้ยให้กับผู้ฝากเงิน และการโอนเงินระหว่างบัญชีเชื่อมโยงกันเป็นระบบเครือข่าย

งานวิทยาศาสตร์ การแพทย์ และงานสาธารณสุขสามารถนำคอมพิวเตอร์มาใช้ในนำมาใช้ในส่วนของการคำนวณที่ค่อนข้างซับซ้อน เช่นงานศึกษาโมเลกุลสารเคมี วิถีการโคจรของการส่งจรวดไปสู่อวกาศ หรืองานทะเบียนการเงิน สถิติ และเป็นอุปกรณ์สำหรับการตรวจรักษาโรคได้ซึ่งจะให้ผลที่แม่นยำกว่าการตรวจด้วยวิธีเคมีแบบเดิม และให้การรักษาได้รวดเร็วขึ้น

งานคมนาคมและสื่อสารในส่วนที่เกี่ยวกับการเดินทางจะใช้คอมพิวเตอร์ในการจองวันเวลา ที่นั่งซึ่งมีการเชื่อมโยงไปยังทุกสถานีหรือทุกสายการบินได้ทำให้สะดวกต่อผู้เดินทางที่ไม่ต้องเสียเวลารอ อีกทั้งยังใช้ในการควบคุมระบบการจราจรเช่น ไฟสัญญาณจราจร และ การจราจรทางอากาศหรือในการสื่อสารก็ใช้ควบคุมวงโคจรของดาวเทียมเพื่อให้อยู่ในวงโคจรซึ่งจะช่วยส่งผลต่อการส่งสัญญาณให้ระบบการสื่อสารมีความชัดเจน

งานวิศวกรรมและสถาปัตยกรรมสถาปนิกและวิศวกรสามารถใช้คอมพิวเตอร์ในการออกแบบ หรือ จำลองสภาวการณ์ ต่างๆ เช่นการรับแรงสั่นสะเทือนของอาคารเมื่อเกิดแผ่นดินไหวโดยคอมพิวเตอร์จะคำนวณและแสดงภาพสถานการณ์ใกล้เคียงความจริงรวมทั้งการใช้ควบคุมและติดตามความก้าวหน้าของโครงการต่างๆ เช่น คนงาน เครื่องมือผลการทำงาน

งานราชการเป็นหน่วยงานที่มีการใช้คอมพิวเตอร์มากที่สุด โดยมีการใช้หลายรูปแบบทั้งนี้ขึ้นอยู่กับบทบาทและหน้าที่ของหน่วยงานนั้นๆ เช่น กระทรวงศึกษาธิการมีการใช้ระบบประชุมทางไกลผ่านคอมพิวเตอร์ , กระทรวงวิทยาศาสตร์และเทคโนโลยีได้จัดระบบเครือข่ายอินเทอร์เน็ตเพื่อเชื่อมโยงไปยังสถาบันต่างๆ,กรมสรรพากรใช้จัดในการจัดเก็บภาษีบันทึกการเสียภาษี เป็นต้น

การศึกษาได้แก่การใช้คอมพิวเตอร์ทางด้านการเรียนการสอนซึ่งมีการนำคอมพิวเตอร์มาช่วยการสอนในลักษณะบทเรียน CAI หรืองานด้านทะเบียนซึ่งทำให้สะดวกต่อการค้นหาข้อมูลนักเรียนการเก็บข้อมูลยืมและการส่งคืนหนังสือห้องสมุด

องค์ประกอบของคอมพิวเตอร์

เครื่องคอมพิวเตอร์ที่เราเห็นๆกันอยู่นี้เป็นเพียงองค์ประกอบส่วนหนึ่งของระบบคอมพิวเตอร์เท่านั้นแต่ถ้าต้องการให้เครื่องคอมพิวเตอร์แต่ละเครื่องสามารถทำงานได้อย่างมีประสิทธิภาพตามที่เราต้องการนั้นจำเป็นต้องอาศัยองค์ประกอบพื้นฐาน 4 ประการมาทำงานร่วมกันซึ่งองค์ประกอบพื้นฐานของระบบคอมพิวเตอร์ประกอบไปด้วยฮาร์ดแวร์ (Hardware) ซอฟต์แวร์(Software) บุคลากร (People ware) ข้อมูล / สารสนเทศ (Data/Information)

ฮาร์ดแวร์ (Hardware)

หมายถึง อุปกรณ์ต่างๆ ที่ประกอบขึ้นเป็นเครื่องคอมพิวเตอร์มีลักษณะเป็นโครงร่างสามารถมองเห็นด้วยตาและสัมผัสได้ (รูปธรรม) เช่น จอภาพคีย์บอร์ด เครื่องพิมพ์ เมาส์ เป็นต้น ซึ่งสามารถแบ่งออกเป็นส่วนต่างๆตามลักษณะการทำงาน ได้ 4 หน่วย คือ หน่วยรับข้อมูล (Input Unit) หน่วยประมวลผลกลาง (Central Processing Unit: CPU) หน่วยแสดงผล (Output Unit) หน่วยเก็บข้อมูลสำรอง (Secondary Storage) โดยอุปกรณ์แต่ละหน่วยมีหน้าที่การทำงานแตกต่างกัน

ซอฟต์แวร์ (Software)

หมายถึง ส่วนที่มนุษย์สัมผัสไม่ได้โดยตรง (นามธรรม) เป็นโปรแกรมหรือชุดคำสั่งที่ถูกเขียนขึ้นเพื่อสั่งให้เครื่องคอมพิวเตอร์ทำงานซอฟต์แวร์จึงเป็นเหมือนตัวเชื่อมระหว่างผู้ใช้เครื่องคอมพิวเตอร์และเครื่องคอมพิวเตอร์ถ้าไม่มีซอฟต์แวร์เราก็ไม่สามารถใช้เครื่องคอมพิวเตอร์ทำอะไรได้เลยซอฟต์แวร์สำหรับเครื่องคอมพิวเตอร์สามารถแบ่งได้ ดังนี้

ซอฟต์แวร์สำหรับระบบ (System Software)คือ ชุดของคำสั่งที่เขียนไว้เป็นคำสั่งสำเร็จรูปซึ่งจะทำงานใกล้ชิดกับคอมพิวเตอร์มากที่สุดเพื่อคอยควบคุมการทำงานของฮาร์ดแวร์ทุกอย่างและอำนวยความสะดวกให้กับผู้ใช้ในการใช้งานซอฟต์แวร์หรือโปรแกรมระบบที่รู้จักกันดีก็คือ DOS, Windows, UNIX, Linux รวมทั้งโปรแกรมแปลคำสั่งที่เขียนในภาษาระดับสูง เช่น ภาษา Basic, FORTRAN, Pascal, COBOL, C เป็นต้น นอกจากนี้โปรแกรมที่ใช้ในการตรวจสอบระบบ เช่น Norton’s Utilities ก็นับเป็นโปรแกรมสำหรับระบบด้วยเช่นกัน

ซอฟต์แวร์ประยุกต์ (Application Software) คือ ซอฟต์แวร์หรือโปรแกรมที่สั่งคอมพิวเตอร์ทำงานต่างๆ ตามที่ผู้ใช้ต้องการไม่ว่าจะด้านเอกสาร บัญชี การจัดเก็บข้อมูล เป็นต้นซอฟต์แวร์ประยุกต์สามารถจำแนกได้เป็น 2 ประเภท คือ

- ซอฟต์แวร์สำหรับงานเฉพาะด้าน คือโปรแกรมซึ่งเขียนขึ้นเพื่อการทำงานเฉพาะอย่างที่เราต้องการ บางที่เรียกว่า User’s Program เช่น โปรแกรมการทำบัญชีจ่ายเงินเดือน โปรแกรมระบบเช่าซื้อโปรแกรมการทำสินค้าคงคลัง เป็นต้น ซึ่งแต่ละโปรแกรมก็มักจะมีเงื่อนไขหรือแบบฟอร์มแตกต่างกันออกไปตามความต้องการ หรือกฎเกณฑ์ของแต่ละหน่วยงานที่ใช้ซึ่งสามารถดัดแปลงแก้ไขเพิ่มเติม (Modifications) ในบางส่วนของโปรแกรมได้เพื่อให้ตรงกับความต้องการของผู้ใช้และซอฟต์แวร์ประยุกต์ที่เขียนขึ้นนี้โดยส่วนใหญ่มักใช้ภาษาระดับสูงเป็นตัวพัฒนา

- ซอฟต์แวร์สำหรับงานทั่วไป เป็นโปรแกรมประยุกต์ที่มีผู้จัดทำไว้เพื่อใช้ในการทำงานประเภทต่างๆ ทั่วไป โดยผู้ใช้คนอื่นๆสามารถนำโปรแกรมนี้ไปประยุกต์ใช้กับข้อมูลของตนได้ แต่จะไม่สามารถทำการดัดแปลงหรือแก้ไขโปรแกรมได้ ผู้ใช้ไม่จำเป็นต้องเขียนโปรแกรมเอง ซึ่งเป็นการประหยัดเวลาแรงงาน และค่าใช้จ่ายในการเขียนโปรแกรม นอกจากนี้ยังไม่ต้องใช้เวลามากในการฝึกและปฏิบัติ ซึ่งโปรแกรมสำเร็จรูปนี้มักจะมีการใช้งานในหน่วยงานที่ขาดบุคลากรที่มีความชำนาญเป็นพิเศษในการเขียนโปรแกรมดังนั้นการใช้โปรแกรมสำเร็จรูปจึงเป็นสิ่งที่อำนวยความสะดวกและเป็น

ประโยชน์อย่างยิ่งตัวอย่างโปรแกรมสำเร็จรูปที่นิยมใช้ได้แก่ MS-Office, Lotus, Adobe Photoshop, SPSS, Internet Explorer และ เกมส์ต่างๆ เป็นต้น

บุคลากร (People ware)

หมายถึง บุคลากรในงานด้านคอมพิวเตอร์ ซึ่งมีความรู้เกี่ยวกับคอมพิวเตอร์สามารถใช้งาน สั่งงานเพื่อให้คอมพิวเตอร์ทำงานตามที่ต้องการ แบ่งออกได้ 4 ระดับดังนี้

ผู้จัดการระบบ (System Manager) คือ ผู้วางนโยบายการใช้คอมพิวเตอร์ให้เป็นไปตามเป้าหมายของหน่วยงาน

นักวิเคราะห์ระบบ (System Analyst) คือ ผู้ที่ศึกษาระบบงานเดิมหรืองานใหม่และทำการวิเคราะห์ความเหมาะสมความเป็นไปได้ในการใช้คอมพิวเตอร์กับระบบงานเพื่อให้โปรแกรมเมอร์เป็นผู้เขียนโปรแกรมให้กับระบบงาน

โปรแกรมเมอร์ (Programmer) คือผู้เขียนโปรแกรมสั่งงานเครื่องคอมพิวเตอร์เพื่อให้ทำงานตามความต้องการของผู้ใช้โดยเขียนตามแผนผังที่นักวิเคราะห์ระบบได้เขียนไว้

ผู้ใช้ (User) คือ ผู้ใช้งานคอมพิวเตอร์ทั่วไป ซึ่งต้องเรียนรู้วิธีการใช้เครื่องและวิธีการใช้งานโปรแกรมเพื่อให้โปรแกรมที่มีอยู่สามารถทำงานได้ตามที่ต้องการ

เนื่องจากเป็นผู้กำหนดโปรแกรมและใช้งานเครื่องคอมพิวเตอร์มนุษย์จึงเป็นตัวแปรสำคัญในอันที่จะทำให้ผลลัพธ์มีความน่าเชื่อถือเนื่องจากคำสั่งและข้อมูลที่ใช้ในการประมวลผลได้รับจากการกำหนดของมนุษย์ (People ware) ทั้งสิ้น

การดูแลคอมพิวเตอร์เบื้องต้น

มีคนอีกจำนวนมากๆ ที่ไม่เคยดูแล รักษาเครื่องคอมพิวเตอร์เบื้องต้น หรือไม่ทราบว่าจะดูแลรักษาเครื่องคอมพิวเตอร์ของเราให้อยู่กับเรานานๆ ได้อย่างไร อันนี้ไม่ได้โทษใคร แต่เราอยากจะแนะนำวิธีการดูแลรักษาเครื่องคอมพิวเตอร์ของเรา แบบพื้นฐาน อย่างน้อย จะได้ทราบว่า คอมพิวเตอร์ของเราอยู่ในสภาพแบบไหน พร้อมใช้งานหรือไม่ เริ่มต้นการดูแลรักษา ตรวจสอบเครื่องคอมพิวเตอร์

1. **สภาพภายนอก** แนะนำให้ทำความสะอาดสักนิด อย่างน้อยก็เพื่ออนามัย และสุขภาพของคุณเอง คุณทราบหรือไม่ แป้นพิมพ์หรือคีย์บอร์ด มันสกปรกขนาดไหน (ลองคิดเล่นๆ ดูว่า วันๆ คุณหยิบจับอาหาร และใช้งานแป้นพิมพ์หรือไม่ และฝุ่นละอองข้างๆ มีมากน้อยเพียงใด) ควรทำสะอาดบ้าง อย่างน้อย สัปดาห์ละ 1 ครั้ง
2. **สายไฟ สายสัญญาณต่างๆ** หลวม หรือหักชำรุดหรือไม่ แนะเสียบปลั๊กแล้ว ไฟติดๆ ดับๆ บ่อยๆ แนะนำให้รีบแก้ไข ถ้าแก้ไขไม่ได้ ให้รีบซื้อเปลี่ยนใหม่ดีกว่า ไฟติดๆ ดับๆ บ่อยๆ มีบ่อยกับคอมพิวเตอร์อย่างมาก วันดี คืนดีอาจเปิดไม่ติดเลย
3. **พื้นที่ว่างบนฮาร์ดดิสก์** หลังจากเปิด Windows เข้ามาแล้ว ลองเช็คพื้นที่ในฮาร์ดดิสก์ เสียก่อนว่า เหลือเท่าไหร่ ถ้าเหลือน้อยกว่า 500 MB ก็ควรพิจารณาเพิ่มพื้นที่ว่างได้แล้ว โดยเฉพาะกับ Drive C: (ซึ่งเป็นที่เก็บโปรแกรม) แนะนำให้สำรองข้อมูล โดยเฉพาะไฟล์ต่างๆ?ทีอยู่ใน My Documents ออกไปบ้าง หรืออาจสำรองลง Drive อื่นๆ (ถ้ามี)
4. **ตรวจสอบสภาพฮาร์ดดิสก์** นอกเหนือเรื่องพื้นที่ว่างแล้ว สิ่งสำคัญอีกอย่างหนึ่งก็คือ การตรวจสอบฮาร์ดดิสก์ว่ามีจุดไหนเสียหรือไม่ วิธีการไม่จำเป็นต้องแกะเครื่องคอมฯ มาตรวจสอบ เพียงแค่ใช้โปรแกรมช่วยตรวจสอบ

ประเภท Disk Defragment ก็สามารถเช็คได้แล้วว่า ฮาร์ดดิสก์ของเรามี "Bad Sector" หรือไม่ (Bad Sector เป็นจุดเสียของฮาร์ดดิสก์) ถ้ามี แนะนำให้รีบสำรองข้อมูล และเปลี่ยนฮาร์ดดิสก์ไปเลยจะปลอดภัยกว่า

5. **ตรวจสอบไวรัสบ้าง** ถึงแม้ว่าเราจะมีโปรแกรม Antivirus แล้วก็ตาม เราก็ยังคงจำเป็นต้องมีการตรวจสอบไวรัสอย่างสม่ำเสมอ อย่างน้อยอาทิตย์ละครั้ง และที่สำคัญก็ควรอัปเดทโปรแกรมแบบออนไลน์ให้ทันสมัยอยู่เสมอด้วยเช่นกัน

วิธีแก้ปัญหาเวลาคอมพิวเตอร์ทำงานช้าลง

สาเหตุของปัญหาที่คอมพิวเตอร์ทำงานช้าลงนั้น อาจมาจากปัจจัยหลายๆ อย่างประกอบกัน ทั้งนี้ขึ้นกับลักษณะการใช้งานของแต่ละบุคคล ตัวอย่างเช่น ถ้าเป็นคนทีชอบติดตั้งโปรแกรม ทดสอบโปรแกรมใหม่ๆ ตลอดเวลา ปัญหาคอมพิวเตอร์ทำงานช้าลง ดูจะเป็นเรื่องปกติ เพราะการติดตั้งโปรแกรมมากๆ ย่อมทำให้ระบบคอมพิวเตอร์โดยเฉพาะในส่วนของ Register มีปัญหาได้ง่าย เป็นต้น

ตรวจสอบปัญหาทีละขั้นตอน

1. **ตรวจสอบ Hard Disk มีพื้นที่ว่างสักเท่าไหร่** อย่างน้อยควรมีพื้นที่ใน Drive C: อย่างน้อย 500 MB - 1 GB ถ้าเต็มก็คงต้องลบไฟล์เก่าๆ ที่ไม่ใช้ออกเสียบ้าง (จะช่วยการทำงานของคอมพิวเตอร์ให้ดีขึ้น ได้เยอะ)
2. **ลบไฟล์ขยะออกจากระบบเสียบ้าง** โดยเฉพาะนักท่องเน็ตทั้งหลาย เพราะเวลาเราเข้าเว็บไซต์ จะมีไฟล์ที่โหลดเข้ามาในเครื่องคอมฯ ของเรา ดังนั้น ต้องลบบ้าง อาจใช้โปรแกรม Disk Cleanup ของ Windows เองก็ได้ (เข้าไปที่ Start ->All Programs -> Accessories -> System Tools -> Disk Cleanup) ช่วยได้เยอะเหมือนกัน แถมยังลบไวรัสบางตัวออกไปได้ด้วย
3. **ปรับปรุง Hard disk ให้อย่างในสภาพพร้อมใช้งาน** โดยการจัดเรียงข้อมูลบน hard disk ซึ่งจะช่วยได้มาก ในกรณีที่เราใช้งานคอมพิวเตอร์และบันทึกข้อมูลบ่อยๆ เนื่องจากการจัดเก็บข้อมูลบน hard disk จะจัดเก็บในลักษณะของการสุ่ม ดังนั้นไฟล์ หนึ่งไฟล์ อาจถูกจัดเก็บแบบไม่ต่อเนื่อง ดังนั้นเวลาจะนำมาใช้งาน ก็เสียเวลาในการค้นหาไฟล์ (การจัดเรียงข้อมูลและตรวจสอบ hard disk สามารถเข้าไปได้ที่ Start -> All Programs -> Accessories -> System Tools -> Disk Defragmenter) **สิ่งสำคัญ** การทำ Defragment จะต้องทำการ shutdow Windows ก่อนเริ่มใช้งานใหม่ทุกครั้ง
4. **อัปเดทโปรแกรม Antivirus** และสั่ง Scan Virus ทุกๆ Drive (เคยทำบ้างหรือเปล่าครับ)

วิธีดูแลรักษาเครื่องคอมพิวเตอร์ประจำวัน

1. **ตอนเช้า** ปัดฝุ่น ทำความสะอาดบริเวณใกล้เคียง เพื่ออนามัยของตัวคุณเอง จากประสบการณ์พบว่า คนส่วนใหญ่ทำงานในขณะที่หน้าจอสกปรก บริเวณข้างเคียงฝุ่นเต็มไปหมด ระวังน่ะครับจะเป็นโรคภูมิแพ้ มาทำความสะอาดเพื่อสุขภาพของตัวคุณเองดีกว่า
2. ลบขยะภายในเครื่องคอมฯ แหล่งสะสมของปัญหา รวมทั้งไวรัส ด้วยโปรแกรมที่มีมากับ Windows ทุกเวอร์ชั่น Disk Cleanup (การเข้าถึงโปรแกรม ให้คลิกเข้าไปที่ Start -> All programs ->Accessories -> System Tools และคลิกเลือก Disk Cleanup)

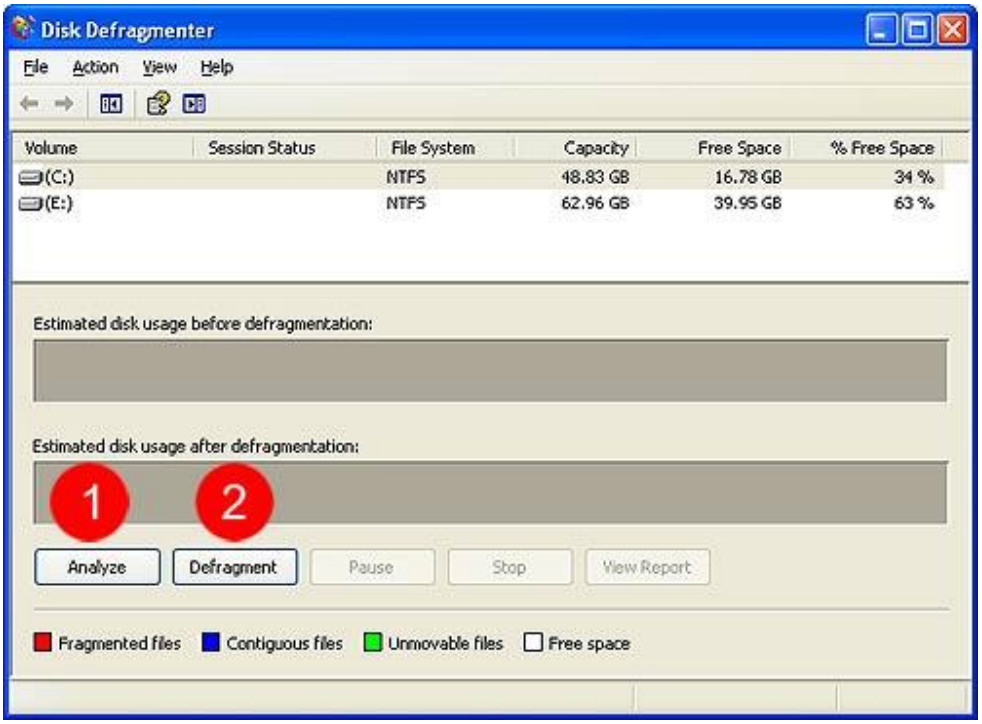
3. อัปเดท Anti-virus ด้วยกับกดปุ่ม "Live Update" บางโปรแกรมอาจเรียก "Update" แล้วแต่โปรแกรมที่คุณใช้งาน เราสามารถตรวจสอบเบื้องต้นได้ง่ายๆ ว่า โปรแกรม Anti-virus ของเรา Update หรือไม่ โดยการเปิดโปรแกรมนั้นๆ ให้ดูหัวข้อเกี่ยวกับ Update และดูวันที่ล่าสุดที่มีการ Update ถ้าตรงกับวันที่ปัจจุบัน หรือใกล้เคียงก็ถือว่าใช้ได้แล้ว
4. ตรวจสอบพื้นที่ของ Hard Disk ว่าคงเหลืออยู่เท่าไหร่ เพราะโปรแกรมภายใต้ Windows ทั่วไปจะมีการใช้ Hard Disk เป็นส่วนหนึ่งในการประมวลผลข้อมูล และโดยเฉพาะกับผู้ที่ใช้งานโปรแกรมตัดต่อภาพ เช่น Adobe Photoshop เป็นต้น ยิ่งจำเป็นต้องมีพื้นที่ว่างใน hard disk มากๆ โดยเฉพาะ Drive C:\ แนะนำว่าควรมีอย่างน้อยสัก 1-2 เป็นอย่างต่ำ (ต่ำมากๆ แล้วน่ะครับ) ส่วนวิธีการตรวจสอบให้ดับเบิลคลิกที่ My Computer จากนั้นดูคำว่า Free Space ใน Drive C:\
5. **พักเที่ยง** แนะนำให้สั่งรัน scan virus ทุกวัน (แนะนำให้ตั้ง schedule ให้รันอัตโนมัติไปเลย) เพราะช่วงเวลานี้เป็นเวลาดี ที่จะได้ตรวจสอบไวรัสอย่างเต็มที่ ไม่ขัดจังหวะเวลาทำงาน เพราะระหว่างการ scan virus จะทำให้เครื่องคอมฯ ทำงานช้าลงไปได้บ้าง ระหว่างนี้ สามารถปิดหน้าจอได้ด้วย ประหยัดพลังงาน ประหยัดเงิน แถมช่วยทำให้หน้าจอมีอายุยาวนานขึ้น
6. **ก่อนกลับบ้าน** อย่าลืม Shutdown Windows ให้ถูกวิธี ห้ามปิดด้วยปุ่ม Power เป็นอันขาด เพราะอาจทำให้คุณไม่สามารถเข้าทำงาน Windows ได้อีก เพราะเครื่องพัง..

ตรวจสุขภาพฮาร์ดดิสก์ด้วย Disk Defragment

วิธีการดูแลรักษาคอมพิวเตอร์พื้นฐานอย่างหนึ่ง ซึ่งเป็นหัวข้อที่ถูกแนะนำมากที่สุด นั่นคือ การทำ Disk Defragment หรือ การตรวจสอบสุขภาพฮาร์ดดิสก์ สำหรับประโยชน์ที่ได้จากการทำ Disk Defragment ประกอบด้วย

- เป็นการจัดเรียงข้อมูลใหม่ ทำให้คอมพิวเตอร์ทำงานได้เร็วขึ้น
- ทำให้ทราบว่ามีจุดใด จุดหนึ่งของฮาร์ดดิสก์ เสียหายหรือไม่
- ทำให้ทราบและสามารถป้องกันปัญหาที่อาจเกิดขึ้น
- เพิ่มพื้นที่ในฮาร์ดดิสก์ได้ (บางส่วน)

ขั้นตอนการทำ Disk Defragment



1. คลิกที่ปุ่ม Start
2. เลือก All Programs
3. เลือก Accessories
4. คลิกเลือกเมนู System Tools
5. เลือกคำสั่ง Disk Defragmenter จะพบหน้าต่าง Disk Defragmenter
6. แนะนำให้คลิกทำ "Analyze" ก่อน (ใช้เวลาไม่นาน)
7. จากนั้นให้ทำ "Defragment" ต่อทันที
8. รอสักครู่ (ทั้งนี้ขึ้นกับข้อมูล และขนาดของฮาร์ดดิสก์)

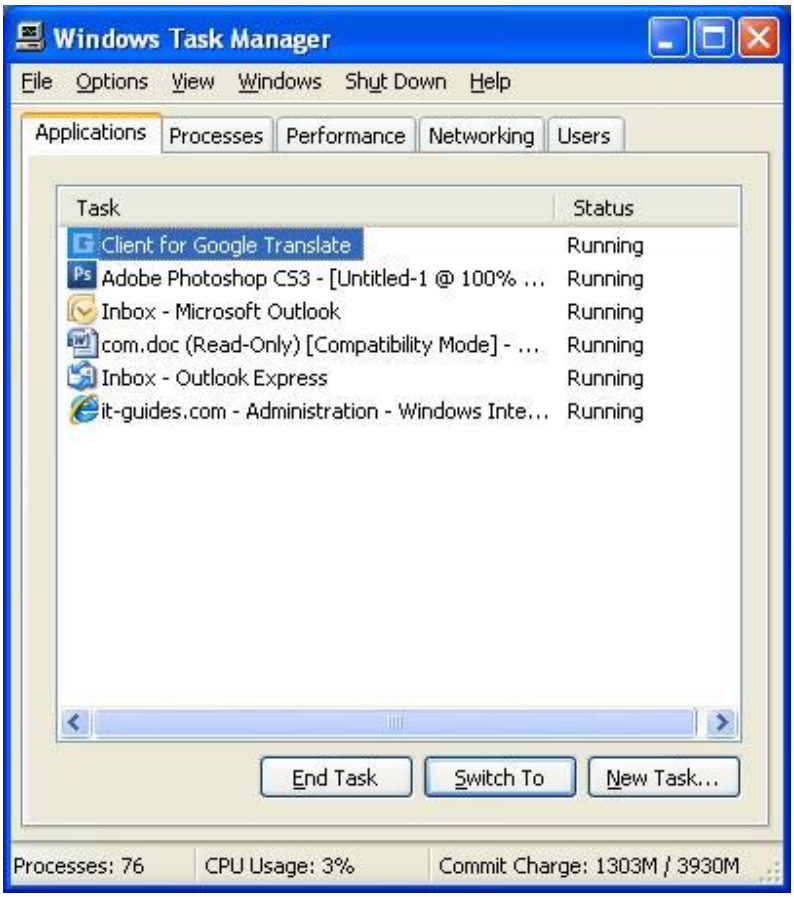
ข้อควรทราบก่อนทำ Disk Deframenter

- ปิดโปรแกรมการใช้งานอื่นๆ ให้หมด
- ยกเลิก Screen Saver (ให้คลิกขวาที่หน้า Desktop เลือก Properties เลือกแท็ป Screen Saver และเลือก "None")

- ถ้าเป็น Notebook แนะนำให้ยกเลิกระบบ Power Save (ประหยัดพลังงาน) แนะควรเสียบสายไฟด้วย เพราะอาจต้องใช้เวลานานพอสมควร

ที่สำคัญ หลังจากทำ Disk Defragmenter แล้ว **จะต้อง Shutdown Windows** ทุกครั้ง และรอสัก 2-3 นาทีค่อยเริ่มเปิดใช้งานใหม่

วิธีแก้ไขปัญหา คอมพิวเตอร์ค้าง



1. ลองกดปุ่ม Ctrl + Alt + Del ทั้ง 3 ปุ่ม พร้อมกันเราจะพบหน้าต่าง "Task Manager" ให้สังเกตแท็ป "Applications" ถ้ามีโปรแกรมใด โปรแกรมหนึ่งมี "Status" Non Response" ให้คลิกเลือกโปรแกรมนั้นๆ และคลิกปุ่ม "End Task"
2. ถ้าไม่มีเลย กดปุ่ม Ctrl + Alt + Del ไม่ได้มีทางเดียวคือ การกดปุ่ม (Power) ปิดค้างไว้ จนกระทั่ง Windows Shutdown ลงเองจากนั้นให้ให้รอสักครู่ และเริ่มเปิดเครื่องคอมพิวเตอร์ใหม่อีกครั้ง

ไวรัสและภัยจากการใช้เทคโนโลยีสารสนเทศ

ภัยคุกคามด้านความปลอดภัยข้อมูลคอมพิวเตอร์นั้น นับวันยิ่งทวีความซับซ้อน และ เพิ่มความรุนแรงขึ้น สังเกตุได้จากสถิติของสำนักวิจัยหลายสำนักได้ทำการวิเคราะห์ภัยคุกคามต่างๆ ที่กำลังเป็นปัญหาใหญ่ของผู้ดูแลระบบความปลอดภัยข้อมูลคอมพิวเตอร์ หรือ ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ ตลอดจนกระทบถึงการปฏิบัติงานขององค์กร เพราะทุกวันนี้ ระบบสารสนเทศ และ เครือข่ายอินเทอร์เน็ตนั้น มีความสำคัญเป็นแกนหลักในการทำธุรกิจและ ธุรกรรมของทุก

องค์กรไม่ว่าจะเป็นภาครัฐและเอกชนดังนั้นถ้าระบบสารสนเทศไม่มีความปลอดภัยที่ดีพอ และ เรายังจัดการกับปัญหาของระบบได้ไม่ถูกทางหรือไม่ถูกจุด ทำให้ปัญหาต่าง ๆ ยังคงอยู่ ถึงแม้ว่าเราจะลงทุนกับระบบรักษาความปลอดภัยข้อมูลคอมพิวเตอร์ไปมากเท่าไหร่ก็ตาม ดังนั้นเราควรทำความเข้าใจศึกษาและวิเคราะห์ปัญหาภัยคุกคามทางคอมพิวเตอร์เหล่านั้นเพื่อที่จะได้วางแผนจัดการได้อย่างตรงประเด็น เพื่อ ความปลอดภัยและเสถียรภาพที่ดีขึ้นของระบบคอมพิวเตอร์ในองค์กร รวมถึงคอมพิวเตอร์ที่เราใช้อยู่เป็นส่วนตัวในลักษณะ Home User อีกด้วย

1. SPAM Email และ Malicious Email content

เราคงปฏิเสธไม่ได้ว่า Email ได้กลายเป็นส่วนหนึ่งของชีวิตประจำวันในการทำงานไปแล้วปัญหาก็คือพวกผู้ไม่หวังดีได้ใช้ Email เป็นเครื่องมือในการส่งข้อมูลที่มีอันตรายให้กับเราและองค์กรเช่น MalWare หรือโปรแกรมมุ่งร้ายในรูปแบบต่างๆไม่ว่าจะมาทาง Attached File หรือมาในรูปแบบของเนื้อหาล่อลวงใน Email Body จากปี 1997 ปริมาณ SPAM Email เพิ่มขึ้นถึง 10 เท่าและมีแนวโน้มที่จะเพิ่มขึ้นเป็นทวีคูณในปีต่อๆไปเนื่องจากทุกวันนี้บรรดา SPAMMER สามารถทำเงินได้จากการส่ง SPAM Email กลายเป็นอาชีพด้านมืดที่ทำรายได้งามให้กับเหล่ามิจฉาชีพทางอินเทอร์เน็ตจนทางสหรัฐอเมริกาต้องออกกฎหมาย "CAN SPAM ACT" ขึ้นมาเพื่อต่อต้านเหล่า SPAMMER แต่ก็ยังไม่สามารถกำจัด SPAM Email ให้หมดไปจากโลกอินเทอร์เน็ตได้

วิธีการแก้ปัญหาที่ถูกทางก็คือการใช้ระบบ ANTI-SPAM/ANTI-Virus ที่บริเวณ Internet Gateway หรือ DMZ กรอง SPAM Email ในจุดที่ที่ระบบเรารับ - ส่ง Email จากอินเทอร์เน็ตและการใช้ ANTI-SPAM Software ช่วยที่ PC Client เพื่อเป็นการกรอง SPAM MAIL แบบละเอียดอีกชั้นหนึ่งตลอดจนพยายามไม่ประกาศ Email เราใน Web board หรือในเว็บไซต์ของเราเองถ้าต้องการประกาศ Email ให้ผู้อื่นรับทราบให้ใช้วิธีประกาศเป็นรูปภาพหรือใช้ HTML Characterจะปลอดภัยกว่าการประกาศแสดงเป็น Plain Test ธรรมดาซึ่งจะทำให้พวก SPAMMER สามารถเข้ามาเก็บ Email ของเราไปทำการส่ง SPAM Email ต่อไปโดยใช้โปรแกรมประเภท BOTNET เช่น Email Harvester Program เป็นต้น

2. SPYWARE

มีงานวิจัยเรื่อง SPYWARE ได้สรุปว่า 80% ของ PC ทั่วโลกติด SPYWARE และเครื่อง PC เหล่านั้นล้วนมีโปรแกรม ANTI-VIRUS แล้วเป็นส่วนใหญ่ปัญหาก็คือโปรแกรม SPYWARE ไม่ใช่โปรแกรม VIRUS ยกตัวอย่างเช่นโปรแกรมดักคีย์บอร์ดและเก็บหน้าจอการใช้งานคอมพิวเตอร์ของเราที่ในวงการเรียกว่าโปรแกรม "KEY LOGGER" เป็นโปรแกรม SPYWARE ที่ระบบ ANTI-VIRUS ส่วนใหญ่มองไม่เห็นและไม่สามารถกำจัด SPYWARE เหล่านี้ออกจากเครื่องคอมพิวเตอร์ของเราได้เราติดโปรแกรม SPYWARE ก็เพราะการใช้งานอินเทอร์เน็ตโดยการเข้า Web site ต่างๆโดยไม่ระมัดระวังให้ดีพอรวมทั้งการ Download ไฟล์ที่มี SPYWARE ติดมาด้วยตลอดจนการเปิด Email attached file ที่มีโปรแกรม SPYWARE แนบมาด้วยขณะนี้โปรแกรม SPYWARE สามารถมาในรูปของ Cookies เวลาเราเข้าเว็บไซต์ที่ไม่เหมาะสมเช่นเว็บภาพลามกหรือเว็บที่ใช้ในการหา Serial number ของซอฟท์แวร์ผิดกฎหมายเป็นต้นบางครั้ง SPYWARE ก็ติดมากับโปรแกรมประเภท P2P ที่กำลังได้รับความนิยมอยู่ในขณะนี้ทางแก้ปัญหาก็คือเราต้องระมัดระวังในการใช้งานอินเทอร์เน็ตให้มากขึ้นตลอดจนหมั่นใช้โปรแกรมประเภท Freeware หรือ Shareware เช่น AD-AWARE หรือ SPYBOT Search & Destroy ในการช่วยตรวจสอบระบบ PC ของเราว่าตกเป็นเหยื่อ SPYWARE หรือไม่ถ้าตรวจพบก็ควรกำจัดออกโดยเร็วจะทำให้เราไม่เสียความเป็นส่วนตัวและทำให้ PC ของเราเร็วขึ้นตลอดจนประหยัด Bandwidth ในการใช้งานเครือข่ายให้แก่องค์กรโดยรวมอีกด้วย

3. Malware (Malicious Software)

Mal ware คือ Malicious Software หรือโปรแกรมมุ่งร้ายที่มาในรูปแบบต่างๆไม่ว่าจะเป็น ActiveX หรือ Java Applet ที่มากับการใช้งาน Internet Browser โดยไม่ได้รับการติดตั้ง Patch หรืออาจมาในรูปของ Attached File ที่อยู่ใน Email ตลอดจนแฝงมากับโปรแกรม Shareware หรือโปรแกรม Utility หรือโปรแกรม P2P ที่เรานิยมใช้ในการ Download เพลงหรือภาพยนตร์ผ่านทางอินเทอร์เน็ตโปรแกรม Mal ware อาจจะเป็น SPYWARE, Trojan Horse, Key logger หรือ Viruses และ Worm ที่เรารู้จักกันดีในช่วงหลังๆไวรัสคอมพิวเตอร์มักจะมากับ Email โดยมักจะมาในรูป Zip File และมีการปลอมแปลงชื่อผู้ส่งปลอมแปลง Email Subject เป็นส่วนใหญ่เทคนิคการหลอกผู้ใช้ Email ให้หลงเชื่อที่เราเรียกว่า "Social Engineering" เป็นวิธีการเก่าแก่ที่ผู้ไม่หวังดีนิยมใช้เป็นประจำทางแก้ปัญหานอกจากจะใช้โปรแกรม ANTI-VIRUS และ ANTI-MalWare แล้วยังควรจะต้องฝึกอบรม "Information Security Awareness Training" ให้กับผู้ใช้งานคอมพิวเตอร์อีกด้วยโดยเฉพาะกลุ่มผู้ใช้คอมพิวเตอร์ที่ไม่ใช่คนไอที (Non-IT people) เพื่อให้ผู้บริหารหรือผู้ใช้งานคอมพิวเตอร์ทั่วไปมีความเข้าใจถึงวิธีการหลอกลวงของผู้ไม่หวังดีและเพื่อให้รู้เท่าทันไม่ตกเป็นเหยื่อของผู้ไม่หวังดีเพราะการหวังพึ่งโปรแกรม ANTI-VIRUS โดยการหมั่น Update Virus Signature หรือ VIRUS Pattern ดังนั้นไม่เพียงพอเสียแล้วเพราะไวรัสตัวใหม่ๆสามารถสั่งปิดการทำงานของโปรแกรม ANTI-VIRUS ได้และยังมีไวรัสใหม่ๆที่ออกมาโดยที่โปรแกรม ANTI-VIRUS ยังไม่มี Signature หรือ Pattern ที่เราเรียกว่า ZERO-DAY ATTACK หรือ VIRUS Outbreak ดังนั้นการฝึกอบรมให้ผู้ใช้คอมพิวเตอร์มีความตระหนักและความเข้าใจจึงเป็นหนทางที่ไม่อาจถูกมองข้ามได้ในสถานการณ์การแพร่ระบาดไวรัสในขณะนี้และในอนาคต

4. จากการล่อลวงโดยวิธี Phishing และ Pharming

"Phishing" นั้นอ่านออกเสียงว่า "Fishing" หมายถึงการตกปลาเราอาจตกเป็นเหยื่อของการตกปลาถ้าเราเผลอไปกับเหยื่อที่เหล่า "Phisher" หรือผู้ไม่หวังดีล่อไว้วิธีการของผู้ไม่หวังดีก็คือการส่ง Email ปลอมแปลงชื่อคนส่งและชื่อเรื่อง (Email address & Email subject) ตลอดจนปลอมแปลงเนื้อหาใน Email ให้ดูเหมือนจริงเช่นส่ง Email มาบอกเราว่ามาจากธนาคารที่เราติดต่ออยู่เป็นประจำแล้วบอกให้เรา Login เข้าใช้งาน Internet Banking โดยจะทำ Link มาล่อให้เรา Click ถ้าเราเผลอ Click โดยไม่ระมัดระวังเราก็จะเข้าไปติดกับดักที่ Phisher วางไว้โดยทำการจำลองเว็บไซต์ของธนาคารให้ดูเหมือนจริงแต่จริงๆเป็นเว็บของผู้ไม่หวังดีเอาไว้ดักจับ User Name และ Password ของเราจากนั้น Phisher จะเอาจับ User Name และ Password ของเราเข้าไป Login ใช้งานในเว็บไซต์จริงของธนาคารและทำการโอนเงินหรือชำระเงินค่าสาธารณูปโภคเช่นค่าน้ำ, ค่าไฟ, ค่าโทรศัพท์, ค่า UBC หรือค่าเล่าเรียนโดยที่เราต้องเป็นผู้รับผิดชอบค่าใช้จ่ายทั้งหมดธนาคารคงไม่สามารถรับใช้แทนเราได้เพราะเราเป็นคนบอก User Name และ Password ให้กับผู้ไม่หวังดีเสียเองเป็นต้น

ทางแก้ปัญหาคือเราต้องมีสติและคอยระมัดระวัง Email ประเภทนี้บางครั้ง Email เหล่านั้นอาจมาในรูปของ Trojan Program ที่เข้ามาแก้ไขไฟล์ HOSTS ในเครื่องเราให้ Redirect ไปยังเว็บของผู้ไม่หวังดีโดยตรงเลยก็มีวิธีการแบบนี้รวมทั้งการ Hijack DNS Server เราเรียกว่าวิธีการ "Pharming" ซึ่งกำลังได้รับความนิยมเพิ่มขึ้นรายละเอียดเพิ่มเติมเข้าไปดูได้ที่ Website www.antiphishing.org.

5. จาก Hacker และ Google Hacking Method

ปัจจุบันการ Hack ไปยัง Web Application ดังที่ได้เห็นสถิติจาก Web Site "www.zone-h.org" นั้นได้มีการเปลี่ยนแปลงรูปแบบไปแล้วโดยมีการอาศัย Google.com เป็นช่องทางค้นหา Web ที่มีช่องโหว่ซึ่งสามารถ hack ได้โดยง่ายจากนั้นจึง Hack ตามวิธีการปกติและเนื่องจาก Google hacking นั้นจะเป็นการ hacking แบบไม่เลือกเหยื่อดังนั้นทุก Web ที่มีช่องโหว่ที่ Google เห็นจึงล้วนแล้วแต่มีโอกาสถูก hack เท่าๆกันทั้งสิ้น

คำหลักที่ใช้พิมพ์ใส่ใน Google นั้นบางคำสั่งสามารถทำให้ทราบ Username และ Password ของเหยื่อได้โดยตรงเช่น "filetype:pwd service" และ "inurl:password.log filetype:log" สำหรับวิธีการป้องกันนั้นมีวิธีเดียวคือการ

ทำ "Secure Coding" เป็นการเขียนโปรแกรมอย่างปลอดภัยซึ่งสามารถศึกษา Guide line ได้จาก "www.owasp.org" โดยปรับมาใช้ทั้งในส่วนของ Web Application , Web Server และ Operation System

6. จากโปรแกรม "Peer-to-Peer" (P2P)

เป็นภัยซึ่งเกิดจาก End User เป็นหลักเนื่องจากโปรแกรมประเภทนี้นั้นจะให้ประโยชน์กับเรื่องส่วนตัวของ End User เช่นการใช้โปรแกรม KAZAA เพื่อดาวน์โหลดหนังและเพลงแบบผิดกฎหมายหรือใช้โปรแกรม SKYPE ในการพูดคุยสื่อสารแทนการใช้โทรศัพท์ซึ่งการใช้โปรแกรมดังกล่าวนั้นจะนำภัยสองประเภทมาสู่องค์กรได้แก่

- การสิ้นเปลือง Bandwidth เครือข่ายขององค์กร - ปัญหานี้เกิดขึ้นเนื่องจากการใช้ Bandwidth จำนวนมากเช่น โปรแกรม KAZAA นั้นเป็นการดาวน์โหลดข้อมูลเถื่อน (illegal software) จากเครื่อง PC อื่นๆทั่วโลกหรือโปรแกรม SKYPE ซึ่งใช้เป็นโทรศัพท์ผ่านอินเทอร์เน็ต
- สร้างปัญหาด้าน Confidentiality - เคยพบว่ามีช่องโหว่บน KAZAA ซึ่งทำให้ Hacker สามารถเจาะมายัง Harddisk ของคนทั้งโลกที่ติดตั้งโปรแกรม KAZAA ได้ซึ่งแน่นอนว่าจะทำให้ข้อมูลสำคัญขององค์กรหลุดรั่วไปยังมือของผู้ไม่ประสงค์ดีได้

การแก้ปัญหาสามารถทำได้โดยที่องค์กรควรจะ Implement Preventive Control โดยใช้โปรแกรมประเภท Desktop Management หรือ ANTI-MalWare ซึ่งสามารถควบคุมพฤติกรรมการใช้งานคอมพิวเตอร์ของ End User รวมถึงการติดตั้งและใช้โปรแกรมต่างๆบนเครื่องและอาจใช้โปรแกรมด้าน Network Monitoring เฝ้าระวังเครือข่ายเพิ่มเติมเพื่อเป็น Detective Control ให้กับองค์กรด้วย

7. จาก Wireless Network Threat

การติดตั้ง Wireless Network นั้นเป็นเรื่องที่ค่อนข้างอันตรายเนื่องมาจากโครงสร้างของ wireless network นั้นออกแบบมาอย่างไม่ปลอดภัย อีกทั้งเทคโนโลยีด้านนี้นั้นยังไร้ Boundary สามารถขยายไปยังภายนอกองค์กรได้อีกด้วย

อีกทั้งในปัจจุบันผู้ที่นำเทคโนโลยีด้านนี้มาใช้นั้นยังมีความรู้ในการใช้เทคโนโลยีนี้อย่างปลอดภัยน้อยมากซึ่งจากการสำรวจการใช้งาน Wireless Network

8. SPIM (SPAM Instant Messaging)

SPIM นั้นคือ SPAM ที่ใช้ช่องทาง IM (Instant Messaging) ในการกระจาย Malicious Code โดยผู้ที่เป็น SPIMMER นั้นจะใช้ BOT เพื่อค้นหาชื่อของคนที่ใช้โปรแกรม IM อยู่จากนั้นจึงใช้ BOT แสดงคำพูดเพื่อให้เหยื่อเข้าใจว่าเป็นมนุษย์จากนั้นจึงส่งโฆษณาข้อมูลหลอกลวงลิงค์เวปไซท์หรือแม้แต่ Spyware และ Malware ต่างๆให้กับเหยื่อ

การป้องกันสามารถทำได้ดังนี้

- สำหรับ Yahoo Messenger, ให้คลิ๊กไปที่ Messenger -> Preferences -> Ignore List และเลือกที่ช่อง "Ignore anyone who is not on my Messenger List
- สำหรับ AOL's Instant Messenger, หรือ AIM, ให้คลิ๊กไปที่ My AIM -> Edit Options -> Edit Preferences -> Privacy และเลือกที่ช่อง "Allow only users on my buddy list
- สำหรับ MSN Messenger, ให้คลิ๊กไปที่ Tools -> Options -> Privacy และเลือกที่ช่อง "Only people on my Allow List can see my status and send me messages
- สำหรับ BitWise IM, ให้คลิ๊กไปที่ Preferences -> Server / Contact List ->และเลือกที่ช่อง "Whitelist

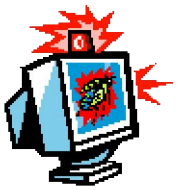
9. PDA Malware

ข้อมูลใน PDA สามารถที่จะเป็นพาหะของ viruses, worms, dialers, Trojan horses และ Malicious Mobile Code ต่างๆได้เหมือนกับข้อมูลที่อยู่ในเครื่อง PC โดยจากผลสำรวจการใช้งาน PDA ของนักธุรกิจในสหรัฐอเมริกาโดยมหาวิทยาลัย Pepperdine University เมื่อปี 2004 พบว่าครึ่งหนึ่งของจำนวนผู้ที่ถูกสำรวจไม่มีการใช้โปรแกรมหรือลงโปรแกรมใดๆที่เกี่ยวข้องกับการรักษาความปลอดภัยของข้อมูลบน PDA เลยซึ่ง 81 เปอร์เซ็นของผู้ที่ถูกสำรวจยังบอกด้วยว่าพวกเขาบันทึกข้อมูลที่มีคุณค่าหรือความสำคัญมากใน PDA

ในปัจจุบันนั้นได้มีโปรแกรม Anti-Virus/Anti-Malware สำหรับ PDA เป็นจำนวนมากซึ่งคุณสามารถติดตามได้จากผู้จำหน่ายโปรแกรม Anti-virus/Anti-Malware รายใหญ่ทุกรายและควรลองนำมาใช้ก่อนซื้อ

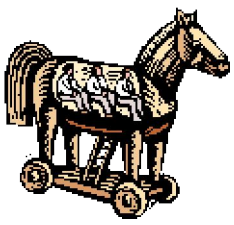
10. Virus และ Worm

ไวรัสสำหรับคอมพิวเตอร์นั้นหมายถึงโปรแกรมคอมพิวเตอร์ที่ถูกเขียนขึ้นมา แต่ไม่ได้มีไว้สำหรับใช้งานแต่เป็นการก่อนกวน หรือทำลายระบบ ของคอมพิวเตอร์และสามารถที่จะแพร่กระจายได้ด้วยตัวมันเอง โดยการทำลายและแพร่กระจายจะถูกกำหนดจากผู้เขียนโปรแกรมไวรัสนั้นๆ



ไวรัส (Viruses)คือโปรแกรมคอมพิวเตอร์ประเภทหนึ่งที่ถูกออกแบบมาให้แพร่กระจายตัวเองจากไฟล์หนึ่งไปยังไฟล์อื่นๆภายในเครื่องคอมพิวเตอร์ไวรัสจะแพร่กระจายตัวเองอย่างรวดเร็วไปยังทุกไฟล์ภายในคอมพิวเตอร์หรืออาจจะทำให้ไฟล์เอกสารติดเชื้ออย่างช้าๆ แต่ไวรัสจะไม่สามารถแพร่กระจายจากเครื่องหนึ่งไปยังอีกเครื่องหนึ่งได้ด้วยตัวมันเองโดยทั่วไปเกิดจากการที่ผู้ใช้เป็นพาหะ นำไวรัสจากเครื่องหนึ่งไปยังอีกเครื่องหนึ่งเช่นเวลาที่ส่ง E-mail โดยแนบเอกสาร หรือไฟล์ที่มีไวรัสไปด้วย, การทำสำเนาไฟล์ที่ติดไวรัสไปไว้บนไฟล์เซริฟเวอร์, การแลกเปลี่ยนไฟล์โดยใช้แผ่นดิสก์เก็ต เมื่อผู้ใช้ทั่วไปรับไฟล์ หรือดิสก์มาใช้งานไวรัสก็จะแพร่กระจายภายในเครื่อง และจะเป็นวงจรในลักษณะนี้ต่อไป

หนอน (Worms)ในอีกความหมายหนึ่ง เป็นสิ่งที่อันตรายต่อระบบมาก (สามารถทำความเสียหายต่อระบบได้จากภายใน เหมือนกับหนอนที่กัดกินผลไม้จากภายใน)โดยทั่วไปก็จะคล้ายกับไวรัสคอมพิวเตอร์และด้วยการอาศัยพฤติกรรมการทำงานของมนุษย์ยุค IT ในการแพร่กระจายตัวเองไปยังเครื่องคอมพิวเตอร์เครื่องอื่นหนอนร้ายเป็นโปรแกรมคอมพิวเตอร์ที่ถูกออกแบบมาให้สามารถแพร่กระจายตัวเองจากเครื่องคอมพิวเตอร์เครื่องหนึ่งไปยังอีกเครื่องหนึ่งโดยอาศัยระบบเน็ตเวิร์ค (E-mail) ซึ่งการแพร่กระจายสามารถทำได้ด้วยตัวของมันเองซึ่งจะแพร่กระจายได้อย่างรวดเร็วและทำความเสียหายรุนแรงกว่าไวรัสมาก



โทรจัน (Trojan)ชื่อที่คุ้นหูจากมหากาพย์เมืองทรอยในอดีตของโฮมเมอร์ถูกนำมาใช้เป็นชื่อของโปรแกรมคอมพิวเตอร์ที่ถูกออกแบบมาให้แฝงตัวเองเข้าไปในระบบและจะทำงานโดยการดักจับเอารหัสผ่านเข้าสู่ระบบต่างๆและส่งกลับไปยังผู้ประสงค์ร้าย เพื่อเข้าใช้หรือโจมตีระบบในภายหลังซึ่งแฝงมาในหลายๆ รูปแบบ เช่นเกมส์ การ์ดอวยพร หรือจดหมายต่างๆ โปรแกรมโทรจันไม่ได้ถูกออกแบบมาเพื่อทำลายระบบ หรือสร้างความเสียหายต่อระบบ คอมพิวเตอร์โทรจันต่างจาก ไวรัสและหนอนคือมันไม่สามารถทำสำเนาตัวเองและแพร่กระจายตัวเองได้แต่มันสามารถที่จะอาศัยตัวกลาง ซึ่งอาจเป็นโปรแกรมต่างๆ จดหมายหรือการไปโหลดไฟล์จากแหล่งต่างๆ เมื่อเรียกใช้งานไฟล์เหล่านี้โทรจันก็จะทำงานและจะเปิดช่องทางต่างๆให้ผู้บุกรุกเข้าโจมตีระบบได้ดังเช่นที่พวกกรีกทำกับชาวเมืองทรอยเมื่อครั้งอดีต

ข่าวไวรัสหลอกลวง (Hoax) เป็นรูปแบบหนึ่งที่มีผลต่อผู้ใช้คอมพิวเตอร์จำนวนมากโดยไวรัสหลอกลวงพวกนี้จะมาในรูปของจดหมายอิเล็กทรอนิกส์การส่งข้อความต่อๆกันไปผ่านทางโปรแกรมรับส่งข้อความ หรือห้องสนทนาต่างๆซึ่งสามารถสร้างความวุ่นวายให้เกิดขึ้นได้มากหรือน้อยเพียงใด ก็ขึ้นกับเทคนิคและการใช้จิตวิทยาของผู้สร้างข่าวขึ้นมาโดยส่วนใหญ่จดหมายประเภทนี้จะมีหัวข้อที่ชวนเชื่อ อ้างแหล่งข้อมูลและบริษัทใหญ่ๆเป็นการสร้างความเชื่อมั่น และเมื่อผู้รับส่งต่อไปยังเพื่อนสนิทและคนคุ้นเคย ก็ยิ่งสร้างความเชื่อมั่นมากขึ้นจากนั้นผู้รับก็จะทำตัวเป็นผู้ส่งต่อๆ ไปอีกหลายๆทอดซึ่งเป็นลักษณะเด่นของไวรัสหลอกลวง หากได้รับจดหมายประเภทนี้ก็ไม่ควรที่จะส่งไปต่อๆ

ข้อควรปฏิบัติในการป้องกันไวรัส

1. ตรวจสอบ E-mail ทุกฉบับที่ส่งเข้ามา ว่ามาจากบุคคลที่รู้จักหรือไม่ข้อมูลต้นทาง และปลายทางของ E-mail ถูกต้องมีหัวข้อเรื่องที่ติดต่อชัดเจน (หากไม่แน่ใจให้สงสัยไว้ก่อน)
2. หากมีไฟล์แนบมากับ e-mail จะต้องทำการ SCAN ตรวจหาไวรัสก่อนการใช้งานทุกครั้ง
    - เอกสาร Word Excel อาจมีไวรัสประเภท Macro Virus แฝงมาได้
    - ไฟล์จำพวก . COM, .EXE, ZIP หรืออื่นๆ อาจมีไวรัสประเภท Worm, Trojan หรืออื่นๆได้ระวังไฟล์ Happyxxx.COM, .EXE, PICS4YOU.EXE หรืออื่นๆที่น่าสงสัย
3. ตรวจสอบทุกครั้งเมื่อมีการนำเอาไฟล์ข้อมูล โปรแกรมต่างๆ จากเครื่องอื่นหรือแหล่งอื่นมาใช้งาน (การโหลดโปรแกรมจากอินเตอร์เน็ต, การแชร์ดิสก์, การแลกเปลี่ยนข้อมูลข้ามเครื่อง ข้ามฝ่าย)
4. Update Virus Definition อยู่เสมอ (ระยะนี้ควรทำทุกสัปดาห์)
5. สำรองข้อมูลตามคำแนะนำของเจ้าหน้าที่ระบบคอมพิวเตอร์อย่างเคร่งครัด

อาการที่น่าสงสัย

1. เมื่อมีการบู๊ตระบบแล้วระบบไม่สามารถบู๊ตได้ตามปกติ มีข้อความเตือนเช่น "CMOS Check sum Error" (ข้อความเตือนนี้ สามารถเกิดได้จากเหตุอื่นด้วยเช่น Battery หมด)
2. เปิดเครื่องแล้วจอมืดเป็นเวลานาน (รีเซ็ทแล้วก็ไม่ทำงาน)
3. เมื่อมีการบู๊ตและเข้าสู่ระบบระหว่างที่รอวินโดว์ปรากฏข้อความที่ไม่คุ้นเคยปรากฏขึ้นมา
4. ไฟล์ Autoexec.bat ถูกแก้ไขใหม่

การป้องกันไวรัสในองค์กร

ไวรัสคอมพิวเตอร์ หลายๆท่านคงจะทราบดีว่า มหันตภัยร้ายจากไวรัสคอมพิวเตอร์ต่างๆก่อให้เกิดความเสียหาย ความวุ่นวายในการทำงานได้อย่างไรบ้างซึ่งหลายคนก็ตระหนักดีว่ามันมีความร้ายกาจขนาดไหน หรือบางท่านอาจประสบมาด้วยตัวเองบ้างแล้วก็เป็นได้ หรืออาจเคยได้ยินได้ฟังมาบ้างบางท่านอาจมีความเข้าใจผิดๆทำให้เกิดความกลัวจนเกินเหตุแล้วมาตรการสำหรับการป้องกัน ควรจะเป็นหน้าที่ของใคร ? ผู้ดูแลระบบของเรา หรือผู้ใช้เครื่องที่ต้องดูแลกันเองแล้วจะเลือกวิธีการใดในการป้องกัน จะใช้ระบบที่เป็นฮาร์ดแวร์ หรือระบบที่เป็นซอฟต์แวร์ แบบใดให้ความน่าเชื่อถือในการทำงานมากกว่าก่อนที่เราจะศึกษากันถึงวิธีการในการป้องกัน เราต้องมาทำการศึกษากันถึงพฤติกรรมและลักษณะการทำงานของไวรัส เพื่อให้เข้าใจถึงการทำงานของไวรัสสร้างความเข้าใจที่ถูกต้อง และศึกษาว่าไวรัสมีอยู่กี่กลุ่มกี่ประเภท มีกี่สายพันธุ์

หลังจากนั้นเราจึงมาศึกษาเพื่อหาวิธีป้องกันระบบให้ปลอดภัยจากไวรัสคอมพิวเตอร์ดังคำกล่าวโบราณที่กล่าวว่า "รู้เขารู้เรารบร้อยครั้งชนะร้อยครั้ง"

กลุ่มของไวรัส

กลุ่มของไวรัสมีการจัดแบ่งกลุ่มออกได้เป็นหลายกลุ่มและกลุ่มหนึ่งที่น่าสนใจเป็นกลุ่มที่เกิดขึ้นใหม่ ได้แก่กลุ่มของไวรัสที่เรียกว่า "มาโคร ไวรัส" ซึ่งจะทำงานและแพร่กระจายไปกับไฟล์ข้อมูลประเภทเอกสารต่างๆถูกค้นพบครั้งแรกในไฟล์เอกสารของโปรแกรมไมโครซอฟท์เวิร์ด และต่อมาพบในเอ็กเซลและเพาเวอร์พ้อยท์ด้วย ซึ่งปัจจุบันโปรแกรมสำหรับตรวจสอบและค้นหาไวรัส หลายๆตัวสามารถที่จะทำงานกับไฟล์เอกสารที่มีส่วนขยายเช่น .DOT ,.DOC เหล่านี้ได้ และปัจจุบันมีการจัดกลุ่มของไวรัสตามลักษณะการทำงานได้ดังนี้

- Common Viruses : เป็นไวรัสทั่วๆไปไม่หวังผลในการทำลายเน้นการทำให้เกิดความกลัวและสร้างความรำคาญ ง่ายต่อการตรวจสอบและกำจัด
- Program Viruses : ไวรัสที่สามารถแพร่กระจายได้เมื่อมีการเรียกใช้โปรแกรมที่มีไวรัสอยู่ให้ทำงานและจะกระจายไปสู่โปรแกรมอื่นอย่างรวดเร็ว
- Boot Viruses : ไวรัสทีสามารถแฝงตัวเองและแพร่กระจายในส่วนพื้นที่เฉพาะของดิสก์ หรือฮาร์ดดิสก์ คือในส่วนของ Boot Record หรือ Master Boot Record เช่น ไวรัส Stone เป็นต้น
- Stealth Viruses : ไวรัสที่มีความสามารถในการหลบซ่อนปิดบังซ่อนเร้นตัวเองจากการตรวจสอบได้ทำให้ยากแก่การตรวจสอบ และกำจัด
- Polymorphic Viruses : เป็นไวรัสที่มีลักษณะการทำงานหลายรูปแบบในตัวเองมีรูปแบบที่แตกต่างกันในการแพร่กระจายแต่ละครั้ง ทำให้ยากแก่การตรวจจับ
- Multipartite Viruses : ไวรัสแบบผสมที่รวมเอาการทำงานของไวรัสหลายๆแบบไว้ด้วยกัน สามารถแพร่กระจายได้ทั้งในไฟล์และโปรแกรม
- Macro Viruses : มาโครไวรัส เป็นไวรัสที่เกิดขึ้นใหม่โดยถูกสร้างขึ้นมาจากภาษามาโครของเวิร์ด (คือ Word Basics) และจะแพร่กระจายกับไฟล์เอกสารของเวิร์ด เอ็กเซลล์ หรือ เพาเวอร์พ้อยท์ เช่นไวรัสที่ชื่อ WM.CAP เป็นต้น

ไวรัสสามารถสร้างความเสียหายได้ในระดับใด

ไวรัสคอมพิวเตอร์สามารถติดไปกับโปรแกรมต่างๆที่สามารถทำงานได้เช่นเวิร์ดโปรแซสซิ่ง สเปรดชีต หรือ โปรแกรมระบบปฏิบัติการ ไวรัสสามารถติดไปกับส่วนต่างๆ ของดิสก์ หรือส่วนที่เฉพาะเจาะจงของระบบดิสก์ได้ เช่น Boot Record ได้ซึ่งมันจะถูกเรียกให้ทำงานทันทีที่มีการนำแผ่นดิสก์ที่มีไวรัสไปใช้งานหรือมีการบูตระบบให้ทำงาน และจะเริ่มกระบวนการแพร่กระจาย แต่ไวรัสคอมพิวเตอร์จะไม่สามารถสร้างความเสียหายให้เกิดขึ้นกับระบบที่เป็นฮาร์ดแวร์ได้ เช่นจอภาพหรือคีย์บอร์ด แต่บางครั้งการทำงานของไวรัสทำให้เราเข้าใจผิดพลาดว่าระบบฮาร์ดแวร์มีปัญหาที่เป็นเช่นนั้นเพราะว่าไวรัสเข้าไปทำการควบคุมโปรแกรมที่ทำหน้าที่ควบคุมการทำงานของจอภาพและคีย์บอร์ด เช่นการทำให้เกิดตัวอักษรแปลกๆ หรือตัวอักษรร่วงหล่นจากจอภาพและไวรัสจะไม่สามารถทำให้ดิสก์เสียหายได้ เพียงแต่จะอาศัยอยู่ในดิสก์เท่านั้นและยังสามารถติดกับไฟล์ได้หลายๆประเภทและมันจะทำให้เกิดความผิดพลาดในการทำงานกับโปรแกรมหรือข้อมูลนั้นๆเท่านั้น

มาตรการการป้องกัน

ในการป้องกันไวรัสไม่ให้สร้างความเสียหายให้แก่ระบบควรจะเลือกใช้วิธีใดในการป้องกันการเลือกใช้ ฮาร์ดแวร์ หรือซอฟต์แวร์อย่างไหนมีประสิทธิภาพในการป้องกันมากกว่ากัน ซึ่งควรจะมาทำการ พิจารณากันว่าในองค์กรควรจะเลือกวิธีการใด ในการป้องกันองค์กรให้ปลอดภัยจากไวรัส

เลือกใช้ฮาร์ดแวร์ หากมีการเลือกใช้ฮาร์ดแวร์ในการป้องกันไวรัสแน่นอนที่สุดหากมีการใช้ฮาร์ดแวร์ก็ต้องมีการใช้การ์ดที่ทำหน้าที่ตรวจสอบและป้องกัน ที่สำคัญที่สุดนอกจากการทำงานของการ์ดแล้วการที่การ์ดจะรู้จักไวรัสตัวใหม่ๆ การวิเคราะห์โปรแกรมต้องสงสัยและการ์ดให้ความคุ้มครองได้ในระดับไหนแล้วความเข้ากันได้กับระบบฮาร์ดแวร์ของระบบคอมพิวเตอร์ และระบบปฏิบัติการหรือโปรแกรมที่ใช้งานมีการสนับสนุนการทำงานที่เพียงพอหรือไม่เช่นการซัพพอร์ททางด้านเทคนิค การให้ข้อมูลข่าวสารใหม่ๆของไวรัสการอัพเกรดความสามารถของการ์ด ราคาของการ์ดที่จะนำมาใช้เหมาะสมกับความสามารถของการ์ดหรือไม่ถ้ามองถึงในด้านการทำงานแล้วอุปกรณ์ที่เป็นฮาร์ดแวร์และทำงานในลักษณะที่เกี่ยวข้องกับความปลอดภัย มักจะมีโปรแกรมควบคุม และจัดการการทำงานมาด้วยเสมอ ก็คือโปรแกรมไดรเวอร์ และต้องมีโปรแกรมทำงาน โปรแกรมช่วยเหลือโปรแกรมยูทิลิตี้ ซึ่งยังคงเป็นการใช้ซอฟต์แวร์ควบคุมการทำงานของฮาร์ดแวร์อยู่ดีแล้วการเลือกใช้ซอฟต์แวร์เพื่อป้องกันไวรัสที่มีอยู่ในปัจจุบันมีความปลอดภัยในระดับไหนความน่าเชื่อถือเป็นอย่างไรซึ่งโปรแกรมประเภทที่ว่าในปัจจุบันมีหลายรูปแบบให้เลือกใช้เพื่อความเหมาะสมขององค์กรหรือหน่วยงานขนาดต่างๆและเหมาะสมกับระบบปฏิบัติการหลายๆแบบให้เลือกใช้ความเข้ากันได้ของการทำงานมีสูงกว่าระบบฮาร์ดแวร์ แล้วจะเลือกใช้ตัวไหนดีสำหรับโปรแกรมป้องกันไวรัสที่โดดเด่นและรู้จักกันอย่างแพร่หลายในหมู่นักเล่นคอมพิวเตอร์ เช่น โปรแกรมที่ชื่อ SCAN จากค่าย McAfee สแกนมีความสามารถในการตรวจสอบไฟล์ข้อมูลประเภทต่างๆและตัวโปรแกรมมีขนาดเล็ก การทำงานมีทั้งการทำงานตามปกติการตรวจจับลักษณะการทำงานของไฟล์ต้องสงสัยการทำงานในหลายได้ในหลายระบบปฏิบัติการเช่น Dos Windows 3.X Window95 Window NT และความสามารถในการตรวจสอบไฟล์ที่มาจากระบบเน็ตเวิร์ค หรืออินเตอร์เน็ต ที่เรียกว่า WebScan การอัพเดตฐานข้อมูลของไวรัส (Virus Signature) และการรู้จักไวรัสตัวใหม่ๆซึ่งตรงนี้อาจเป็นจุดอ่อนของโปรแกรมตัวนี้ก็ได้เพราะมีการเปลี่ยนแปลงรุ่นของโปรแกรมที่เร็วมากและการอัพเดตฐานข้อมูลผู้ใช้ต้องดำเนินการดาวน์โหลดโปรแกรมรุ่นใหม่และทำการติดตั้งเองทั้งหมดซึ่งถ้าผู้ใช้แต่ละคนไม่หมั่นทำการอัพเดตซึ่งปกติจะทำเดือนละครั้งก็จะเป็นจุดที่ไวรัสจะเข้าโจมตีได้เช่นกัน

โปรแกรมตัวต่อไปที่นิยมไม่แพ้กันและมีชื่อเสียงคุ้นเคยกันมานานก็คือโปรแกรมตระกูล Norton Anti Virus จากค่าย Symantec โปรแกรมตัวนี้มีจุดเด่นที่เป็นจุดเข็งและเป็นหัวใจในการทำงานหลายประการเช่น การจัดการกระบวนการทำงานในรูปแบบอัตโนมัติการค้นหาไวรัสตามเวลาที่ได้ตั้งเอาไว้การอัพเดตฐานข้อมูลไวรัสที่สามารถทำได้โดยอัตโนมัติด้วยการคลิกเม้าท์เพียงปุ่มเดียวโปรแกรมจะทำการติดต่อกับเครื่อง Server ของบริษัทเพื่อทำการอัพเดตข้อมูลให้เรียกว่าการทำ "Live - Up-date" ซึ่งผู้ใช้ไม่ต้องทำการดาวน์โหลดข้อมูลด้วยตัวเองและรอการทำงานจนเสร็จและติดตั้งโปรแกรมอีกครั้งหนึ่ง การทำ Live - Up-date สามารถทำได้ตลอดเวลาเช่นตอนเที่ยงก่อนทานข้าวก็ทำเอาไว้โปรแกรมจะทำการติดตั้งโดยอัตโนมัติเมื่อกลับจากทานข้าวก็ทำการ บูตระบบให้โปรแกรมฐานข้อมูลไวรัสตัวใหม่ทำงานก็เสร็จกระบวนการซึ่งฐานข้อมูลจะมีการปรับปรุงทุกๆ 15 -30 วัน นอกจากนี้การตรวจจับไฟล์ที่ต้องสงสัยการทำงานหลังฉากก็มีประสิทธิภาพในการทำงานสูง การแจ้งเตือนทำได้ชัดเจน รวดเร็วมีข้อเสียคือโปรแกรมตรวจจับมีขนาดในหน่วยความจำที่ค่อนข้างใหญ่สำหรับเครื่องที่หน่วยความจำน้อย

นอกจากนี้ยังมีโปรแกรมที่เราไม่ค่อยรู้จักได้แก่ Dr.Solomon's PC-Cillin Cheyenen เป็นต้น สำหรับหน่วยงานหรือองค์กรขนาดใหญ่ที่มีระบบ Server ใช้งานโปรแกรมสำหรับระบบที่ว่านี้โปรแกรมที่น่าสนใจก็มี Cheyenne Inoculan ซึ่งเหมาะกับการทำงานกับระบบเน็ตเวิร์คที่เป็น Windows NT และ Windows Client มีความสามารถตรวจจับไวรัสที่ติด

มากับจดหมายอิเล็กทรอนิกส์ได้และมีการจัดการที่เกี่ยวข้องกับความปลอดภัยของระบบที่ค่อนข้างดีเช่นการที่อนุญาติให้ผู้ดูแลระบบสามารถที่จะตรวจสอบเครื่องที่ต้องสงสัยว่ามีไวรัสที่อยู่ภายในระบบได้อีกโปรแกรมที่น่าสนใจสำหรับองค์กรขนาดใหญ่ก็คือ LDVP 5.0 หรือ LanDesk Virus Protect ของบริษัทอินเทลซึ่งมีความสามารถในการทำงานที่ไม่ขึ้นกับระบบปฏิบัติการมีการจัดการที่ดีและจะมีความสามารถสูงขึ้นหากมีการทำงานร่วมกับโปรแกรมจัดการระบบที่ชื่อ LanDesk Manager จากบริษัทเดียวกัน

ระบบรักษาความปลอดภัยในคอมพิวเตอร์ (Computer Security System)

ในปัจจุบันเทคโนโลยีต่างๆ ได้มีการพัฒนาขึ้นเป็นอย่างมาก ทั้งนี้เพื่ออำนวยความสะดวกสบายให้แก่มนุษย์ซึ่งในเทคโนโลยีเหล่านี้ได้รวมไปถึงเทคโนโลยีการสื่อสารที่ทำให้ระยะทางและเวลาไม่เป็นอุปสรรคอีกต่อไปแต่ถึงแม้ว่าปัญหาเก่าๆจะหมดสิ้นไปปัญหาใหม่ที่เกิดขึ้นมากลับมีความรุนแรงมากกว่าปัญหาเดิมหลายเท่า ได้แก่ปัญหาเกี่ยวกับความปลอดภัยของระบบคอมพิวเตอร์และระบบสารสนเทศซึ่งปัจจุบันเว็บไซต์หรือองค์กรธุรกิจส่วนใหญ่จะต้องมีระบบรักษาความปลอดภัยที่มีประสิทธิภาพมากยิ่งขึ้นเพื่อป้องกันภัยคุกคามจากผู้ที่ประสงค์ร้ายต่อธุรกิจ ข้อมูลที่เป็นความลับขององค์กรหรือข้อมูลส่วนตัวของบุคคลทั่วไปที่องค์กรนั้นมีอยู่โดยเนื้อหาประกอบไปด้วย

1. แนวคิดเกี่ยวกับระบบรักษาความปลอดภัยในคอมพิวเตอร์
2. การรักษาความปลอดภัยในองค์กร
3. การรักษาความปลอดภัยบนเครือข่ายอินเตอร์เน็ต
4. การรักษาความปลอดภัยของข้อมูลส่วนบุคคล
5. แนวโน้มของระบบรักษาความปลอดภัยในอนาคต

แนวคิดเกี่ยวกับรักษาความปลอดภัยในคอมพิวเตอร์

แนวคิดเกี่ยวกับรักษาความปลอดภัยในคอมพิวเตอร์เกิดขึ้นเนื่องจากบุคคลที่ไม่ประสงค์ดีเข้ามาทำลายข้อมูลภายในระบบคอมพิวเตอร์ด้วยรูปแบบต่างๆ กันไป ไม่ว่าจะเป็นการส่งไวรัสเข้าสู่ระบบคอมพิวเตอร์ซึ่งมีผลทำให้ข้อมูลต่าง ๆที่มีอยู่นั้นเกิดความเสียหายหรือการโจรกรรมข้อมูลที่เป็นความลับซึ่งมีความสำคัญด้านการแข่งขันทางธุรกิจและความมั่นคงของชาติหรือการละเมิดข้อมูลส่วนบุคคลของผู้อื่น เป็นต้น ดังนั้นตัวบุคคลและองค์กรต่าง ๆจึงต้องมีการเพิ่มความสามารถในการรักษาความปลอดภัยให้กับระบบคอมพิวเตอร์ของตนให้มากขึ้น

ผู้ที่สามารถเจาะระบบรักษาความปลอดภัยเข้ามาได้มีอยู่ 2 ประเภท คือ Hacker และ Cracker โดยมีวิธีในการเข้าใช้ระบบหลายวิธีด้วยกันโดยทั่วไปจะเข้าสู่ระบบโดยใช้การ Log in แบบผู้ใช้โดยทั่ว ๆ ไป ข้อแตกต่างระหว่าง Hacker และ Cracker ก็คือ จุดประสงค์ของการเจาะเข้าเครื่องคอมพิวเตอร์ผู้อื่นดังนี้

Hacker คือผู้เชี่ยวชาญที่มีความรู้สามารถถอดรหัสหรือเจาะรหัสของระบบรักษาความปลอดภัยของเครื่องคอมพิวเตอร์คนอื่นได้โดยมีวัตถุประสงค์เพื่อทดสอบขีดความสามารถของระบบเท่านั้นหรืออาจจะทำในหน้าที่การงาน เช่น ผู้ที่มีหน้าที่เกี่ยวข้องกับระบบรักษาความปลอดภัยของเครือข่าย หรือองค์กรเพื่อทำการทดสอบประสิทธิภาพของระบบว่ามีจุดบกพร่องใดเพื่อแก้ไขต่อไป

Cracker ผู้เชี่ยวชาญที่มีความรู้สามารถถอดรหัสหรือเจาะรหัสของระบบรักษาความปลอดภัยของเครื่องคอมพิวเตอร์คนอื่นได้โดยมีวัตถุประสงค์เพื่อบุกรุกระบบหรือเข้าสู่เครื่องคอมพิวเตอร์คนอื่นเพื่อขโมยข้อมูลหรือทำลายข้อมูลคนอื่นโดยผิดกฎหมายโดยภัยคุกคามที่เกิดขึ้นกับระบบรักษาความปลอดภัยของคอมพิวเตอร์สามารถแบ่งออกได้ 5 รูปแบบ ดังนี้

1. ภัยคุกคามแก่ระบบเป็นภัยคุกคามจากผู้ไม่ประสงค์ที่เข้ามาทำการปรับเปลี่ยน แก้ไขหรือลบไฟล์ข้อมูลสำคัญภายในระบบคอมพิวเตอร์แล้วส่งผลให้เกิดความเสียหายต่อระบบคอมพิวเตอร์ ทำให้ไม่สามารถใช้งานได้ตัวอย่างเช่น Cracker แอบเจาะเข้าไปในระบบเพื่อลบไฟล์ระบบปฏิบัติการเป็นต้น

2. ภัยคุกคามความเป็นส่วนตัวเป็นภัยคุกคามที่ Cracker เข้ามาทำการเจาะข้อมูลส่วนบุคคลหรือติดตามร่องรอยพฤติกรรมของผู้ใช้งาน แล้วส่งผลให้เกิดความเสียหายขึ้นตัวอย่างเช่น การใช้โปรแกรมสปาย (Spyware) ติดตั้งบนเครื่องคอมพิวเตอร์ของบุคคลอื่นและส่งรายงานพฤติกรรมของผู้ใช้ผ่านทางระบบเครือข่ายหรือทางอีเมล์เป็นต้น

3. ภัยคุกคามต่อทั้งผู้ใช้และระบบเป็นภัยคุกคามที่ส่งผลเสียหายให้แก่ผู้ใช้งานและเครื่องคอมพิวเตอร์เป็นอย่างมากตัวอย่างเช่น ใช้ Java Script หรือ Java Applet ทำการล็อคเครื่องคอมพิวเตอร์ไม่ให้ทำงานหรือบังคับให้ผู้ใช้งานปิดโปรแกรมบราวเซอร์ขณะใช้งานอยู่ เป็นต้น

4. ภัยคุกคามที่ไม่มีเป้าหมายเป็นภัยคุกคามที่ไม่มีเป้าหมายที่แน่นอน เพียงแต่ต้องการสร้างจุดสนใจโดยปราศจากความเสียหายที่จะเกิดขึ้น ตัวอย่างเช่นส่งข้อความหรืออีเมล์มารบกวนผู้ใช้งานในระบบหลาย ๆ คน

5. ภัยคุกคามที่สร้างความรำคาญเป็นภัยคุกคามที่สร้างความรำคาญ โดยปราศจากความเสียหายที่จะเกิดขึ้นตัวอย่างเช่น แอบเปลี่ยนคุณลักษณะ (Property) รายละเอียดสีของเครื่องคอมพิวเตอร์จากเดิมที่เคยกำหนดไว้โดยไม่ได้รับอนุญาต เป็นต้น

จากความสำคัญของข้อมูลและภัยคุกคามต่าง ๆเหล่านี้ทำให้สามารถแบ่งลักษณะการรักษาความปลอดภัยบนคอมพิวเตอร์ตามลักษณะการใช้งานได้ 3 ลักษณะ คือ การรักษาความปลอดภัยในองค์กรการรักษาความปลอดภัยบนเครือข่ายอินเตอร์เน็ตและการรักษาความปลอดภัยของข้อมูลส่วนบุคคล

1. การรักษาความปลอดภัยในองค์กร

บุคคลผู้ไม่ประสงค์ดีต่อองค์กรมีอยู่ 2 จำพวก คือผู้ที่ทำงานอยู่ภายในองค์กรเองและผู้ที่เป็นบุคคลภายนอกการรักษาความปลอดภัยของข้อมูลและระบบคอมพิวเตอร์ภายในองค์กรจึงต้องป้องกันผู้บุกรุกทั้ง 2 จำพวกนี้ให้ได้ โดยวิธีการที่บุคคลเหล่านี้ใช้มีด้วยกันหลายวิธีแต่สามารถแบ่งเป็นประเภทได้ 2 ประเภท คือ การบุกรุกทางกายภาพ (เข้าถึงระบบได้โดยตรง) เช่น การเข้ามาคัดลอกข้อมูลใส่แผ่นดิสก์กลับไปการขโมยฮาร์ดดิสก์ออกไป การสร้างความเสียหายโดยตรงกับฮาร์ดแวร์ต่าง ๆหรือการติดตั้งซอฟต์แวร์ ที่ดักจับ Password ของผู้อื่นแล้วส่งไปให้บุกรุก เป็นต้น ประเภทที่สองคือการบุกรุกทางเครือข่ายคอมพิวเตอร์ เช่นการปล่อยไวรัสคอมพิวเตอร์เข้ามาทำลายระบบหรือขโมยข้อมูลการเจาะเข้ามาทางรอยโหว่ของระบบปฏิบัติการโดยตรงเพื่อขโมย หรือข้อมูล Password เป็นต้น ระบบรักษาความปลอดภัยที่ใช้ป้องกันการบุกรุกทางกายภาพที่นิยมใช้ คือ ระบบ Access Control ส่วนระบบที่ป้องกันการบุกรุกทางเครือข่าย คือ Firewall นอกจากนี้ยังใช้วิธีการ Backup ข้อมูลที่สำคัญเก็บเอาไว้เพื่อใช้ในกรณีที่ข้อมูลเกิดความเสียหายจากสาเหตุใด ๆ ก็ตาม

2.1 Access Control

Access Control คือระบบควบคุมการเข้าใช้งานเป็นวิธีการที่คิดค้นขึ้นมาเพื่อป้องกันการโจรกรรมข้อมูลจากบุคคลที่ไม่มีสิทธิในการเข้าใช้ข้อมูลหรือระบบ (Unauthorized) โดยผู้ที่สามารถเข้าใช้ระบบโดยผ่านระบบ Access Control นี้ได้จะต้องได้รับการอนุญาตหรือได้รับสิทธิในการเข้าใช้งานก่อน (Authorize) ซึ่งแต่ละบุคคลจะมีสิทธิในการเข้าใช้ระบบไม่เท่ากัน เช่นบางคนอาจได้แค่เรียกใช้ข้อมูลเท่านั้น แต่บางคนสามารถแก้ไขข้อมูลได้ เป็นต้นเมื่อได้รับสิทธิแล้วต้องการเข้าใช้ระบบจะต้องมีการพิสูจน์แล้วปรากฏว่าบุคคลผู้นั้นเป็นผู้ที่ได้รับสิทธิจริงจึงจะสามารถเข้าใช้งานได้ ระบบควบคุมการเข้าใช้งานที่ได้รับความนิยมในปัจจุบันนี้ แบ่งออกได้เป็น 3 รูปแบบดังนี้

ชื่อผู้ใช้และรหัสผ่าน (User Name and Password) ชื่อผู้ใช้ (User Name, User ID) คือ ตัวอักษรหรือตัวเลขซึ่งบ่งบอกว่าผู้ใช้เป็นใคร ส่วน รหัสผ่าน (Password) เป็นรหัสเฉพาะเพื่อเข้าใช้ระบบ ซึ่งเปรียบเสมือนกุญแจ (Key) ที่ใช้เปิดประตู การจะเข้าใช้คอมพิวเตอร์ที่มีระบบควบคุมการเข้าใช้งานในลักษณะนี้ผู้ใช้จะต้องบอกชื่อผู้ใช้ซึ่งเป็นชื่อที่ขึ้นทะเบียนไว้กับคอมพิวเตอร์ระบบจะตรวจสอบข้อมูลของผู้ใช้เหล่านี้จากบัญชีที่ผู้ใช้กรอกข้อมูลไว้เมื่อเริ่มต้นโดยชื่อผู้ใช้จะไม่ซ้ำกันทำให้คอมพิวเตอร์สามารถบ่งบอกความแตกต่างของผู้ใช้แต่ละคนได้หลังจากกรอกชื่อข้อมูล (User Name) แล้วต้องการป้อนรหัสผ่าน (Password) ด้วยหากชื่อผู้ใช้และรหัสผ่านไม่ตรงชื่อผู้ใช้และรหัสผ่านที่มีอยู่ในทะเบียนระบบจะปฏิเสธการเข้าใช้งาน

โดยทั่วไปคอมพิวเตอร์จะอนุญาตให้ผู้ใช้ตั้งชื่อผู้ใช้และรหัสผ่านได้ด้วยตนเองซึ่งรหัสผ่านที่มีประสิทธิภาพในการป้องกันการเข้าใช้นั้นต้องประกอบไปด้วยลักษณะ 2 ประการ คือ

1. จำนวนของตัวอักษรหรือตัวเลขที่ประกอบกันเป็นรหัสผ่านนั้นต้องมีความยาวที่เหมาะสมคือ ไม่ต่ำกว่า 6 ตัวอักษร

2. รหัสผ่านที่ตั้งนั้นไม่ควรจะเป็นคำที่ผู้อื่นคาดเดาได้ง่าย เช่น วันเกิด หรือชื่อเล่น เป็นต้น

Possessed Object เป็นรูปแบบหนึ่งในการควบคุมการเข้าใช้ระบบที่นิยมกันมากในปัจจุบันการเข้าใช้คอมพิวเตอร์ที่มีระบบเช่นนี้ต้องใช้กุญแจ (Key) ซึ่งกุญแจในที่นี้จะหมายถึงวัตถุที่คอมพิวเตอร์อนุญาตให้ใช้ในการเข้าระบบได้เช่นบัตร ATM หรือ Keycard กุญแจเหล่านี้จะมี Personal Identification Number (PIN) หรือ รหัสตัวเลขซึ่งบ่งบอกว่ากุญแจเหล่านั้นเป็นของใครและต้องมีรหัสผ่านคอยควบคุมการเข้าใช้ระบบ เช่น บัตร ATM เป็นตัวอย่างที่แสดงการทำงานของ PIN ได้ดีที่สุด การใช้ บัตร ATM ต้องกดรหัสตัวเลข 4 ตัวเพื่อใช้งาน ซึ่งตัวเลขเหล่านี้เป็นรหัสส่วนบุคคล เป็นต้น

อุปกรณ์ Biometric เป็นอุปกรณ์รักษาความปลอดภัยซึ่งใช้ลักษณะส่วนบุคคลเป็นรหัสผ่าน เช่น อุปกรณ์ตรวจสอบลายนิ้วมือ ขนาดของฝ่ามือ หรือดวงตา อุปกรณ์ลักษณะนี้จะแปลงลักษณะเฉพาะส่วนบุคคลเป็นรหัสตัวเลข (Digital Code) เพื่อเปรียบเทียบรหัสตัวเลขนั้นกับข้อมูลที่เก็บไว้ หากไม่ตรงกันคอมพิวเตอร์จะปฏิเสธการเข้าใช้ระบบ

อุปกรณ์สแกนลายนิ้วมือเป็นตัวอย่างของอุปกรณ์ Biometric ที่ใช้กันอย่างแพร่หลายในปัจจุบันเครื่องสแกนลายนิ้วมือจะใช้การตรวจสอบความโค้งและรอยบากของลายนิ้วมือซึ่งแต่ละคนจะมีลักษณะไม่เหมือนกัน ทำให้ตรวจสอบได้ว่าเจ้าของลายนิ้วมือเป็นใครมีสิทธิ์เข้าใช้ระบบหรือไม่และที่สำคัญอุปกรณ์ชนิดนี้มีราคาถูกจึงได้รับความนิยมอย่างมาก

ตัวอย่างของอุปกรณ์ Biometric แบบอื่น ๆ ได้แก่ Hand Geometry System, Face Recognition System, Voice Verification System, Signature Verification System หรือ Iris Verification System เป็นต้น

อุปกรณ์ Biometric นับว่าเป็นอุปกรณ์ที่ป้องกันการเข้าใช้ระบบที่มีประสิทธิภาพมากที่สุดในปัจจุบัน เนื่องจากการใช้ลักษณะเฉพาะตัวของแต่ละบุคคลเป็นกุญแจในการเข้าใช้ระบบซึ่งยากที่จะลอกเลียนแบบแต่การใช้ลักษณะเฉพาะตัวเป็นกุญแจเช่นนี้จะเกิดปัญหาเมื่อบุคคลเหล่านั้นประสบอุบัติเหตุหรือมีเหตุการณ์ซึ่งทำให้ลักษณะเฉพาะเหล่านั้นเปลี่ยนแปลงไปผู้ใช้จะไม่สามารถเข้าใช้ระบบได้ เช่น มีดบาดนิ้วมือทำให้ลายนิ้วมือเปลี่ยนไปหรือการผ่าตัดตาซึ่งทำให้มีความเปลี่ยนแปลงกับกระจกตา เป็นต้น

นอกจากระบบควบคุมการเข้าใช้ข้อมูลดังกล่าวแล้วยังสามารถเลือกใช้ซอฟต์แวร์และผู้ให้บริการที่มีความสามารถในการตรวจจับและป้องกันการบุกรุกได้ ดังต่อไปนี้

ซอฟต์แวร์ตรวจจับการบุกรุก (Intrusion Detection Software : IDS)

ซอฟต์แวร์ตรวจจับการบุกรุก จะคอยจับตาดูระบบและทรัพยากรของเครือข่ายแล้วรายงานให้ผู้ดูแลรักษาความปลอดภัยทราบเมื่อมีความเป็นไปได้ว่ามีผู้บุกรุกเข้ามาแล้วตัวอย่างกิจกรรมที่น่าสงสัยว่ามีผู้บุกรุกเข้ามาเช่น มีผู้พยายาม Log in เข้าใช้ข้อมูล แต่เข้าไม่ได้หลาย ๆ ครั้ง มีการเข้าใช้ระบบในช่วงเวลาที่ผิดปกติเป็นต้น การใช้ IDS นี้เป็นการเพิ่มการป้องกันอีกชั้นหนึ่งในกรณีที่ผู้บุกรุกได้ผ่านระบบรักษาความปลอดภัยชั้นนอก (เช่น รหัสผ่าน ไฟร์วอลล์ เป็นต้น) เข้ามาแล้ว

ผู้ให้บริการจัดการความปลอดภัย (Management Security Service Provider : MSSP)

ผู้ให้บริการจัดการความปลอดภัยจะคอยจับตาดูผู้บุกรุกและดูแลรักษาฮาร์ดแวร์และซอฟต์แวร์รักษาความปลอดภัยของเครือข่ายให้เหมาะสำหรับองค์กรขนาดเล็กถึงขนาดกลางเนื่องจากต้นทุนในการจ้างผู้เชี่ยวชาญด้านการรักษาความปลอดภัยบนเครือข่ายเพื่อป้องกันการดำเนินงานทางธุรกิจอาจสูงเกินไป

การป้องกันและกำจัดไวรัสคอมพิวเตอร์

ไวรัสคอมพิวเตอร์ (Virus Computer) เป็นโปรแกรมชนิดหนึ่งที่ถูกเขียนขึ้นมาเพื่อก่อให้เกิดความเสียหายกับเครื่องคอมพิวเตอร์และข้อมูลภายในเครื่องโดยไวรัสนี้สามารถสำเนาตัวเองและไปฝังตัวหรือซ่อนตัวอยู่ภายในหน่วยความจำของเครื่องคอมพิวเตอร์ร่วมกับโปรแกรมอื่นที่มีอยู่แล้วได้เมื่อผู้ใช้คอมพิวเตอร์เรียกใช้งานโปรแกรมที่ถูกไวรัสฝังตัวรวมอยู่ด้วยโปรแกรมไวรัสก็จะทำงานทันทีตามวัตถุประสงค์ของผู้เขียนโปรแกรมไวรัส เช่นเมื่อเรียกใช้โปรแกรมหรือไฟล์ที่มีไวรัสฝังตัวอยู่ จะทำให้ไฟล์นั้นถูกลบทิ้งหรือจะทำให้ไฟล์ระบบถูกทำลาย หรืออาจทำให้เครื่องคอมพิวเตอร์หยุดทำงานเป็นต้น

จุดประสงค์ของไวรัสจะแตกต่างกันไปตามแต่ผู้เขียนไวรัสต้องการ เช่นให้ฝังตัวเพื่อเพิ่มเนื้อที่ในฮาร์ดดิสก์ ให้ลบไฟล์ที่มีนามสกุล .EXE ทิ้งให้ย้ายไฟล์จากที่หนึ่งไปยังอีกที่หนึ่ง ให้ปรากฏข้อความบางข้อความให้ทำลายไฟล์ที่สำคัญทันทีเมื่อถึงวันที่ที่กำหนดไว้ เป็นต้นซึ่งส่วนใหญ่มุ่งเน้นไปที่การก่อความเสียหายให้กับเครื่องคอมพิวเตอร์

ช่องทางการกระจายของไวรัสสามารถมาจากหลายช่องทาง ได้แก่

1. การใช้งานแผ่นดิสก์และคอมพิวเตอร์ร่วมกัน ในกรณีที่ผู้ใช้โอนไฟล์ข้อมูลจากเครื่องคอมพิวเตอร์ที่ติดไวรัสไปยังแผ่นดิสก์ (Floppy Disk) แสดงว่าไวรัสได้ติดมากับแผ่นดิสก์ดังกล่าวแล้วและเมื่อผู้ใช้นำแผ่นดิสก์ดังกล่าวไปใช้กับ

เครื่องคอมพิวเตอร์เครื่องอื่น ๆก็จะทำให้เครื่องคอมพิวเตอร์เหล่านั้นติดไวรัสไปด้วย ดังนั้นก่อนจะเรียกใช้ข้อมูลจากแผ่นดิสก์ควรตรวจสอบแผ่นดิสก์ก่อนว่ามีไฟล์ที่ติดไวรัสอยู่หรือไม่หากพบว่ามี ให้ทำการกำจัดด้วยโปรแกรมกำจัดไวรัส เช่น McAfee VirusScan หรือ Norton AntiVirus เป็นต้น แต่ถ้าโปรแกรมกำจัดไวรัสดังกล่าว ไม่สามารถกำจัดไวรัสชนิดนั้นได้ แสดงว่าโปรแกรมไม่รู้จักไวรัสชนิดนั้น ผู้ใช้จะต้องเข้าไปอัพเดท (Update) ชนิดของไวรัสจากเว็บไซต์ของโปรแกรมนั้นบนอินเตอร์เน็ต

2. การทำงานบนระบบเครือข่าย ในกรณีที่เครื่องคอมพิวเตอร์มีการเชื่อมต่อกับระบบเครือข่าย เช่น เครือข่าย LAN ถึงแม้ว่าเครื่องคอมพิวเตอร์ของผู้ใช้เครื่องใดเครื่องหนึ่งไม่ติดไวรัสแต่หากมีการเรียกใช้ข้อมูลจากเครื่องอื่นที่ติดไวรัสไวรัสก็สามารถสำเนาตัวเองแนบมาพร้อมกับข้อมูลที่เรียกใช้นั้นได้และทำให้เครื่องคอมพิวเตอร์เครื่องนั้นติดไวรัสได้ในที่สุด ดังนั้นการใช้งานเครื่องคอมพิวเตอร์ที่เชื่อมต่ออยู่บนเครือข่ายผู้ใช้ควรเพิ่มความระมัดระวังในการเปิดการแชร์ข้อมูล (Data Sharing) เพื่อการใช้งานร่วมกันให้มากยิ่งขึ้น

3. การคัดลอกข้อมูล โปรแกรมหรือเกมจากเครื่องคอมพิวเตอร์ที่ติดไวรัสก็จะทำให้ไวรัสสำเนาตัวเองมากับสื่อที่ใช้ในการคัดลอกและเมื่อผู้ใช้โอนไฟล์ที่คัดลอกมาไว้ในเครื่องคอมพิวเตอร์ของตนไวรัสก็จะสำเนาตัวเองลงมาที่เครื่องคอมพิวเตอร์ของผู้ใช้เช่นเดียวกัน ดังนั้นการคัดลอกข้อมูลหรือโปรแกรมใด ๆควรตรวจสอบก่อนว่าไฟล์ข้อมูลหรือโปรแกรมที่ต้องการนั้นติดไวรัสหรือไม่

4. การดาวน์โหลดไฟล์การรับไฟล์ที่แนบมากับอีเมล์ กรณีที่เครื่องคอมพิวเตอร์ทั้งที่เป็นแบบ Stand-alone และเชื่อมต่ออยู่บนระบบเครือข่าย ซึ่งมีการเชื่อมต่อกับเครือข่ายอินเตอร์เน็ตมีการดาวน์โหลดไฟล์หรือรับอีเมล์ซึ่งแนบไฟล์ที่ติดไวรัสมาด้วยจะทำให้เครื่องคอมพิวเตอร์เครื่องนั้นติดไวรัสที่มากับไฟล์ได้ ดังนั้นก่อนการดาวน์โหลดไฟล์ข้อมูลและรับไฟล์ข้อมูลที่แนบมากับอีเมล์ควรตรวจสอบว่ามีไวรัสมาด้วยหรือไม่ปัจจุบันเว็บไซต์ผู้ให้บริการรับ-ส่ง อีเมล์ได้จัดเตรียมเครื่องมือตรวจสอบไวรัสในไฟล์ที่แนบมากับอีเมล์ซึ่งเพิ่มความสะดวกให้กับผู้ใช้เป็นอย่างมาก

อาการของเครื่องคอมพิวเตอร์เมื่อติดไวรัส อาการที่บ่งชี้ให้เห็นว่าเครื่องคอมพิวเตอร์ติดไวรัส อาจมีดังนี้

1. เครื่องทำงานช้าผิดปกติ
2. พื้นที่ในหน่วยความจำมีขนาดเล็กลงผิดปกติ
3. ไฟล์ข้อมูลมีขนาดใหญ่ผิดปกติ
4. ฮาร์ดดิสก์มีพื้นที่ลดลงอย่างไม่ทราบสาเหตุ
5. ใช้เวลาในการเรียกใช้โปรแกรมนานเกินไป
6. เครื่องคอมพิวเตอร์หยุดการทำงาน (Hang) โดยไม่ทราบสาเหตุ
7. บูทเครื่องจากฮาร์ดดิสก์ไม่ได้
8. เปิดไฟล์ข้อมูลไม่ได้
9. เปิดไฟล์ได้แต่เป็นภาษาแปลกๆ
10. ไม่สามารถเรียกใช้โปรแกรมได้
11. เกิดอาการแปลก ๆตามคำสั่งของโปรแกรมไวรัส เช่น ปรากฏข้อความแปลก ๆ บนจอภาพ เป็นต้น

การป้องกันไวรัสไม่มีวิธีการใดที่จะรับประกันได้แน่นอนว่าระบบเครือข่ายและคอมพิวเตอร์จะปลอดภัยจากไวรัส แต่การระมัดระวังในการใช้งานคอมพิวเตอร์จะช่วยลดโอกาสการติดไวรัสได้การป้องกันไม่ให้คอมพิวเตอร์ติดไวรัสมีด้วยกันหลายวิธี ดังนี้

1. ทุกครั้งที่นำซอฟต์แวร์ที่ไม่ทราบแหล่งที่ผลิตหรือได้รับแจกฟรีมาใช้ต้องตรวจสอบว่าปลอดไวรัสอย่างแน่นอนก่อนนำไปใช้เสมอ
2. ควรตรวจสอบทั้งฮาร์ดแวร์และซอฟต์แวร์อย่างสม่ำเสมออย่างน้อยวันละ 1 ครั้ง
3. เตรียมแผ่นที่ไม่ได้ติดไวรัสไว้สำหรับบูทเครื่องเมื่อถึงคราวจำเป็น
4. ควรสำรองข้อมูลไว้เสมอ
5. พยายามสังเกตสิ่งผิดปกติที่เกิดขึ้นกับเครื่องอย่างสม่ำเสมอ เช่น การทำงานที่ช้าลงขนาดของไฟล์ใหญ่ขึ้น ไดร์ฟมีเสียงผิดปกติ หรือหน้าจอแสดงผลแปลก ๆ
6. ไม่นำแผ่นดิสก์ไปใช้กับเครื่องคอมพิวเตอร์อื่น ถ้ายังไม่ได้ปิดแถบป้องกันการบันทึก (Write Protect)
7. ควรแยกแผ่นโปรแกรมและแผ่นข้อมูลออกจากกันโดยเด็ดขาด
8. ไม่อนุญาตให้คนอื่นมาเล่นเครื่องคอมพิวเตอร์โดยปราศจากการควบคุมอย่างใกล้ชิด
9. ควรมีโปรแกรมป้องกันไวรัสใช้ตรวจสอบและป้องกัน
10. ควรใช้ฮาร์ดแวร์ป้องกันไวรัส

การตรวจสอบและกำจัดไวรัส ผู้ใช้สามารถตรวจสอบและกำจัดไวรัสได้ด้วยซอฟต์แวร์ Anti-virus ซึ่งจัดว่าเป็นซอฟต์แวร์อรรถประโยชน์ที่มีขายทั่วไปหรือผู้ใช้อาจทำการติดตั้งการ์ดป้องกันไวรัส ที่เรียกว่า “Anti Virus Card (AVC)” ก็ได้

การใช้ซอฟต์แวร์ Anti-virusโปรแกรมป้องกันไวรัสมีมากมายหลายชนิดโดยผู้ผลิตแต่ละรายพยายามสร้างเอกลักษณ์ให้แก่โปรแกรมของตน แต่ทุก ๆโปรแกรมก็มีหน้าที่หลักเหมือนกันคือการป้องกันและกำจัดไวรัสที่เข้าโจมตีเครื่องคอมพิวเตอร์ ดังนั้น ซอฟต์แวร์จากทุก ๆค่ายจะมีส่วนที่ทำงานเหมือนกันคือการตรวจหารูปแบบภายในไฟล์หรือหน่วยความจำของเครื่องคอมพิวเตอร์ของผู้ใช้เพื่อบ่งชี้ว่ามีส่วนใดที่อาจจะมีไวรัสแฝงตัวอยู่ผลิตภัณฑ์ Anti-virus เหล่านี้จะมีการเก็บข้อมูลประวัติของไวรัสแต่ละตัวไว้ (บางครั้งเรียกว่า “Signatures”) เพื่อใช้เป็นต้นแบบในการค้นหาซึ่งผู้ผลิตซอฟต์แวร์จะเป็นผู้ทำการรวบรวมและจัดเตรียมข้อมูลประวัติของไวรัสซอฟต์แวร์ Anti-virus ที่ได้รับความนิยมในปัจจุบันได้แก่ McAfee VirusScan และ Norton AntiVirus โดยที่ McAfee VirusScan จะสามารถตรวจสอบไฟล์ข้อมูลประเภทต่าง ๆและกำจัดไวรัสที่ติดมากับไฟล์ได้ โปรแกรมมีขนาดเล็กติดตั้งได้ง่ายอีกทั้งยังสามารถทำงานได้บนระบบปฏิบัติการชนิดใดก็ได้นอกจากนี้ยังสามารถตรวจสอบไฟล์ที่มาจากระบบเครือข่ายโดยเฉพาะเครือข่ายอินเตอร์เน็ตได้อีกด้วย แต่ผู้ใช้ที่เลือกใช้ McAfee VirusScan จะต้องอัพเดทชนิดของไวรัสให้เป็นปัจจุบันเสมอ โดยการดาวน์โหลดโปรแกรม McAfee VirusScan ตัวใหม่ ที่ได้รับการอัพเดทแล้วจากอินเตอร์เน็ตมาติดตั้งที่เครื่องคอมพิวเตอร์เป็นระยะ เนื่องจากไวรัสชนิดใหม่ ๆเกิดขึ้นรวดเร็วมาก หากเป็น McAfee VirusScan รุ่นเก่าจะไม่รู้จักและไม่สามารถกำจัดไวรัสชนิดใหม่ได้สำหรับ Norton AntiVirus สามารถตรวจสอบไฟล์ข้อมูลได้ว่ามีไวรัสหรือไม่สามารถค้นหาไวรัสตามเวลาที่กำหนดไว้ได้เช่นเดียวกันแต่โปรแกรมชนิดนี้จะมีข้อดีในส่วนของการอัพเดทชนิดของไวรัสที่ผู้ใช้ไม่ต้องดาวน์โหลดโปรแกรมมาติดตั้งใหม่ เพียงแต่ผู้ใช้เลือกคำสั่ง “Live Update” โปรแกรมจะทำการติดต่อกับเครื่องแม่ข่ายของบริษัทเพื่ออัพเดทข้อมูลไวรัสชนิดใหม่ให้โดยอัตโนมัตินับว่าเป็นการใช้งานที่สะดวกอย่างมาก แต่ข้อเสียของ Norton AntiVirus คือโปรแกรมมีขนาดใหญ่ต้องใช้เนื้อที่ในหน่วยความจำค่อนข้างมาก

ในปัจจุบันมีการตรวจพบไวรัสชนิดใหม่ ๆอยู่เป็นประจำ ดังนั้นประสิทธิภาพของซอฟต์แวร์ Anti-virus จึงขึ้นอยู่กับการที่เครื่องคอมพิวเตอร์นั้นจะต้องมีข้อมูลประวัติของไวรัสล่าสุดอยู่ตลอดเวลาเพื่อให้ซอฟต์แวร์ Anti-virus ตรวจพบไวรัส

ชนิดล่าสุดในเครื่องคอมพิวเตอร์ได้ ดังนั้นสิ่งสำคัญที่สุดก็คือผู้ใช้จะต้องปรับปรุงให้ข้อมูลประวัติไวรัสในเครื่องคอมพิวเตอร์ของตนทันสมัยอยู่ตลอดเวลา

- *การใช้ Anti Virus Card* เป็นอุปกรณ์คอมพิวเตอร์ชนิดหนึ่งที่มีลักษณะเป็นการ์ด เสียบบนเมนบอร์ด (Main Board) ทำหน้าที่ในการตรวจจับไวรัสที่จะมาฝังตัวในหน่วยความจำของเครื่องคอมพิวเตอร์หากพบว่ามีไวรัสก็จะทำลายทันทีพร้อมทั้งทำการซ่อมแซมส่วนที่ถูกทำลายให้กลับสู่สภาพเดิม แต่การใช้การ์ด Anti Virus ผู้ใช้จะต้องคอยอัพเดทข้อมูลไวรัสชนิดต่าง ๆเช่นเดียวกับการใช้ซอฟต์แวร์ป้องกันไวรัส

บทสรุป

แต่ละระบบก็มีจุดเด่นและจุดด้อยที่แตกต่างกันหากเป็นองค์กรที่มีขนาดค่อนข่างใหญ่ มีการใช้ระบบปฏิบัติการหลายๆตัวแล้วทางเลือกที่ดีน่าจะเป็นการเลือกใช้ซอฟท์แวร์ป้องกันที่สามารถจัดการระบบมีความสามารถในการทำงานกับระบบเน็ตเวิร์คได้และการใช้โปรแกรมที่ถูกต้องตามกฎหมายก็ยังเป็นการประหยัดงบประมาณมากกว่าการใช้ระบบที่เป็นฮาร์ดแวร์เพราะระบบที่เป็นฮาร์ดแวร์ใช้ได้กับเครื่องใดเครื่องหนึ่งเท่านั้นต้องมีการถอดประกอบเครื่องและติดตั้งโปรแกรมควบคุมจึงสามารถทำงานได้นอกจากนี้ในปัจจุบันก็ยังไม่สนับสนุนการทำงานร่วมกับระบบเน็ตเวิร์คด้วยถึงแม้จะมีการติดตั้งที่ตัว Server ก็ตามการทำงานก็ยังไม่เด่นนัก ในด้านความเข้ากันได้กับระบบปฏิบัติการสำหรับเครื่องที่ทำงานเป็น Stand alone ในสำนักงานการใช้โปรแกรมจำพวก Scan หรือ Norton Anti Virus ก็ดูจะมีประสิทธิภาพมากกว่า เมื่อเทียบกันทั้งในด้านราคาและความง่ายในการใช้งาน และสำหรับเครื่องที่มีอยู่ในปัจจุบันการใช้งาน Norton Anti Virus ก็น่าจะเป็นทางเลือกที่ดีกว่าและไม่น่าจะเป็นปัญหากับเรื่องหน่วยความจำในปัจจุบัน

การใช้งานอินเทอร์เน็ตและการสืบค้น

ระบบอินเตอร์เน็ต

อินเทอร์เน็ต (Internet) หมายถึง เครือข่ายคอมพิวเตอร์ขนาดใหญ่ ที่มีการเชื่อมต่อระหว่างเครือข่ายหลายๆ เครือข่ายทั่วโลก โดยใช้ภาษาที่ใช้สื่อสารกันระหว่างคอมพิวเตอร์ที่เรียกว่า โพรโทคอล (Protocol) ผู้ใช้เครือข่ายนี้สามารถสื่อสารถึงกันได้ในหลายๆ ทาง อาทิเช่น อีเมล เว็บบอร์ด และสามารถสืบค้นข้อมูลและข่าวสารต่างๆ รวมทั้งคัดลอกแฟ้มข้อมูลและโปรแกรมมาใช้ได้

วิวัฒนาการของอินเทอร์เน็ต

อินเทอร์เน็ตในปัจจุบัน ถูกพัฒนามาจากโครงการวิจัยทางการทหารของกระทรวงกลาโหมของประเทศสหรัฐอเมริกา คือ Advanced Research Projects Agency (ARPA) ในปี พ.ศ. 2512 โครงการนี้เป็นการวิจัยเครือข่ายเพื่อการสื่อสารของการทหารในกองทัพอเมริกา หรืออาจเรียกสั้นๆ ได้ว่า ARPA Net ในปี พ.ศ. 2513 ARPA Net ได้มีการพัฒนาเพิ่มมากขึ้นโดยการเชื่อมโยงเครือข่ายร่วมกับมหาวิทยาลัยชั้นนำของอเมริกา คือ มหาวิทยาลัยยูทาห์ มหาวิทยาลัยแคลิฟอร์เนียที่ซานตาบาบารา มหาวิทยาลัยแคลิฟอร์เนียที่ลอสแองเจลิส และสถาบันวิจัยของมหาวิทยาลัยสแตนฟอร์ด และหลังจากนั้นเป็นต้นมาก็มีการใช้ อินเทอร์เน็ตกันอย่างแพร่หลายมากขึ้น

สำหรับในประเทศไทย อินเทอร์เน็ตเริ่มมีการใช้ครั้งแรกในปี พ.ศ. 2530 ที่มหาวิทยาลัยสงขลานครินทร์ โดยได้รับความช่วยเหลือจากโครงการ IDP (The International Development Plan) เพื่อให้มหาวิทยาลัยสามารถติต่อสื่อสารทางอีเมลกับมหาวิทยาลัยเมลเบิร์นในออสเตรเลียได้ ได้มีการติดตั้งระบบอีเมล์ขึ้นครั้งแรก โดยผ่านระบบโทรศัพท์ ความเร็วของโมเด็มที่ใช้ในขณะนั้นมีความเร็ว 2,400 บิต/วินาที จนกระทั่งวันที่ 2 มิถุนายน พ.ศ. 2531 ได้มีการส่งอีเมลฉบับแรกที่ติดต่อระหว่างประเทศไทยกับมหาวิทยาลัยเมลเบิร์น มหาวิทยาลัยสงขลานครินทร์จึงเปรียบเสมือนประตูทางผ่าน (Gateway) ของไทยที่เชื่อมต่อไปยังออสเตรเลียในขณะนั้น

ในปี พ.ศ. 2533 ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) ได้เชื่อมต่อคอมพิวเตอร์ของสถาบันการศึกษาของรัฐ โดยมีชื่อว่า เครือข่ายไทยสาร (Thai Social/Scientific Academic and Research Network : ThaiSARN) ประกอบด้วย มหาวิยาลัยสงขลานครินทร์ จุฬาลงกรณ์มหาวิทยาลัย สถาบันเทคโนโลยีแห่งเอเชีย (AIT) มหาวิทยาลัยธรรมศาสตร์ มหาวิทยาลัยเกษตรศาสตร์ เพื่อให้บริการอินเทอร์เน็ตภายในประเทศ เพื่อการศึกษาและวิจัย

ในปี พ.ศ. 2538 ได้มีการบริการอินเทอร์เน็ตเชิงพาณิชย์ขึ้น เพื่อให้บริการแก่ประชาชน และภาคเอกชนต่างๆ ที่ต้องการเชื่อมต่ออินเทอร์เน็ต โดยมีบริษัทอินเทอร์เน็ตไทยแลนด์ (Internet Thailand) เป็นผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider: ISP) เป็นบริษัทแรก เมื่อมีคนนิยมใช้อินเทอร์เน็ตเพิ่มมากขึ้น บริษัทที่ให้บริการอินเทอร์เน็ตจึงได้ก่อตั้งเพิ่มขึ้นอีกมากมาย

ความสำคัญของอินเทอร์เน็ต

ในปัจจุบันอินเทอร์เน็ตมีบทบาทและมีความสำคัญต่อชีวิตประจำวันของคนเราเป็นอย่างมาก เพราะทำให้วิถีชีวิตเราทันสมัยและทันเหตุการณ์อยู่เสมอ เนื่องจากอินเทอร์เน็ตจะมีการเสนอข้อมูลข่าวปัจจุบัน และสิ่งต่าง ๆ ที่เกิดขึ้นให้ผู้ใช้ทราบเปลี่ยนแปลงไปทุกวัน สารสนเทศที่เสนอในอินเทอร์เน็ตจะมีมากมายหลายรูปแบบเพื่อสนองความสนใจและความต้องการของผู้ใช้ทุกกลุ่ม อินเทอร์เน็ตจึงเป็นแหล่งสารสนเทศสำคัญสำหรับทุกคนเพราะสามารถค้นหาสิ่งที่ตนสนใจได้ในทันทีโดยไม่ต้องเสียเวลาเดินทางไปค้นคว้าในห้องสมุด หรือแม้แต่การรับรู้ข่าวสารทั่วโลกก็สามารถอ่านได้ในอินเทอร์เน็ตจากเว็บไซต์ต่าง ๆ ของหนังสือพิมพ์

ดังนั้นอินเทอร์เน็ตจึงมีความสำคัญกับวิถีชีวิตของคนเราในปัจจุบันเป็นอย่างมากในทุก ๆ ด้าน ไม่ว่าจะเป็นบุคคลที่อยู่ในวงการธุรกิจ การศึกษา ต่างก็ได้รับประโยชน์จากอินเทอร์เน็ตด้วยกันทั้งนั้น

1. ด้านการศึกษา อินเทอร์เน็ตมีความสำคัญ ดังนี้

1.1. สามารถใช้เป็นแหล่งค้นคว้าหาข้อมูล ไม่ว่าจะเป็นข้อมูลทางวิชาการ ข้อมูลด้านการบันเทิง ด้านการแพทย์ และอื่น ๆ ที่น่าสนใจ

1.2. ระบบเครือข่ายอินเทอร์เน็ต จะทำหน้าที่เปรียบเสมือนเป็นห้องสมุดขนาดใหญ่

1.3. นักเรียนนักศึกษาสามารถใช้อินเทอร์เน็ตติดต่อกับมหาวิทยาลัยหรือโรงเรียนอื่น ๆ เพื่อค้นหาข้อมูลที่กำลังศึกษาอยู่ได้ ทั้งที่ข้อมูลที่เป็นข้อความเสียง ภาพเคลื่อนไหวต่าง ๆ

2. ด้านธุรกิจและการพาณิชย์ อินเทอร์เน็ตมีความสำคัญ ดังนี้

2.1. ค้นหาข้อมูลต่าง ๆ เพื่อช่วยในการตัดสินใจทางธุรกิจ

2.2. สามารถซื้อขายสินค้า ทำธุรกรรมผ่านระบบเครือข่าย

2.3. เป็นช่องทางในการประชาสัมพันธ์ โฆษณาสินค้า ติดต่อสื่อสารทางธุรกิจ

2.4. ผู้ใช้ที่เป็นบริษัท หรือองค์กรต่าง ๆ ก็สามารถเปิดให้บริการ และสนับสนุนลูกค้าของตนผ่านระบบเครือข่ายอินเทอร์เน็ตได้ เช่น การให้คำแนะนำ สอบถามปัญหาต่าง ๆ ให้แก่ลูกค้า แจกจ่ายตัวโปรแกรมทดลองใช้ (Shareware) โปรแกรมแจกฟรี (Freeware)

การทำงานของอินเทอร์เน็ต

การสื่อสารข้อมูลด้วย**อินเทอร์เน็ต**จะมีโปรโตคอล (Protocol) ซึ่งเป็นระเบียบวิธีการสื่อสารที่เป็นมาตรฐานของการเชื่อมต่อกำหนดไว้ โปรโตคอลที่เป็นมาตรฐานสำหรับการเชื่อมต่ออินเทอร์เน็ต คือ TCP/IP (Transmission Control Protocol/Internet Protocol)

เครื่องคอมพิวเตอร์ทุกเครื่องที่เชื่อมต่อเข้ากับเครือข่ายอินเทอร์เน็ตจะต้องมีหมายเลขประจำเครื่อง ที่เรียกว่า IP Address เพื่อเอาไว้อ้างอิงหรือติดต่อกับเครื่องคอมพิวเตอร์อื่นๆ ในเครือข่าย ซึ่ง IP ในที่นี้ก็คือ Internet Protocol ตัวเดียวกับใน TCP/IP นั่นเอง

โดเมนเนม (Domain name system : DNS)

เนื่องจากการติดต่อสื่อสารกันกันในระบบอินเทอร์เน็ตใช้โปรโตคอล TCP/IP เพื่อสื่อสารกัน โดยจะต้องมี IP address ในการอ้างอิงเสมอ แต่ IP address นี้ถึงแม้จะจัดแบ่งเป็นส่วนๆ แล้วก็ยังมีอุปสรรคในการที่ต้องจดจำ ถ้าเครื่องที่อยู่ในเครือข่ายมีจำนวนมากขึ้น การจดจำหมายเลข IP ดูจะเป็นเรื่องยาก และอาจสับสนจำผิดได้ แนวทางแก้ปัญหาคือการตั้งชื่อหรือตัวอักษรขึ้นมาแทนที่ IP address ซึ่งสะดวกในการจดจำมากกว่า เช่น IP address คือ 203.183.233.6 แทนที่ด้วยชื่อ dusit.ac.th ผู้ใช้งานสามารถ จดจำชื่อ dusit.ac.th ได้ง่ายกว่า การจำตัวเลข

โดเมนที่ได้รับความนิยมกันทั่วโลก ที่ถือว่าเป็นโดเมนสากล มีดังนี้ คือ

.com ย่อมาจาก Commercial สำหรับธุรกิจ
.edu ย่อมาจาก Education สำหรับการศึกษา
.int ย่อมาจาก International Organization สำหรับองค์กรนานาชาติ
.org ย่อมาจาก Organization สำหรับหน่วยงานที่ไม่แสวงหากำไร
.net ย่อมาจาก Network สำหรับหน่วยงานที่มีเครือข่ายของ ตนเองและทำธุรกิจด้านเครือข่าย

การขอจดทะเบียนโดเมน

การขอจดทะเบียนโดเมนต้องเข้าไปจะทะเบียนกับหน่วยงานที่รับผิดชอบ ชื่อโดเมนที่ขอจดนั้นไม่สามารถซ้ำกับชื่อที่มีอยู่เดิม เราสามารถตรวจสอบได้ว่ามีชื่อโดเมนนั้นๆ หรือยังได้จากหน่วยงานที่เราจะเข้าไปจดทะเบียน

การขอจดทะเบียนโดเมน มี 2 วิธี ด้วยกัน คือ

1. การขอจดะเบียนให้เป็นโดเมนสากล (.com .edu .int .org .net)
   ต้องขอจดทะเบียนกับ www.networksolution.com ซึ่งเดิม คือ www.internic.net
2. การขอทดทะเบียนที่ลงท้ายด้วย .th (Thailand)
   ต้องจดทะเบียนกับ www.thnic.net
   โดเมนเนมที่ลงท้าย ด้วย .th ประกอบด้วย

.ac.th	ย่อมาจาก Academic Thailand	สำหรับสถานศึกษาในประเทศไทย
.co.th	ย่อมาจาก Company Thailand	สำหรับบริษัทที่ทำธุรกิจในประเทศไทย
.go.th	ย่อมาจาก Government Thailand	สำหรับหน่วยงานต่างๆ ของรัฐบาล
.net.th	ย่อมาจาก Network Thailand	สำหรับบริษัทที่ทำธุรกิจด้านเครือข่าย
.or.th	ย่อมาจาก Organization Thailand	สำหรับหน่วยงานที่ไม่แสวงหากำไร
.in.th	ย่อมาจาก Individual Thailand	สำหรับของบุคคลทั่วๆ ไป

การใช้งานอินเทอร์เน็ต

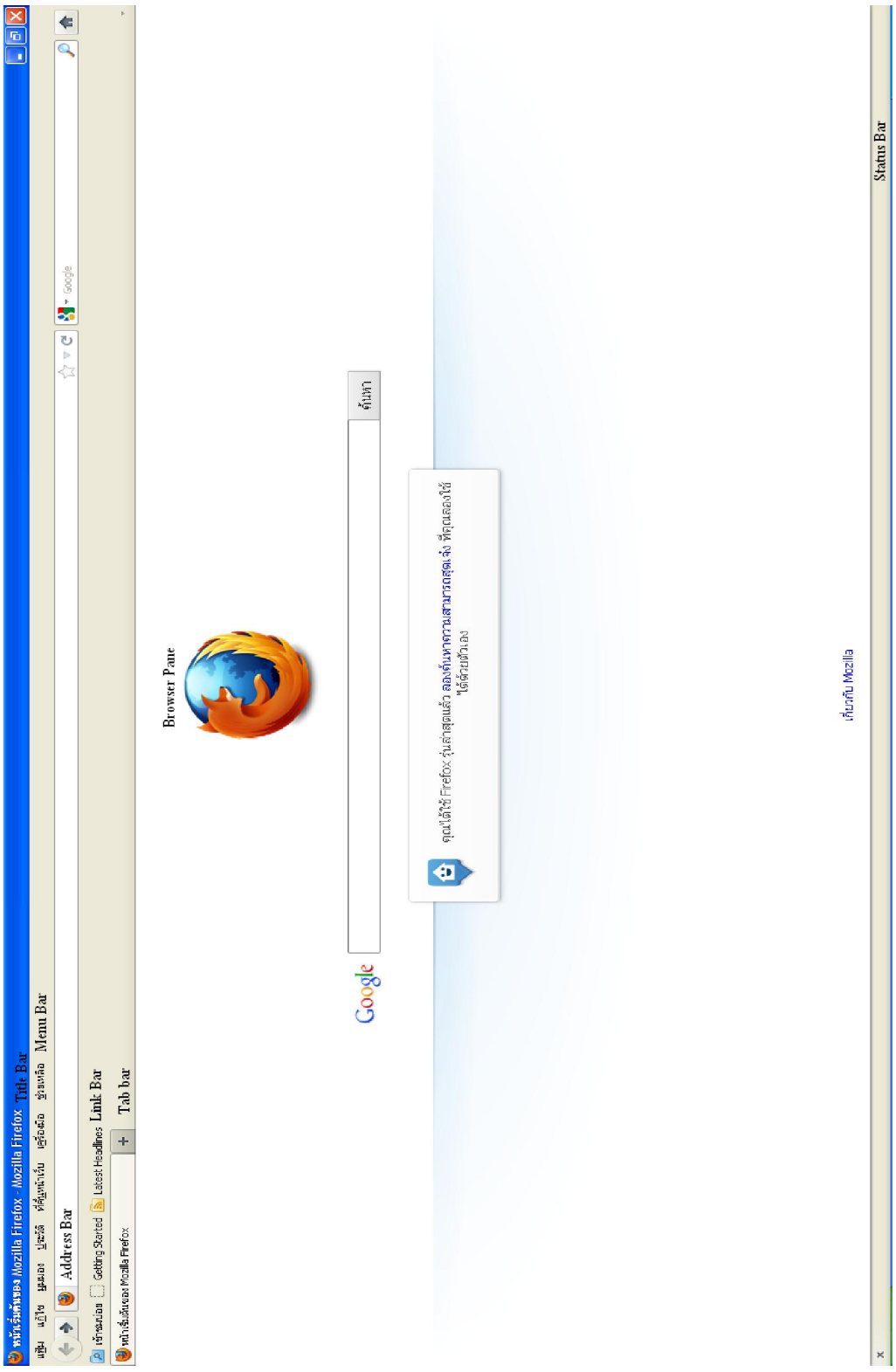
การใช้อินเตอร์เน็ตเราจำเป็นจะต้องรู้จักโปรแกรมที่ใช้ในการใช้งานอินเทอร์เน็ตเรียกว่า “บราวเซอร์”

บราวเซอร์ (Browser) คือ เครื่องมือที่ช่วยให้สามารถท่องเที่ยวไปในโลกอินเตอร์เน็ตได้อย่างไร้ขีดกั้นทางด้านพรมแดน นอกจากนี้ Browser ยังช่วยอำนวยความสะดวกในการเยี่ยมชมเว็บไซต์ต่างๆ ซึ่งในขณะนี้บริษัทผลิตซอฟแวร์ค่ายต่างๆ นับวันจะทวีการแข่งขันกันในการผลิต Browser เพื่อสร้างความพึงพอใจให้แก่นักท่องเว็บให้มากที่สุด หน้าตาของ browser แตกต่างกันไปตามแต่การออกแบบการใช้งานของแต่ละค่ายโปรแกรม ในปัจจุบันบราวเซอร์มีให้ผู้ใช้อินเทอร์เน็ตเลือกอย่างมากมาย และได้มีการจัดอันดับที่ได้รับความนิยมในปี 2554 ดังนี้

ตารางการจัดอันดับ Browser ที่ได้รับความนิยมปี 2554

อันดับ 1	Firefox	www.mozilla.com
อันดับ 2	Google Chrome	www.google.com/chrome
อันดับ 3	Internet Explorer	www.microsoft.com/windows/internet-explorer/default.aspx
อันดับ 4	Opera	www.opera.com
อันดับ 5	Safari	www.apple.com/safari
อันดับ 6	Maxthon	www.maxthon.com
อันดับ 7	Flock	www.flock.com
อันดับ 8	Avant Browser	www.avantbrowser.com
อันดับ 9	Deepnet Explorer	www.deepnetexplorer.com
อันดับ 10	PhaseOut	www.phaseout.net

เมื่อทำความรู้จักกับ Browser แล้วเราต้องศึกษาส่วนประกอบของ Browser ซึ่ง Browser แต่ละนั้นจะมีส่วนประกอบแตกต่างกันออกไป ในที่นี้เราจะเรียนรู้ส่วนประกอบของบราวเซอร์ที่มีชื่อว่า Firefox ซึ่งเป็น Browser ได้รับความนิยมมากที่สุดในปี 2554



1. Title Bar แสดงชื่อของเอกสารบนอินเทอร์เน็ตที่กำลังเปิดชมอยู่ในขณะนั้น

2. Menu Bar เมนูคำสั่งในการทำงาน เมื่อคลิกที่ชื่อของเมนู จะมีรายการเมนูย่อยแสดงออกมาให้เลือกใช้
3. Address Bar ที่อยู่ของเอกสารเว็บหรือที่อยู่ของสถานที่บนอินเทอร์เน็ต ซึ่งเรียกว่า URL
4. Link Bar ใช้เก็บลิงค์พิเศษที่เราต้องการจะเข้าถึงอย่างรวดเร็ว
5. Tab Bar แสดงจำนวนหน้าที่เปิดไว้ใน Browser
6. Browser Pane จอภาพที่แสดงข้อมูลของเว็บเพ็จ
7. Status Bar เป็นแถบแสดงสถานการณ์ทำงาน

บริการต่างๆ บนอินเทอร์เน็ต

1. เวิลด์ไวด์เว็บ (WWW)

เวิลด์ไวด์เว็บ หรือเครือข่ายใยแมงมุม เหตุที่เรียกชื่อนี้เพราะว่าเป็นลักษณะของการเชื่อมโยงข้อมูล จากที่หนึ่งไปยังอีกที่หนึ่งเรื่อยๆ เวิลด์ไวด์เว็บ เป็นบริการที่ได้รับความนิยมมากที่สุด ในการเรียกดูเว็บไซต์ต้องอาศัยโปรแกรมเว็บเบราว์เซอร์ (web browser) ในการดูข้อมูล เว็บเบราว์เซอร์ที่ได้รับความนิยมใช้ในปัจจุบัน เช่น โปรแกรม Internet Explorer (IE) , Netscape Navigator

2. จดหมายอิเล็กทรอนิกส์ (Electronic Mail)

การติดต่อสื่อสารโดยใช้อีเมลสามารถทำได้โดยสะดวก และประหยัดเวลา หลักการทำงานของอีเมลก็คล้ายกับการส่งจดหมายธรรมดา นั้นคือ จะต้องมีที่อยู่ที่ระบุชัดเจน ก็คือ อีเมลแอดเดรส (E-mail address) องค์ประกอบของ e-mail address ประกอบด้วย

1. ชื่อผู้ใช้ (User name)
2. ชื่อโดเมน Username@domain_name เช่น abcd@pcru.ac.th

การใช้งานอีเมล สามารถแบ่งได้ดังนี้ คือ

1. Corporate e-mail คือ อีเมล ที่หน่วยงานต่างๆสร้างขึ้นให้กับพนักงานหรือบุคลากรในองค์กรนั้น เช่น abcd@pcru.ac.th คือ e-mail ของบุคลากรของมหาวิทยาลัยราชภัฏเพชนบูรณ์ เป็นต้น

2. Free e-mail คือ อีเมล ที่สามารถสมัครได้ฟรีตาม web mail ต่างๆ เช่น Hotmail, Yahoo Mail, และ Gmail เป็นต้น

3. บริการโอนย้ายไฟล์ (File Transfer Protocol)

เป็นบริการที่เกี่ยวข้องกับการโอนย้ายไฟล์ผ่านระบบอินเทอร์เน็ต การโอนย้ายไฟล์สามารถแบ่งได้ดังนี้ คือ

1. การดาวน์โหลดไฟล์ (Download File)

การดาวน์โหลดไฟล์ คือ การรับข้อมูลเข้ามายังเครื่องคอมพิวเตอร์ของผู้ใช้ ในปัจจุบันมีหลายเว็บไซต์ที่จัดให้มีการดาวน์โหลดโปรแกรมได้ฟรีเช่น www.download.com

2. การอัพโหลดไฟล์ (Upload File)

การอัพโหลดไฟล์คือการนำไฟล์ข้อมูลจากเครื่องของผู้ใช้ไปเก็บไว้ในเครื่องที่ให้บริการ (Server) ผ่านระบบอินเทอร์เน็ต เช่น กรณีที่ทำการสร้างเว็บไซต์ จะมีการอัพโหลดไฟล์ไปเก็บไว้ในเครื่องบริการเว็บไซต์ (Web server) ที่เราขอใช้บริการพื้นที่ (web server) โปรแกรมที่ช่วยในการอัพโหลดไฟล์เช่น FTP Commander

4. บริการสนทนาบนอินเทอร์เน็ต (Instant Message)

การสนทนาบนอินเทอร์เน็ตคือ การส่งข้อความถึงกันโดยทันทีทันใด นอกจากนี้ยังสามารถส่งสัญลักษณ์ต่างๆ อาทิ รูปภาพ ไฟล์ข้อมูลได้ด้วย การสนทนาบนอินเทอร์เน็ตเป็นโปรแกรมที่กำลังได้รับความนิยมในปัจจุบัน โปรแกรมประเภทนี้ เช่น โปรแกรม MSN Messenger, Yahoo Messenger, Skype เป็นต้น

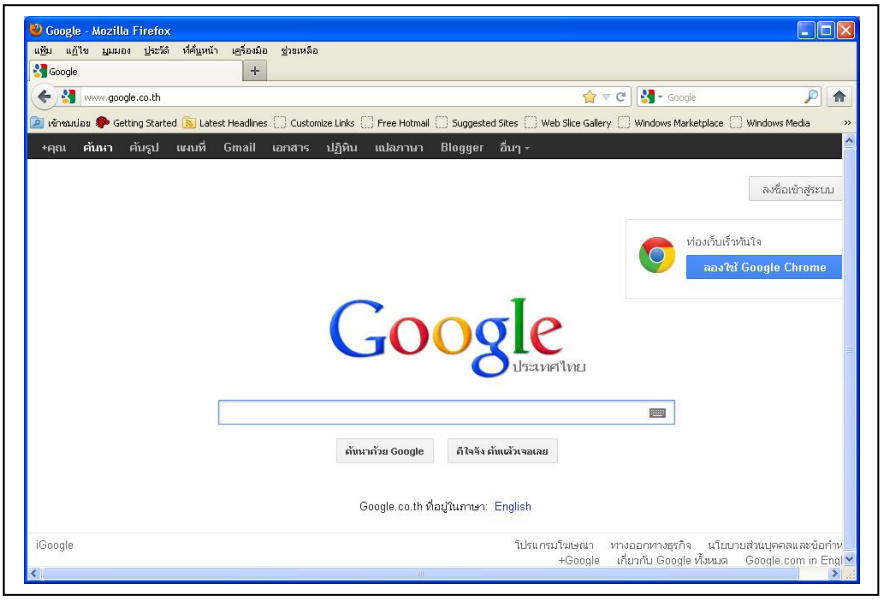
5. บริการค้นหาข้อมูลบนอินเทอร์เน็ต (Search Engine)

โดยทั่วไปลักษณะการสืบค้นข้อมูลบนอินเทอร์เน็ตสามารถแบ่งลักษณะรูปแบบการค้นหา เป็น 3 ลักษณะ คือ

5.1 Web Directory คือ การค้นหาโดยการเลือก Directory ที่จัดเตรียมและแยกหมวดหมู่ไว้ให้เรียบร้อยแล้ว ซึ่งบรรจุเนื้อหาหรือเว็บไซต์ต่างๆ ไว้เป็นหมวดหมู่หรือกลุ่มใหญ่ ๆ และแต่ละกลุ่มจะแบ่งเป็นเรื่องย่อยๆ ต่อไปเรื่อยๆ เหมือนกับหลักการจัดหมวดหมู่หนังสือในห้องสมุดข้อดีคือ ช่วยให้ผู้ใช้ได้ข้อมูลที่ตรงกับความต้องการ เนื่องจากนำข้อมูลมาจัดหมวดหมู่ไว้อย่างเป็นระบบ และสามารถกำหนดค้นได้ง่ายในหัวข้อโดยเลือกจากรายการที่ทำไว้แล้วwebsite ที่ให้บริการ web directory เช่น www.yahoo.com, www.sanook.com

ภาพแสดงตัวอย่าง Web Directory (www.sanook.com)

5.2 การค้นหาแบบดัชนี (Index) หรือ สำคัญ (Keyword) คือ การค้นหาข้อมูลโดยใช้โปรแกรม Search โดยการเอาคำที่เราต้องการค้นหาไปเทียบกับเว็บไซต์ต่างๆ ว่ามีเว็บไซต์ใดบ้างที่มีคำที่เราต้องการค้นหาโดยการค้นจากข้อความในเว็บเพจที่ได้ผ่านการสำรวจมาแล้ว จะอ่านข้อความ ประมาณ 200-300 ตัวอักษรแรกของเว็บเพจ วิธีการค้นหาของ Search Engine ประเภทนี้จะให้ความสำคัญกับการเรียงลำดับข้อมูลก่อนหลัง การค้นหาข้อมูล การค้นหาวิธีนี้จะมีความรวดเร็วมาก แต่มีความละเอียดในการจัดแยกหมวดหมู่ของข้อมูลค่อนข้างน้อย เนื่องจากไม่ได้คำนึงถึงรายละเอียดของเนื้อหาเท่าที่ควร แต่ถ้าต้องการแนวทางด้านกว้างของข้อมูล การค้นหาแบบนี้จะเหมาะสมที่สุด website ที่ให้บริการ search engine เช่น www.google.co.th



5.3 Metasearch คือ ลักษณะการสืบค้นหาข้อมูลจะมีลักษณะเดียวกันกับ search engine แต่จะทำการส่งคำที่ต้องการไปค้นหาในเว็บไซต์ที่ให้บริการสืบค้นข้อมูลอื่นๆ อีก ถ้าข้อมูลที่ได้มีซ้ำกัน ก็จะแสดงเพียงรายการเดียว จุดเด่นของการค้นหาด้วยวิธีการนี้ คือ สามารถเชื่อมโยงไปยัง Search Engine ประเภทอื่นๆ และยังมีความหลากหลายของข้อมูล แต่การค้นหาด้วยวิธีนี้มีจุดด้อย คือ วิธีการนี้จะไม่ให้ความสำคัญกับขนาดเล็กใหญ่ของตัวอักษร และมักจะผ่านเลยคำประเภท Natural Language (ภาษาพูด) ดังนั้น หากจะใช้ Search Engine ประเภทนี้จะพบกับข้อบกพร่องเหล่านี้ด้วย

6. บริการกระดานข่าวหรือ เว็บบอร์ด (Web board)

เว็บบอร์ด เป็นศูนย์กลางในการแสดงความคิดเห็น มีการตั้งกระทู้ ถาม-ตอบ ในหัวข้อที่สนใจ เว็บบอร์ดของไทยที่เป็นที่นิยมและมีคนเข้าไปแสดงความคิดเห็นมากมาย คือ เว็บบอร์ดของพันธ์ทิพย์ (www.pantip.com)

7. ห้องสนทนา (Chat Room)

ห้องสนทนา คือ การสนทนาออนไลน์อีกประเภทหนึ่ง ที่มีการส่งข้อความสั้นๆ ถึงกัน เพื่อทักทายกันระหว่างผู้ที่ใช้เข้าใช้เว็บไซต์ การเข้าไปสนทนาจำเป็นต้องเข้าไปในเว็บไซต์ที่ให้บริการห้องสนทนาเช่น www.sanook.com www.pantip.com

8. บริการสังคมออนไลน์ (Social Media หรือ Social Network)

Social Media หมายถึงสังคมออนไลน์ที่มีผู้ใช้เป็นผู้สื่อสาร หรือเขียนเล่า เนื้อหา เรื่องราว ประสบการณ์ บทความ รูปภาพ และวิดีโอ ที่ผู้ใช้เขียนขึ้นเอง ทำขึ้นเอง หรือพบเจอจากสื่ออื่นๆ แล้วนำมาแบ่งปันให้กับผู้อื่นที่อยู่ในเครือข่ายของตน ผ่านทางเว็บไซต์ Social Network ที่ให้บริการบนโลกออนไลน์ปัจจุบัน การสื่อสารแบบนี้ จะทำผ่านทาง Internet และโทรศัพท์มือถือเท่านั้น

บริการของ Social Media โดยทั่วไปมีหลากหลายรูปแบบ ทั้งกระดานความคิดเห็น (Discussion boards), เว็บบล็อก (Webblogs), วิกิ (wikis), Podcasts, รูปภาพ และวิดีโอ เป็นต้น

การแนะนำบริการสังคมออนไลน์

[1]เครือข่ายสังคมออนไลน์ (Social Network) เป็นรูปแบบของเว็บไซต์ ในการสร้างเครือข่ายสังคม สำหรับผู้ใช้งานในอินเทอร์เน็ต เขียนและอธิบายความสนใจ และกิจการที่ได้ทำ และเชื่อมโยงกับความสนใจและกิจกรรมของผู้อื่น ในบริการเครือข่ายสังคมมักจะประกอบไปด้วย การแช็ต ส่งข้อความ ส่งอีเมล วิดีโอ เพลง อัปโหลดรูป บล็อก การทำงานคือ คอมพิวเตอร์เก็บข้อมูลพวกนี้ไว้ในรูปฐานข้อมูล sql ส่วน video หรือ รูปภาพ อาจเก็บเป็น ไฟล์ก็ได้ บริการเครือข่ายสังคมที่เป็นที่นิยมได้แก่ ไฮไฟฟ์ มายสเปซ เฟซบุ๊ก ออร์กัต มัลติพลาย โดยเว็บเหล่านี้มีผู้ใช้มากมาย เช่น เฟสบุ๊คเป็นเว็บไซต์ที่คนไทยใช้มากที่สุด ในขณะที่ออร์กัตเป็นที่นิยมมากที่สุดในประเทศอินเดีย ปัจจุบัน บริการเครือข่ายสังคม มีผลประโยชน์คือหาเงินจากการโฆษณา การเล่นเกมโดยใช้บัตรเติมเงิน

เนื่องจากมีการให้บริการเครือข่ายสังคมออนไลน์อยู่มากมาย จึงเลือกแนะนำเว็บไซต์ที่มีความนิยมสูงในประเทศไทย ดังนี้

- Facebook

[2]**เฟซบุ๊ก** (Facebook) เป็นบริการเครือข่ายสังคมและเว็บไซต์ เปิดใช้งานเมื่อ 4 กุมภาพันธ์ ค.ศ. 2004 ดำเนินงานและมีเจ้าของคือ บริษัท เฟซบุ๊ก (Facebook, Inc.) จากข้อมูลเดือนกรกฎาคม ค.ศ. 2010 เฟซบุ๊กมีผู้ใช้ประจำ 500 ล้านบัญชี ผู้ใช้สามารถสร้างข้อมูลส่วนตัว เพิ่มรายชื่อผู้ใช้อื่นในฐานะเพื่อนและแลกเปลี่ยนข้อความ รวมถึงได้รับแจ้งโดยทันทีเมื่อพวกเขาปรับปรุงข้อมูลส่วนตัว นอกจากนั้นผู้ใช้ยังสามารถร่วมกลุ่มความสนใจส่วนตัว จัดระบบตามสถานที่ทำงาน โรงเรียน มหาวิทยาลัย หรือ อื่น ๆ ชื่อของเฟซบุ๊กนั้นมาจากชื่อเรียกภาษาปากของสมุดที่ให้กับนักเรียนเมื่อเริ่มแรกเรียนในสถาบันอุดมศึกษา ที่มอบให้โดยคณะบริหารมหาวิทยาลัยในสหรัฐอเมริกา เพื่อช่วยให้นักเรียนสามารถรู้จักผู้อื่นได้ดีมากขึ้น เฟซบุ๊กอนุญาตให้ใครก็ได้เข้าสมัครลงทะเบียนกับเฟซบุ๊ก โดยต้องมีอายุมากกว่า 13 ปีขึ้นไป

เฟซบุ๊กก่อตั้งขึ้นโดย มาร์ก ซักเคอร์เบิร์ก ร่วมกับเพื่อนร่วมห้องในวิทยาลัยของเขาและเป็นนักเรียนวิทยาศาสตร์คอมพิวเตอร์ที่ชื่อ เอ็ดวาร์โด ซาเวริน, ดิสติน มอสโควิตซ์ และคริส ฮิวส์ เดิมทีสมาชิกของเว็บไซต์จะจำกัดเฉพาะกลุ่มผู้ก่อตั้งและนักเรียนมหาวิทยาลัยฮาวาร์ด แต่ต่อมาขยับขยายไปสู่มหาวิทยาลัยอื่นในแถบบอสตัน, กลุ่มไอวีลีก, และมหาวิทยาลัยสแตนฟอร์ด แล้วค่อย ๆ เพิ่มนักเรียนจากมหาวิทยาลับอื่น จนกระทั่งเปิดให้กับนักเรียนระดับไฮสคูล จนในที่สุดทุกคนก็สามารถเข้าสมัครได้โดยอายุมากกว่า 13 ปีขึ้นไป

สำหรับติดต่อแลกข้อมูลข่าวสาร เปิดใช้งานเมื่อ 4 กุมภาพันธ์ พ.ศ. 2547 โดย มาร์ก ซักเคอร์เบิร์ก นักศึกษาจากมหาวิทยาลัยฮาร์เวิร์ด ในช่วงแรกนั้นเฟซบุ๊กเปิดให้ใช้งานเฉพาะนักศึกษามหาวิทยาลัยฮาร์เวิร์ด ซึ่งต่อมาได้ขยายตัวออกไปสำหรับมหาวิทยาลัยทั่วสหรัฐอเมริกา และตั้งแต่ 11 กันยายน พ.ศ. 2549 ได้ขยายมาสำหรับผู้ใช้ทั่วไปทุกคนเหมือนในปัจจุบัน

- Twitter

[3]**ทวิตเตอร์** (Twitter) เป็นบริการเครือข่ายสังคมออนไลน์จำพวกไมโครบล็อก โดยผู้ใช้สามารถส่งข้อความยาวไม่เกิน 140 ตัวอักษร ว่าตัวเองกำลังทำอะไรอยู่ หรือ *ทวีต* (*tweet* - เสียงนกร้อง) ทวิตเตอร์ก่อตั้งขึ้นโดย แจ็ก คอร์ซีย์ ,บิซ สโตน และ อีวาน วิลเลียมส์ เจ้าของบริษัท Obvious Corp ที่ซานฟรานซิสโก สหรัฐอเมริกา เมื่อเดือนมีนาคม ค.ศ. 2006

ข้อความอัปเดตที่ส่งเข้าไปยังทวิตเตอร์จะแสดงอยู่บนเว็บเพจของผู้ใช้คนนั้นบนเว็บไซต์ และผู้ใช้คนอื่นสามารถเลือกรับข้อความเหล่านี้ทางเว็บไซต์ทวิตเตอร์, อีเมล, เอสเอ็มเอส, เมสเซนเจอร์ (IM),RSS, หรือผ่านโปรแกรมเฉพาะอย่าง Twitterific Twhirl ปัจจุบันทวิตเตอร์มีหมายเลขโทรศัพท์สำหรับส่งเอสเอ็มเอสในสามประเทศ คือ สหรัฐอเมริกา แคนาดา และสหราชอาณาจักร

- Google+

[4]**กูเกิล+** (Google+) เป็นบริการเครือข่ายสังคมให้บริการโดยกูเกิล โดยเปิดให้ใช้งานครั้งแรกเมื่อวันที่ 28 มิถุนายน พ.ศ. 2554 ผู้ที่จะเข้ามาทดลองใช้ต้องได้รับเชิญจากบุคคลที่ใช้อยู่เท่านั้นอย่างไรก็ตามระบบการเชิญถูกยุติเนื่องจากมีการใช้งานเป็นจำนวนมากเกินกว่าที่ระบบจะรองรับได้ ภายหลังในวันที่ 20 กันยายน พ.ศ. 2554 จึงเปิดให้ผู้ใช้ทั่วไปได้ใช้งาน

Google+ ทำงานโดยรวมบริการหลายอย่างของทางกูเกิลเข้าไว้ที่เดียวกัน อาทิ เช่น กูเกิล บัซซ์, กูเกิล โพรไฟล์, กูเกิล ทอล์ก และอีกหลายบริการ ปัจจุบันได้มีการรับรองการทำงานผ่านเว็บเบราว์เซอร์,แอปพลิเคชันของแอนดรอยด์ และ แอปพลิเคชันของไอโอเอส สำหรับ ไอโฟน ได้มีการวิเคราะห์มาว่าบริการตัวนี้ของกูเกิลจะเป็นคู่แข่งกับเครือข่ายสังคมเฟซบุ๊ก

- Foursquare

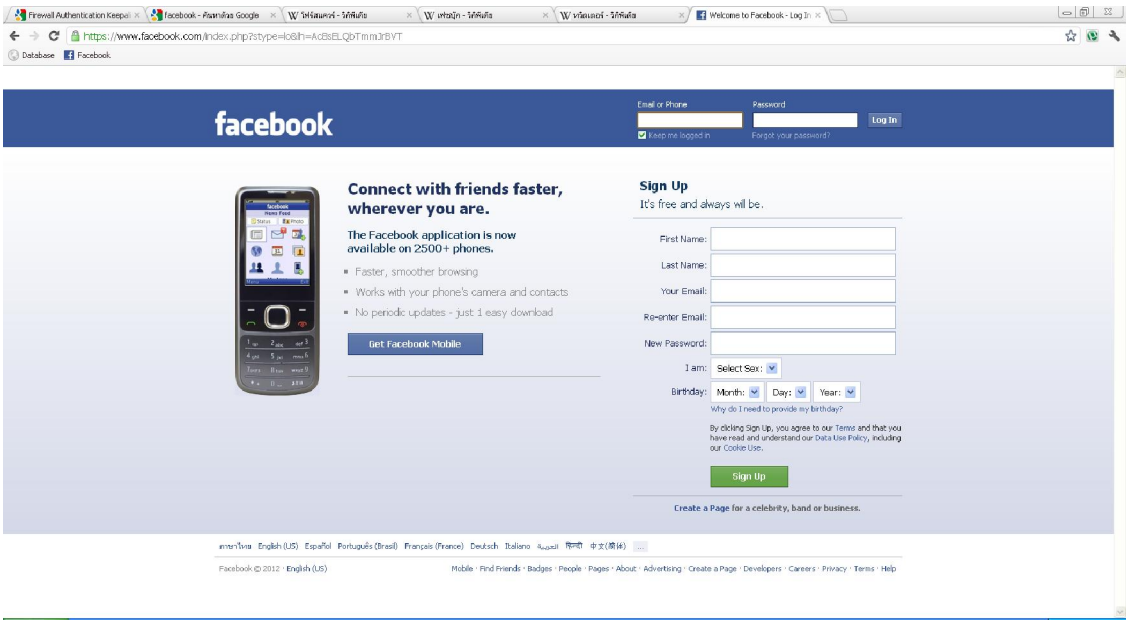
[5]**โฟร์สแควร์** (foursquare) เป็นโซเชียลเน็ตเวิร์กผสมเกม (gamification) ลักษณะคือการอ้างอิงสถานที่ โฟร์สแควร์สร้างโดย เดนนิส โครว์ลีย์ (ซึ่งเดิมเคยร่วมกับอเล็กซ์ เรเนิร์ตสร้าง Dodgeball บริการอ้างอิงสถานที่ที่ในปี 2000 ต่อมาถูกซื้อไปโดยกูเกิ้ลในปี 2005 แล้วกลายมาเป็น Google Latitude ในปี 2009) และ นาวีน เซลวาดูราย บริษัทโฟร์สแควร์สำนักงานใหญ่อยู่ที่นิวยอร์กซิตี สหรัฐอเมริกา

การใช้งานโฟร์สแควร์สามารถเล่นได้ผ่านโทรศัพท์มือถือ (ผ่านทาง mobile web), สมาร์ตโฟน (ผ่านทาง foursquare app) และแอปพลิเคชันต่างๆ ที่สามารถเชื่อมต่อกับโฟร์สแควร์ได้ (เช่น Instagram, Path, Yotomo, GetGlue, Waze, FootFeed, HootSuite เป็นต้น) โดยเมื่อผู้เล่นเปิดตำแหน่งของตัวผู้เล่นจะทำการเรียกสถานที่ที่อยู่ใกล้เคียง ไม่ว่าโรงเรียน ร้านอาหาร โรงแรม โรงพยาบาล ฯลฯ ขึ้นมา และผู้เล่นจะทำการเลือก "เช็กอิน" สถานที่นั้นเพื่อแสดงให้เห็นว่าตนอยู่ที่นี่หรือได้มาที่นี่แล้ว

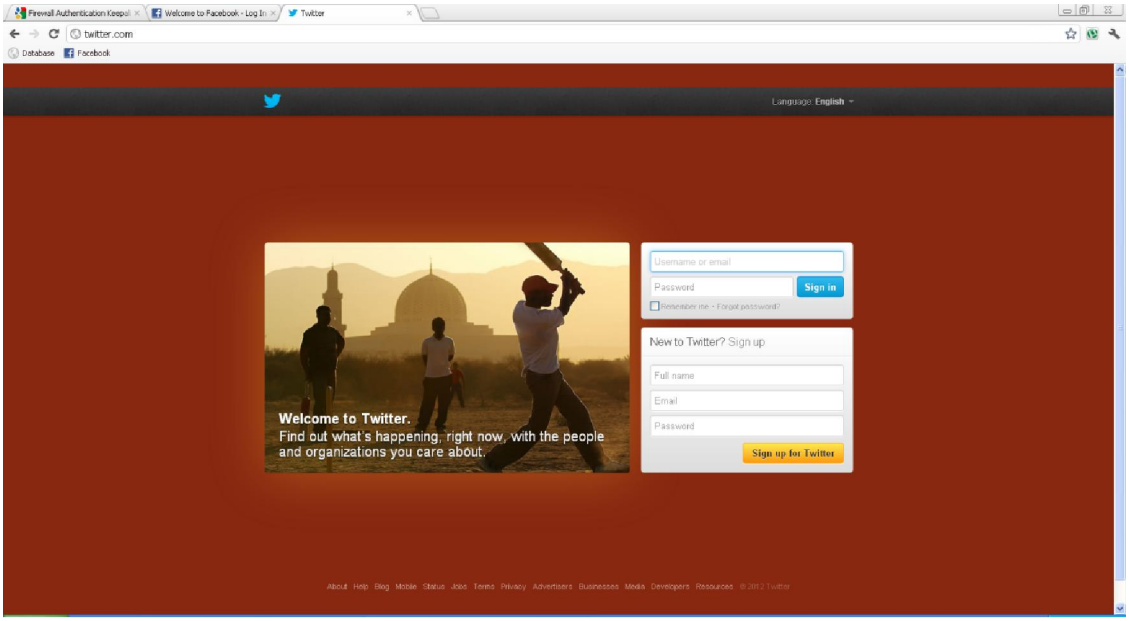
ผู้ใช้งานปัจจุบัน (มกราคม 2555) รายงานว่า มีผู้ใช้อยู่ 15 ล้านคนทั่วโลก

รูปภาพตัวอย่างเว็บไซต์สังคมออนไลน์

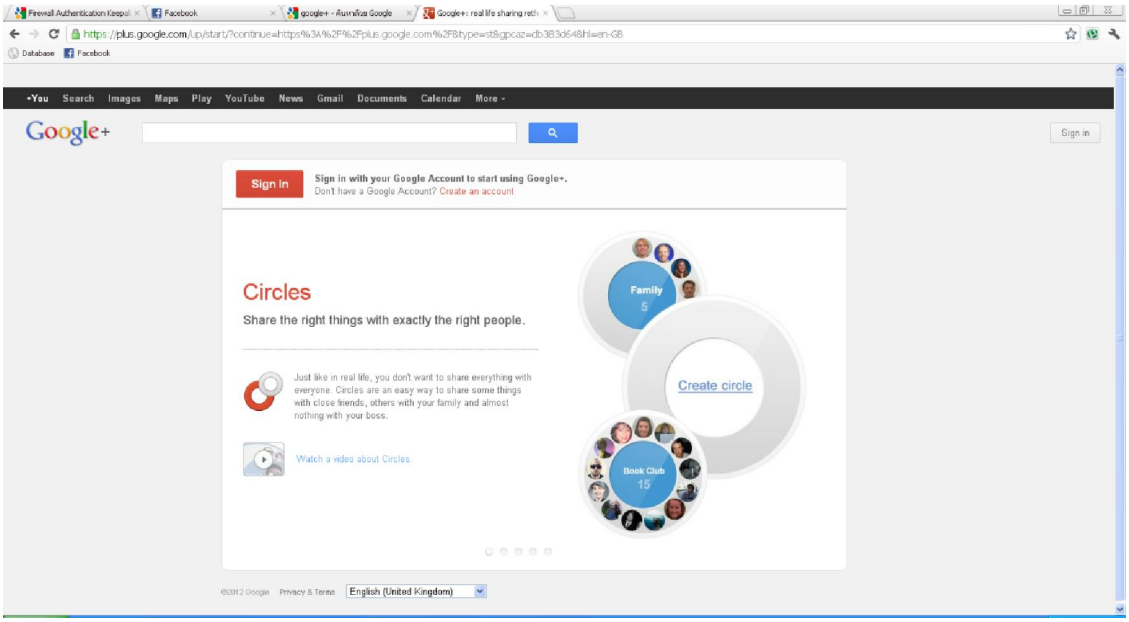
- Facebook



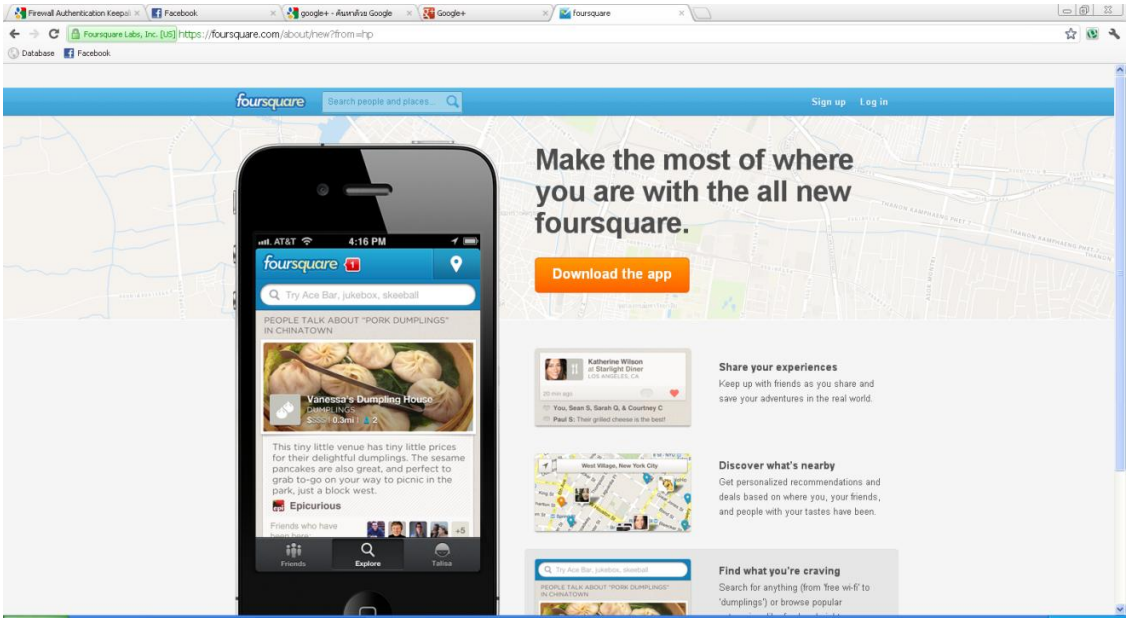
- Twitter



- Google+



- Foursquare



ขั้นตอนและวิธีการสืบค้นข้อมูลบนอินเทอร์เน็ต

อินเทอร์เน็ตเป็นแหล่งรวบรวมข้อมูลขนาดใหญ่ซึ่งมีข้อมูลหลากหลายประเภทและมีแนวโน้มจะเพิ่มขึ้นอย่างรวดเร็ว ดังนั้นการค้นหาข้อมูลที่ต้องการได้อย่างรวดเร็วนั้น ไม่ใช่เรื่องง่าย ๆ สำหรับผู้ที่ไม่คุ้นเคยกับแหล่งข้อมูลนี้ นั่นคือมักประสบปัญหาไม่ทราบว่าข้อมูลที่ต้องการนั้นอยู่ในเว็บไซต์ใด ดังนั้นจึงได้มีเว็บไซต์ที่ให้บริการค้นหาข้อมูลต่าง ๆ บนอินเทอร์เน็ต ที่เรียกว่า **เครื่องมือช่วยค้น หรือ เซิร์ชเอ็นจิน (Search Engine)**

Search Engine คือเครื่องมือที่ใช้ในการค้นหาข้อมูลในอินเตอร์เน็ต

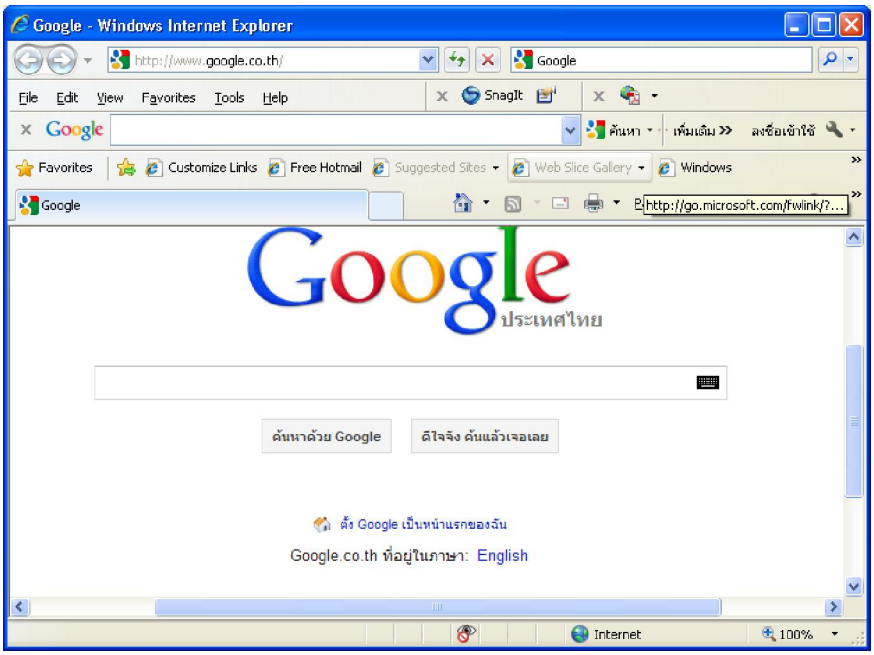
การสืบค้นข้อมูล คือ การนำความรู้เกี่ยวกับอินเทอร์เน็ต มาประยุกต์ใช้ในการศึกษาหาความรู้ ได้แก่ การสืบค้นข้อมูลทางอินเทอร์เน็ต

ในการสืบค้นข้อมูลนั้นถ้าหากเราทราบแหล่งข้อมูลหรือเว็บไซต์ เราก็สามารถพิมพ์หรือระบุ URL ในช่อง Address ได้เลย แต่ถ้าหากเราไม่ทราบว่าแหล่งข้อมูลนั้นอยู่ที่ใด เราสามารถใช้เว็บไซต์ที่เป็น Search Engine ช่วยในการค้นหาได้อย่างรวดเร็ว

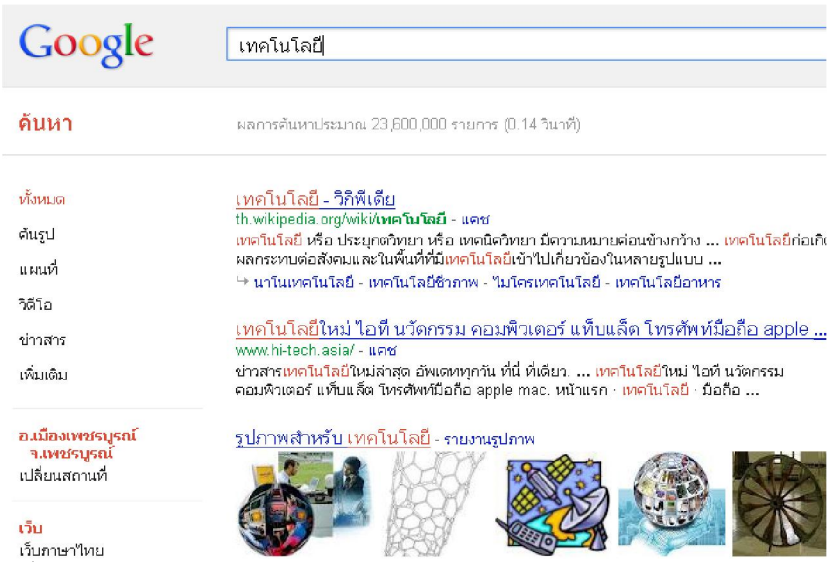
ขั้นตอนการสืบค้นข้อมูล

ขั้นตอนการสืบค้นข้อมูลด้วยโปรแกรม Search Engine โดยใช้งานผ่านเว็บไซต์ Google.com สามารถใช้งานได้ดังนี้

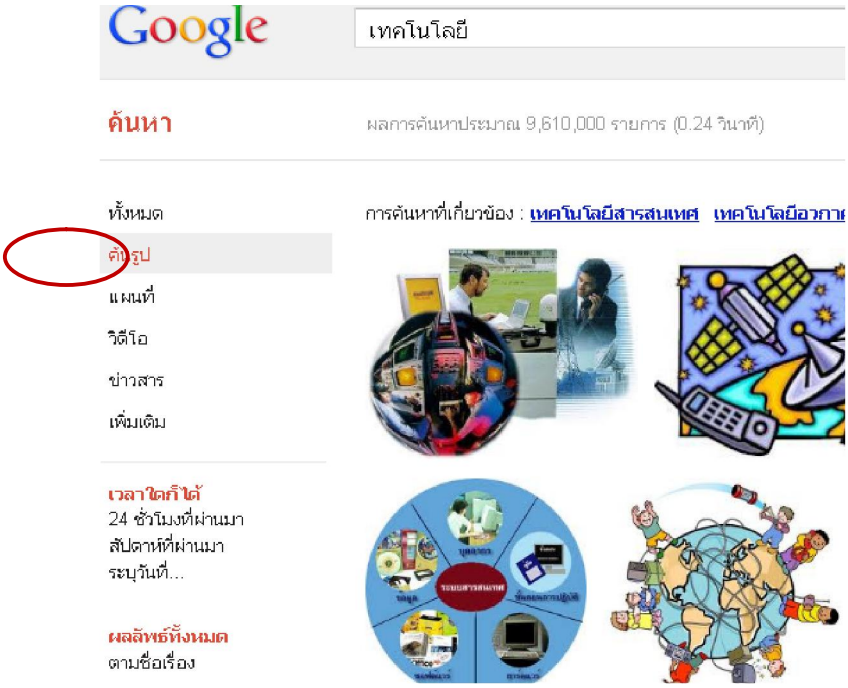
1. เปิดโปรแกรม Web Browser ตัวอย่างเช่น Internet Explorer หรือ Mozilla Firefox



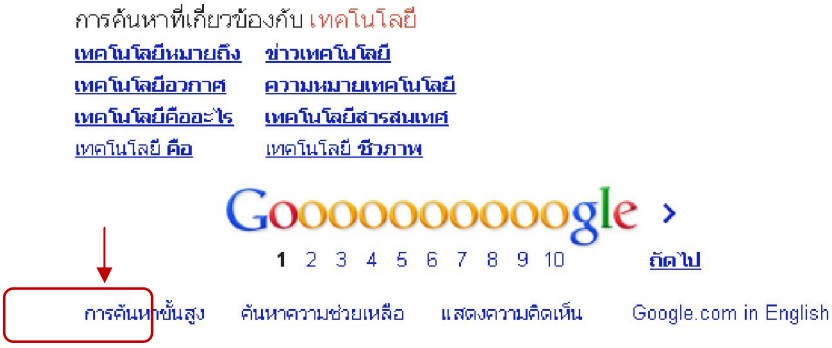
2. ป้อนคำหรือวลีที่ต้องการค้นข้อมูลลงในช่องสำหรับกรอกคำค้นข้อมูลหลังจากนั้นกดปุ่ม Enter จะได้ข้อมูลที่ต้องการค้นหาดังภาพด้านล่าง



3. เมื่อต้องการค้นข้อมูลที่เป็นรูปภาพสามารถกดลิงค์ “ค้นรูป” จะได้รูปภาพดังภาพด้านล่าง



4. การค้นหาข้อมูลระดับสูงหรือการค้นหาแบบพิเศษสามารถกดเลือกที่ลิงค์ด้านล่างของหน้าจอดังภาพด้านล่าง



5. การค้นหาขั้นสูงของ google search engine สามารถกำหนดขอบเขตของการสืบค้นข้อมูลได้ดังภาพด้านล่าง

6. ตัวอย่างการป้อนคำเพื่อสืบค้นข้อมูลซึ่งมีการกำหนดเงื่อนไขในการสืบค้นเช่น “ทุกคำเหล่านี้” “คำหรือวลีที่ตรงตามนี้”“และไม่มีคำเหล่านี้” จากตัวอย่างสามารถอธิบายเงื่อนไขในการสืบค้นได้ดังนี้ ให้ค้นข้อมูลทั้งหมดที่มีอยู่ในระบบโดยมีคำว่า “เทคโนโลยี” และมีคำหรือวลีที่ตรงกับคำว่า “คอมพิวเตอร์” และไม่ข้อมูลที่มีคำว่า “สารสนเทศ” มาแสดงที่หน้าจอ

จากการกรอกข้อมูลตามเงื่อนไขในข้อที่ 6 จะได้ผลดังภาพด้านล่าง

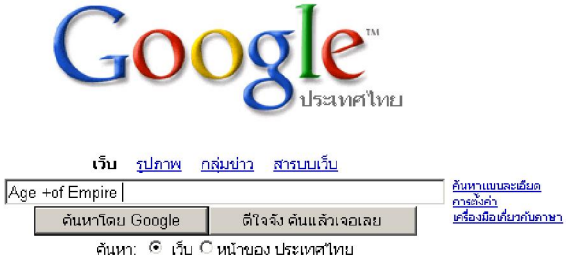
เทคนิคเพิ่มเติมในการค้นหาข้อมูล

การค้นหาโดยทั่วไปส่วนใหญ่แล้วจะใช้คำ Keyword เป็นเครื่องมือในการนำทางการค้นหาอย่างเดียวแต่ถ้าเรารู้จักใช้เครื่องหมายบางตัวร่วมด้วย ก็จะทำให้ขอบเขตการค้นหาของ Google แคบลง ทำให้เราได้ข้อมูลที่ตรงกับความต้องการมากขึ้นเครื่องหมายที่สามารถนำมาช่วยในการค้นหาได้ มีดังนี้

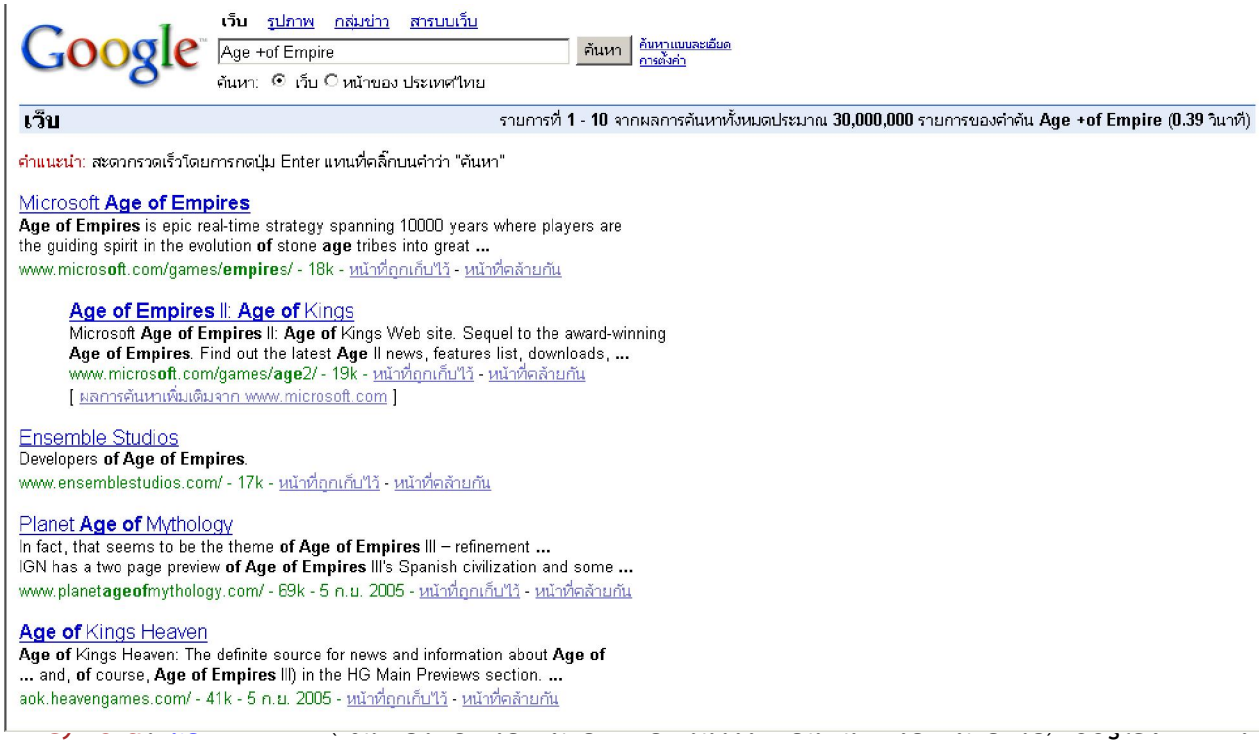
การค้นหาด้วยเครื่องหมายบวก (+)

เหมาะสำหรับการค้นหาคำKeywordที่มีลักษณะเป็นตัวเชื่อม เพราะโดยหลักการทำงานของGoogleแล้วGoogle จะไม่ค้นหาคำประเภทตัวเชื่อม เช่นat, with, on, what, when, where, how, the, to, ofถึงแม้ว่าเราจะมีการระบุเหล่านี้ลงในKeywordด้วยก็ตาม

ดังนั้นถ้าเราต้องการให้Googleทำการค้นหาคำเหล่านี้ด้วย เนื่องจากเป็นคำสำคัญของประโยคที่เราต้องการสามารถใช้เครื่องหมาย + ช่วยได้ โดยมีเงื่อนไข ว่า ก่อนหน้าเครื่องหมาย +ต้องมีการเว้นวรรค 1 เคาะด้วย เช่นถ้าต้องการค้นหาเว็บไซต์เกี่ยวกับเกมส์ที่มีชื่อว่าAge of Empireถ้าเราพิมพ์Keyword ...Age of Empire... Googleจะทำการค้นหาแยกคำโดยไม่สนใจofคืออาจจะค้นหาAgeหรือEmpireแค่ตัวเดียว แต่ถ้าเราระบุว่าAge +of EmpireGoogleจะทำการค้นหาทั้งคำว่าAge, of และ Empireเป็นต้น



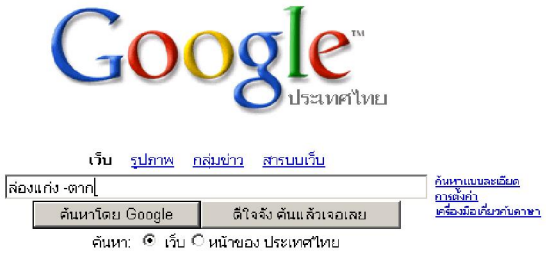
ภาพตัวอย่างการใช้เงื่อนไข (+)



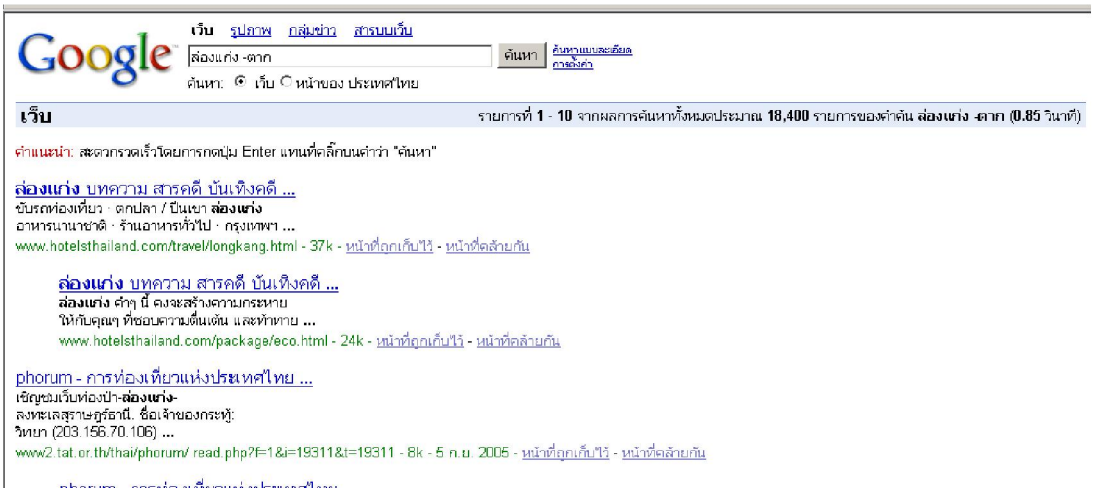
ด้ เช่น

นหา

เว็บไซต์ที่เกี่ยวกับการล่องแก่ง แต่ไม่มีจังหวัดตากเข้ามาเกี่ยวข้อง



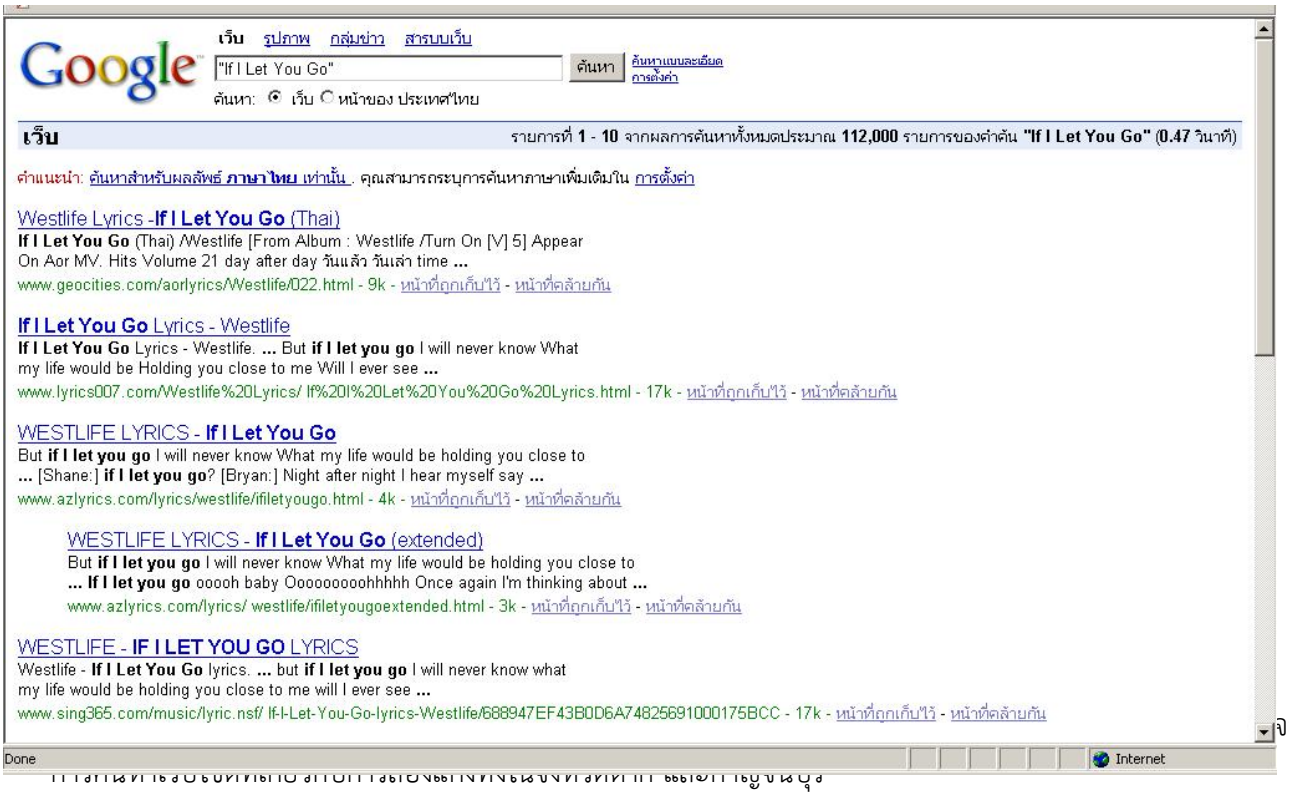
ภาพตัวอย่างการใช้เงื่อนไข (-)



การค้นหาด้วยเครื่องหมายคำพูด ("...")

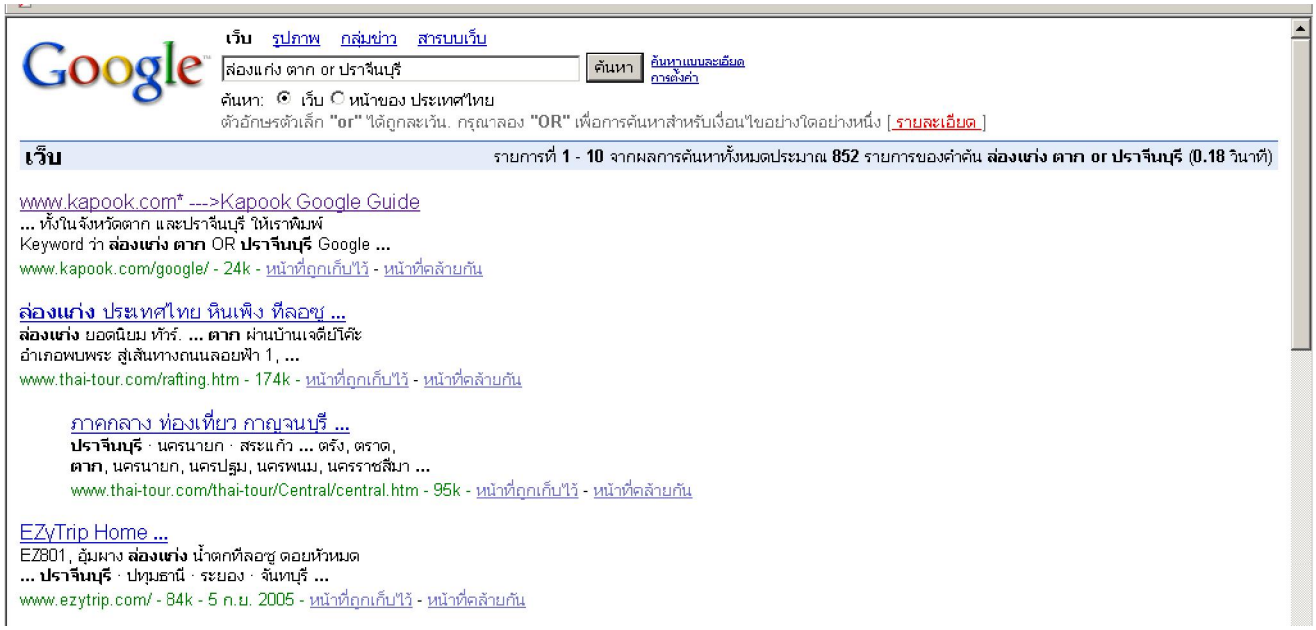
เหมาะสำหรับการค้นหาคำKeywordที่มีลักษณะเป็นประโยควลีที่เราต้องการให้มันแสดงผลทุกคำในประโยค โดยไม่แยกคำ เช่นถ้าเราต้องการหาเว็บไซต์เกี่ยวกับเพลงที่มีชื่อว่าIf I Let You Goให้พิมพ์ว่า"If I Let You Go" **Google**จะทำการค้นหาประโยค "If I Let You Go" ทั้งประโยคโดยไม่แยกคำค้นหา

ภาพตัวอย่างการใช้เงื่อนไข ("...")



จะทำ

ภาพตัวอย่างการใช้เงื่อนไข ("...")



รายละเอียดเพิ่มเติม ของ Google

1. Google จะใช้ and (และ) อยู่ในประโยคเสมอ เช่น ค้นหา harvest moon back to nature Google จะค้นหาแบบ harvest AND moon AND back... (พูดง่ายๆคือค้นหาแบบแยกคำ)
2. การใช้ OR (หรือ)คือการให้ Google หาข้อมูลมากขึ้นจาก คำA และ คำB (พูดง่ายๆ คือนำผลที่ได้มารวมกันรวมกัน) วิธีใช้ พิมพ์ OR ด้วยตัวใหญ่ระหว่างคำที่ต้องการ เช่น vacation london OR parisคือหาทั้งใน Londonและ Paris
3. Google จะละคำทั่วๆไป (เช่น the, to, of) และตัวอักษรเดี่ยวเพราะจะทำให้ค้นหาช้าลง แต่ถ้าคำพวกนั้นสามารถช่วยให้หาข้อมูลง่ายขึ้นก็ต้องใช้เครื่องหมาย + ช่วยโดยนำไปอยู่หน้าคำนั้น (ต้องเว้นวรรคก่อนด้วย) เช่น back +to natureหรือfinal fantasy +x
4. Google สามารถกันขอบเขตการค้นหาให้เล็กลงด้วยการใช้ Advanced Search หรือ การค้นหาแบบพิเศษ ใน Google ภาษาไทย

5. Google สามารถตัดคำพ้องรูปได้โดยใช้เครื่องหมาย - ช่วยโดยการนำไปอยู่คำที่จะตัด เช่น คำว่า bass มี 2 ความหมายคือ เกี่ยวกับปลาและดนตรีเราจะตัดที่มีความหมายเกี่ยวกับดนตรีออกโดยพิมพ์bass -music หมายความว่า bass ที่ไม่มีคำว่า music นอกจากนี้มันยังสามารถตัดอย่างอื่นได้อีก เช่น "front mission 3" -filetype:pdfหมายความว่า เรื่องเกี่ยวกับ front mission 3 แต่ไม่แสดงไฟล์ PDF
6. การค้นหาแบบทั้งวลี (คือการค้นหาทั้งกลุ่มคำ) ให้ใช้เครื่องหมาย " " เช่น "Breath of fire IV"
7. Google สามารถแปลเว็บภาษา Italian, French, Spanish, German, และ Portuguese เป็น ภาษาอังกฤษได้ (โดยคลิ้กที่คำว่า "Translate this page" ด้านข้างชื่อเว็บ)
8. Google สามารถหาไฟล์ในรูปแบบอื่นๆที่ไม่ใช่ HTML ได้ ประเภทไฟล์ที่รองรับคือ

- **Adobe Portable Document Format (นามสกุลของไฟล์ pdf)**
- **Adobe PostScript (นามสกุลของไฟล์ ps)**
- **Lotus 1-2-3 (นามสกุลของไฟล์ wk1, wk2, wk3, wk4, wk5, wki, wks, wku)**
- **Lotus WordPro (นามสกุลของไฟล์ lwp)**
- **MacWrite (นามสกุลของไฟล์ mw)**
- **Microsoft Excel (นามสกุลของไฟล์ xls)**
- **Microsoft PowerPoint (นามสกุลของไฟล์ ppt)**
- **Microsoft Word (นามสกุลของไฟล์ doc)**
- **Microsoft Works (นามสกุลของไฟล์ wks, wps, wdb)**
- **Microsoft Write (นามสกุลของไฟล์ wri)**
- **Rich Text Format (นามสกุลของไฟล์ rtf)**
- **Text (นามสกุลของไฟล์ ans หรือ txt)**

วิธีใช้ filetype: นามสกุลของไฟล์ เช่น "Chrono Cross" filetype:pdfหมายความว่าเอกสารของ Chrono Cross ที่เป็น PDF และมันยังมีความสามารถดูไฟล์เหล่านั้นในรูปแบบของ HTML ได้ (โดยคลิ้ก View as HTML หรือ รูปแบบ HTML ใน Google ไทย)

9. Google สามารถเก็บ Cached ของเว็บที่จะเข้าชมไว้ได้ (โดยคลิ้กที่ Cached หรือ ถูกเก็บไว้ ใน Google ภาษาไทย) ประโยชน์ของมันคือช่วยให้เราสามารถเข้าเว็บบางเว็บที่อาจโดนลบไปแล้วโดยข้อมูลที่ได้เป็นข้อมูลก่อนถูกลบ (ใหม่สุดที่มันจะมีได้)

10. Google สามารถค้นหาหน้าที่คล้ายกัน (โดยคลิ้ก Similar pages หรือ หน้าที่คล้ายกัน ใน Google ภาษาไทย) โดยจะค้นหาข้อมูลที่คล้ายๆ กันให้เรา เช่นถ้าเรากำลังหาข้อมูลการวิจัยความสามารถนี้จะช่วยให้หาข้อมูลได้มากมายในเวลาที่รวดเร็วโดยไม่ต้องเป็นห่วงเรื่อง keyword
11. Google สามารถค้นหา link ทั้งหมดที่เชื่อมไปยังเว็บนั้นได้ วิธีใช้ link:ชื่อ URL เช่น link:www.google.com แต่คุณไม่สามารถใช้ความสามารถนี้ร่วมกับการหาแบบอื่นๆ ได้
12. Google สามารถค้นหาเว็บที่จำเพาะเจาะจงได้ โดยพิมพ์ คำที่คุณต้องการเจาะจง site:ชื่อ URL เช่น ถ้าคุณต้องการหาเว็บเกี่ยวกับการเข้า (admission) มหาวิทยาลัย Stanford ให้พิมพ์admission site:www.stanford.edu

13. ถ้าคุณมีเวลาน้อย (และคิดว่าโชคดี) Google มีบริการการค้นหาด่วน (ชื่อบริการ I'm Feeling Lucky) โดยที่ Google จะนำเว็บที่อยู่ลำดับแรกของการค้นหา ส่งให้คุณเลย (link ไปเว็บนั้นให้เสร็จ) เช่น คุณต้องการค้นหาเว็บมหาวิทยาลัย Stanford อย่างด่วนให้พิมพ์ Stanford แล้วกด I'm Feeling Lucky หรือ ใช่เลย! เจอแน่ๆ ใน Google ไทย
14. Google สามารถหาแผนที่ของสหรัฐอเมริกาได้โดยพิมพ์ ที่อยู่ ชื่อถนน พร้อมด้วยชื่อรัฐเช่น 165 University AvePalo AltoCA Google จะจัดการส่งแผนที่คุณภาพสูงมาให้คุณ
15. Google สามารถหาเบอร์โทร (เฉพาะอเมริกา)หรือพิมพ์เบอร์โทรแล้วหาบริษัทได้โดยพิมพ์

- first name (or first initial), last name, city (state is optional)
- first name (or first initial), last name, state
- first name (or first initial), last name, area code
- first name (or first initial), last name, zip code
- phone number, including area code
- last name, city, state
- last name, zip code

แล้วแต่ว่าคุณจะใช้แบบไหน

16.Google สามารถค้นหา Catalog สินค้าได้ (เข้าไปที่http://catalogs.google.com)
17.Google สามารถเก็บข้อมูลลักษณะการใช้ที่คุณต้องการได้โดยเข้าไปที่Preferencesหรือตัวเลือกใน Google ไทย