การรักษาความปลอดภัยเครื่องคอมพิวเตอร์ของท่าน

กล่าวนำ

เครื่องคอมพิวเตอร์ของท่านนับว่าเป็นเป้าหมายอันดับต้นๆ ของเหล่าแฮคเกอร์ แครกเกอร์ หรือผู้ไม่ประสงค์ดีทั้งหลาย ซึ่งเราจะเรียกรวมๆ ว่า **“ผู้บุกรุก”** เหตุที่เป็นเช่นนี้ก็เนื่องจากผู้บุกรุกเหล่านั้นต้องการข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ของท่าน เช่น **รหัสผ่าน**ต่างๆ ข้อมูลใน**อีเมล์**ของท่าน ข้อมูลของบริษัททท่าน ข้อมูลส่วนตัวของท่าน หมายเลขบัตรเครดิต หมายเลขบัญชีธนาคาร และข้อมูลอื่นๆ ที่ผู้บุกรุกสามารถนำไปใช้ประโยชน์กับตัวเองได้

นอกจากข้อมูลต่างๆ ในเครื่องคอมพิวเตอร์ของท่านแล้ว อีกสิ่งหนึ่งที่มิได้มีความสำคัญด้อยไปกว่ากันเลยที่ผู้บุกรุกต้องการจากเครื่องคอมพิวเตอร์ของท่านก็คือทรัพยากรต่างๆ ของเครื่องคอมพิวเตอร์ของท่าน เช่น พื้นที่ว่างใน**ฮาร์ดดิสค์**ของท่าน ช่องทางการเชื่อมต่อสู่อินเทอร์เน็ตของท่าน การใช้เครื่องของท่านประมวลผลหรือทำงานต่างๆ หรือแม้กระทั่งใช้เครื่องของท่าน **“โจมตี”** เครื่องคอมพิวเตอร์เครื่องอื่นๆ ที่อยู่บนอินเทอร์เน็ตซึ่งการที่ผู้บุกรุกใช้เครื่องของท่านเป็นตัวแทนในการกระทำการต่างๆ ก็จะทำให้เป็นการยากที่จะสืบหาตัวผู้บุกรุกได้ และการโจมตีเหล่านี้ก็จะเกิดขึ้นโดยไม่รู้จบ

ท่านอาจจะสงสัยว่าเพราะเหตุใดผู้บุกรุกจึงเห็นว่าเครื่องคอมพิวเตอร์ส่วนตัวของท่านเป็นเป้าหมายที่น่าสนใจนัก และเพราะเหตุใดผู้บุกรุกเหล่านั้นจึงไม่ไปสนใจเครื่องใหญ่ๆ เช่น เครื่องเซิร์ฟเวอร์ใหญ่ๆ ขององค์กรใหญ่ๆ เป็นต้น เหตุผลก็คือโดยทั่วไปแล้วเครื่องคอมพิวเตอร์ส่วนตัวนั้นเป็นเป้าหมายที่โจมตีได้ง่ายเพราะมักจะไม่ได้รับการป้องกันอย่างเหมาะสมจากการโจมตี โดยเฉพาะเครื่องคอมพิวเตอร์ที่เชื่อมต่อกับอินเทอร์เน็ตผ่านทางเครือข่ายของบริษัท (office LAN) และเครื่องตามบ้านที่เชื่อมต่อกับอินเทอร์เน็ตความเร็วสูงทาง**เคเบิ้ลโมเด็ม**หรือ**ดีเอสแอลโมเด็ม** ที่มีการเชื่อมต่อกับอินเทอร์เน็ตตลอดเวลา (always on) อนึ่ง เครื่องคอมพิวเตอร์ที่เชื่อมต่อกับ อินเทอร์เน็ตผ่านทางสายโทรศัพท์โดยใช้โมเด็มธรรมดานั้นก็ไม่ได้ถือว่ามีความปลอดภัยจากการโจมตี เนื่องจากผู้บุกรุกจะโจมตีเครื่องเหล่านี้เช่นกัน

ไม่ว่าเครื่องของท่านจะเชื่อมต่อกับอินเทอร์เน็ตโดยวิธีใด หากผู้บุกรุกมีความตั้งใจที่จะโจมตีเครื่องของท่านแล้ว ผู้บุกรุกมักจะประสบความสำเร็จ ซึ่งโดยทั่วไปแล้วเจ้าของหรือผู้ใช้เครื่องคอมพิวเตอร์ส่วนตัวมักจะมิได้ตระหนักในเรื่องความปลอดภัยของเครื่องคอมพิวเตอร์ของตัวเอง ท่านควรจะต้องคำนึงถึงความปลอดภัยเมื่อใช้เครื่องคอมพิวเตอร์ของท่าน ไม่ต่างจากการคำนึงถึงความปลอดภัยเมื่อท่านขับรถยนต์หรือเดินข้ามถนน เอกสารนี้จะอธิบายให้ท่านทราบถึงหลักการ

ทำงานคร่าวๆ ของเครือข่ายอินเทอร์เน็ตและวิธีการป้องกันเครื่องคอมพิวเตอร์ของท่านจากผู้บุกรุกและจาก**โปรแกรม**ต่างๆ ที่ผู้บุกรุกจะส่งมายังเครื่องของท่าน

ผู้บุกรุกจะบุกรุกเข้ามาในเครื่องของท่านได้อย่างไร? ผู้บุกรุกสามารถเข้าถึงเครื่องของท่านได้หลายวิธี เช่น ใช้การส่งอีเมล์มาให้ท่าน เมื่อท่านอ่านอีเมล์นี้จะทำให้**ไวรัส**ที่อยู่ในอีเมล์เริ่มทำงานโดยตัวไวรัสจะสร้างช่องทางที่ผู้บุกรุกสามารถใช้ในการเข้าถึงเครื่องคอมพิวเตอร์ของท่านได้ หรือผู้บุกรุกอาจมองหาจุดด้อย จุดอ่อน หรือ ความอ่อนแอ ในโปรแกรมใดโปรแกรมหนึ่งที่ท่านใช้ (เรียกว่าเป็น **“ช่องโหว่”** ของโปรแกรม) แล้วใช้โปรแกรมที่สร้างขึ้นมาเป็นพิเศษเจาะที่ช่องโหว่นั้นเพื่อเข้าถึงเครื่องคอมพิวเตอร์ของท่าน

เมื่อผู้บุกรุกสามารถบุกเข้ามาในเครื่องคอมพิวเตอร์ของท่านได้แล้ว ผู้บุกรุกมักจะนำโปรแกรมของตัวเองมาลงไว้ในเครื่องของท่านเพื่อที่ว่าตนจะได้เข้ามาใช้เครื่องได้อีกในภายหลังถึงแม้ว่าท่านจะทราบถึงการบุกรุกนั้นแล้วปิดหรืออุดช่องโหว่ที่ผู้บุกรุกใช้ในตอนแรกก็จะไม่เป็นผล โปรแกรมเหล่านี้เราเรียกว่า “**ประตูลับ**” (backdoors) เนื่องจากทำหน้าที่คล้ายกับประตูลับให้ผู้บุกรุกเข้ามายังเครื่องของท่านได้อีกภายหลังโดยที่ท่านไม่ทราบว่ามีประตูลับนี้อยู่ โปรแกรมเหล่านี้มักจะได้รับการออกแบบมาให้ทำงานร่วมกับโปรแกรมเดิมของท่าน ดังนั้นจึงเป็นการยากมากที่จะตรวจจับหาโปรแกรมเหล่านี้ได้

ในหัวข้อถัดไปจะกล่าวถึงแนวคิดพื้นฐานของการรักษาความปลอดภัยเครื่องคอมพิวเตอร์ที่ท่านควรทราบ โดยจะเน้นในหัวข้อของคำว่า “ความเชื่อใจกัน” เนื้อหาหลักของเอกสารนี้จะกล่าวถึงหัวข้อความปลอดภัยต่างๆ ที่ท่านควรคำนึงถึง นอกจากนี้ในตอนท้ายของเอกสารจะมีรายชื่อของคำศัพท์และความหมายของคำศัพท์ทางด้านความปลอดภัยของคอมพิวเตอร์ที่ใช้ในเอกสารนี้

ไม่ว่าเครื่องคอมพิวเตอร์ของท่านจะเป็นระบบ ไมโครซอฟท์ วินโดวส์, แอปเปิ้ล แมค โอเอส, ลินุกซ์ หรือระบบอื่นๆ หัวข้อความปลอดภัยต่างๆ ก็จะเหมือนกันและจะไม่เปลี่ยนแปลงมากนักถึงแม้จะมีระบบรุ่นใหม่ๆ ออกมาอีก เนื่องจากหัวข้อความปลอดภัยต่างๆ ที่กล่าวถึงในเอกสารนี้เป็นหัวข้อความปลอดภัยพื้นฐานที่เป็นความจริงเสมอ โดยถ้าท่านมีความเข้าใจแล้วท่านจะสามารถจัดการกับเรื่องความปลอดภัยของเครื่องคอมพิวเตอร์ของท่านได้ไม่ว่าเครื่องของท่านจะเป็นระบบใด

แนวคิดพื้นฐานของการรักษาความปลอดภัยของเครื่องคอมพิวเตอร์

ก่อนที่จะเข้าสู่หัวข้อความปลอดภัยต่างๆ และสิ่งที่จะต้องทำเพื่อปกป้องเครื่องคอมพิวเตอร์ของท่านควรจะได้ทำความเข้าใจถึงความปลอดภัยของเครื่องคอมพิวเตอร์ก่อน และเพื่อให้เป็นการง่ายต่อ

การเข้าใจ เราจะเปรียบเทียบความปลอดภัยของเครื่องคอมพิวเตอร์กับสิ่งที่เราคุ้นเคยในชีวิตประจำวัน

ขอให้ท่านนึกเปรียบเทียบว่าเครื่องคอมพิวเตอร์ของท่านเป็นบ้าน คอนโดมิเนียม หรือ หอพักของท่าน สิ่งที่เกี่ยวกับความปลอดภัยในที่พักอาศัยของท่านจะมีอาทิเช่น ท่านทราบถึงรายละเอียดของที่พักอาศัยของท่านหรือไม่ เช่น ช่องทางเข้าออก ประตู หน้าต่าง และท่านได้ทำอะไรบ้างให้ที่พักอาศัยของท่านมีความปลอดภัยเพิ่มขึ้น (นับแต่จุดนี้ไป เราจะใช้การเปรียบเทียบที่ว่า “เครื่องคอมพิวเตอร์เปรียบเสมือนบ้านหลังหนึ่ง” ไปตลอดทั้งเอกสารนี้)

ยกตัวอย่างด้านความปลอดภัยในที่พักอาศัย เช่น ท่านอาจทราบว่าหากท่านพูดคุยกันเสียงดังภายในบ้าน คนที่อยู่ข้างนอกก็อาจจะได้ยิน ท่านอาจจะตรวจสอบว่าได้ล็อคประตูหน้าต่างทุกบานเรียบร้อยแล้วก่อนที่ท่านจะออกจากบ้าน ท่านคงไม่ได้ให้กุญแจบ้านของท่านกับคนที่ท่านไม่รู้จัก และบางท่านอาจจะติดตั้งระบบสัญญาณกันขโมยเพื่อเสริมความปลอดภัยให้บ้านของท่าน สิ่งที่กล่าวมาเหล่านี้เป็นตัวอย่างหัวข้อด้านความปลอดภัยในที่พักอาศัยซึ่งเราไม่สามารถปฏิเสธได้ว่าเป็นสิ่งที่เราจะต้องปฏิบัติหากเราต้องการจะอาศัยอยู่ในที่นั้นอย่างปลอดภัย

ต่อมาเราจะนำแนวคิดที่กล่าวมาในย่อหน้าที่แล้วมาใช้กับเครื่องคอมพิวเตอร์ของท่าน *สิ่งที่ท่านควรทราบ*คือ การส่งอีเมล์ **ข้อความอิเล็กทรอนิกส์** และ ข้อมูลส่วนใหญ่ไปในเครือข่ายอินเทอร์เน็ตนั้นเป็นการส่งไปอย่างโล่งๆ ซึ่งหมายความว่าผู้ใดก็ตามที่ดักจับข้อมูลของท่านได้จะสามารถอ่านหรือเปลี่ยนแปลงข้อมูลของท่านได้ ดังนั้น *สิ่งที่ท่านควรปฏิบัติ*คือ ใช้ความระมัดระวังในการส่งข้อมูลใดๆ และระมัดระวังในการอ่านและเชื่อถือข้อความใดๆที่มาจากอินเทอร์เน็ตและ *สิ่งที่ท่านควรติดตั้ง*คือ ติดตั้งโปรแกรม**ไฟร์วอล** โปรแกรมต่อต้านไวรัส **โปรแกรมอุดช่องโหว่** และ โปรแกรม**เข้ารหัส**ข้อมูล เพื่อเสริมความปลอดภัยให้กับเครื่องคอมพิวเตอร์ของท่าน

ในส่วนต่อๆไปของเอกสารนี้จะกล่าวถึงสามสิ่งด้านบนคือสิ่งที่ท่านควรทราบ ควรปฏิบัติ และควรติดตั้ง เพื่อเสริมความปลอดภัยให้กับเครื่องคอมพิวเตอร์ของท่าน

สิ่งที่ท่านควรทราบ

ในการที่เราจะสามารถแก้ปัญหาด้านความปลอดภัยของคอมพิวเตอร์ได้นั้นเราจะต้องทราบลักษณะการทำงานของเครือข่ายอินเทอร์เน็ตและเทคโนโลยีต่างๆ ที่เกี่ยวข้องก่อน หากเราทราบลักษณะการทำงานของสิ่งเหล่านี้แล้วเราจะสามารถหาวิธีแก้ไขปัญหาต่างๆที่เกิดขึ้นได้และยังทำให้เราใช้เครือข่ายอินเทอร์เน็ตได้อย่างปลอดภัยและเหมาะสมยิ่งขึ้น ในหัวข้อนี้จะกล่าวถึงความเชื่อใจกันและการส่งข้อมูลไปอย่างโล่งๆ

ความเชื่อใจกัน

โดยธรรมชาติแล้วมนุษย์เรามักจะเชื่อในสิ่งต่างๆที่เราได้ประสบ ยกตัวอย่างเช่น โดยส่วนมากแล้วเราจะเชื่อสิ่งที่เราได้ฟังจากวิทยุ สิ่งที่เราได้รับชมจากโทรทัศน์ และสิ่งที่เราได้อ่านจากหนังสือพิมพ์ เราเชื่อสลากที่ติดบนสินค้า เราเชื่อบุพการีของเรา เชื่อคู่ครองของเรา เชื่อลูกหลานของเรา เราเชื่อผู้ร่วมงานของเรา โดยเรามักจะคิดว่าคนที่ชอบระแวงและไม่ค่อยเชื่อใครนั้นน่าจะเป็นโรคประสาทและเป็นผลให้เราไม่เชื่อความเห็นของคนคนนั้นนัก

เครือข่ายอินเทอร์เน็ตนั้นแรกเริ่มถูกสร้างขึ้นมาโดยมีพื้นฐานอยู่บนความเชื่อใจกัน ในปี คศ. 1960-70 นั้นเครื่องคอมพิวเตอร์มีจำนวนน้อย มีราคาแพงมาก และทำงานได้ค่อนข้างช้า (เมื่อเทียบกับปัจจุบัน) แต่ก็มีประโยชน์แก่งานวิจัยและการศึกษามาก ดังนั้นรัฐบาลประเทศสหรัฐอเมริกาจึงได้ให้เงินทุนในการวิจัยระบบเครือข่ายที่จะสามารถทำให้มีการร่วมกันใช้เครื่องคอมพิวเตอร์จำนวนน้อยเหล่านี้ได้ทั่วประเทศ โครงการวิจัยนี้มีชื่อว่า**อาร์พาเน็ต** (ARPAnet) ซึ่งมาจากชื่อของหน่วยงานวิจัยของสหรัฐอเมริกาที่ชื่อว่า ARPA หรือ Advanced Research Projects Agency ซึ่งเป็นผู้รับผิดชอบและให้งบประมาณแก่โครงการนี้

หลักสำคัญในการใช้งานอาร์พาเน็ตก็คือความเชื่อใจกันของผู้ใช้เครือข่าย ซึ่งในสมัยนั้นยังไม่มีความคิดใดๆที่จะกระทำการอันมิชอบขึ้นในเครือข่ายนี้ การสื่อสารภายในเครือข่ายระหว่างเครื่องคอมพิวเตอร์ในสมัยนั้นจะเป็นไปตามกฎเกณฑ์ง่ายๆที่วางไว้โดยเชื่อว่าผู้ใช้ทุกคนจะปฏิบัติตามกฎเหล่านั้น โดยเป็นไปตามแนวคิดที่ว่าให้เกิดการแบ่งปันทรัพยากรและความรู้ให้ได้ง่ายและมีประสิทธิภาพมากที่สุด ซึ่งแนวคิดนี้ส่งผลมาถึงแนวทางปฏิบัติ กฎเกณฑ์ และเทคโนโลยี ที่ใช้กันอยู่ในเครือข่ายอินเทอร์เน็ตในปัจจุบัน

ในช่วงไม่กี่ปีที่ผ่านมานี้เริ่มมีการใช้เครือข่ายอินเทอร์เน็ตใน**การค้าทางอิเล็กทรอนิกส์** (e-commerce) อย่างแพร่หลายและเมื่อมีผลประโยชน์ทางการค้าเข้ามาเกี่ยวข้อง การใช้หลักความเชื่อใจกันนั้นเริ่มจะไม่เพียงพอ ซึ่งทำให้นับแต่ในยุคของอาร์พาเน็ต ได้มีการเปลี่ยนแปลงต่างๆเกิดขึ้นเช่น การเปลี่ยนแปลงวิธีที่เราใช้ระบบเครือข่ายและการเปลี่ยนแปลงทางเทคโนโลยีต่างๆ ทั้งนี้ก็เพื่อที่จะเสริมความปลอดภัยในการใช้เครือข่ายอินเทอร์เน็ตและให้เราสามารถเชื่อถือในเครือข่ายนี้ได้

เราอาจมองภาพความปลอดภัยของเครือข่ายโดยดูจากตัวอย่างในชีวิตประจำวัน เช่น เมื่อเราได้รับจดหมายผ่านทางไปรษณีย์ ซองจดหมายและตัวจดหมายก็อาจจะมีชื่อและที่อยู่ของผู้ส่ง ท่านเคยสงสัยหรือไม่ว่าชื่อที่อยู่เหล่านี้เป็นชื่อที่อยู่ที่แท้จริง กล่าวคือเป็นชื่อที่อยู่ของผู้ที่ส่งจดหมายนั้น

จริงๆหรือไม่ ท่านอาจตรวจสอบถึงความถูกต้องของชื่อที่อยู่นั้นได้ แต่ก็ไม่ใช่เป็นเรื่องง่ายที่จะทำได้ ท่านอาจจะโทรศัพท์ไปยังหมายเลขโทรศัพท์ที่อยู่บนซองจดหมายนั้น (หากมี) แต่ท่านไม่สามารถแน่ใจได้ว่าหมายเลขโทรศัพท์นั้นเป็นหมายเลขโทรศัพท์ที่แท้จริงและผู้รับสายเป็นตัวจริงหรือไม่ หรือท่านอาจโทรศัพท์ติดต่อไปยังหมายเลขสอบถามหรือให้ตำรวจตรวจสอบให้ซึ่งอาจจะช่วยในการตรวจสอบได้ แต่การกระทำเช่นนี้มีความยุ่งยากมากจะต้องใช้เวลามากและคนส่วนใหญ่ก็ไม่สนใจที่จะทำ

นอกจากชื่อที่อยู่บนจดหมายแล้ว ยังมีข้อมูลอื่นๆอีกมากมายที่ท่านจะได้พบเห็น อาทิเช่น สลากที่ติดบนอาหาร โฆษณา หรือข่าว ข้อมูลเหล่านี้มีความถูกต้องหรือไม่ และท่านจะมีวิธีตรวจสอบข้อมูลเหล่านั้นได้อย่างไร

ข้อมูลบนเครือข่ายอินเทอร์เน็ตนั้นก็คล้ายกับข้อมูลที่เราได้พบเห็นในชีวิตประจำวัน ซึ่งตัวอย่างที่เห็นได้ชัดเจนที่สุดก็คืออีเมล์ซึ่งผู้บุกรุกสามารถปลอมแปลงชื่อที่อยู่ของผู้ส่งได้ ซึ่งเราเรียกการกระทำเช่นนี้ว่าการ **“ปลอมแปลง”** (spoofing) การปลอมแปลงนี้สามารถทำได้กับข้อมูลอื่นๆ ที่ส่งไปในอินเทอร์เน็ตได้นอกเหนือจากอีเมล์ด้วย เช่น การปลอมแปลง **“แพ็คเก็ต”** ซึ่งเป็นหน่วยข้อมูลพื้นฐานของเครือข่ายอินเทอร์เน็ตนั้นสามารถกระทำได้โดยง่าย

จากที่ได้กล่าวมาข้างต้นนั้น สิ่งที่ท่านต้องตระหนักอยู่เสมอคือ ท่านไม่สามารถจะเชื่อถือในข้อมูลที่ได้รับมาจากเครื่องคอมพิวเตอร์อื่นผ่านทางอินเทอร์เน็ตได้อย่างเต็มที่โดยไม่มีเงื่อนไขเพราะความเชื่อถือนั้นอาจทำให้เกิดความสูญเสียขึ้นได้ ยกตัวอย่างเช่น ถ้าท่านเชื่อที่จะเปิดข้อความอีเมล์ที่มีไวรัสอยู่ อาจทำให้ไวรัสนั้นแพร่กระจายมาบนเครื่องคอมพิวเตอร์ของท่าน ซึ่งไวรัสนั้นอาจทำลาย **“ไฟล์”** ของท่านและทำให้ท่านสูญเสียข้อมูลที่สำคัญได้

หลักการทำงานของอินเทอร์เน็ตนั้นเริ่มต้นจากรากฐานของความเชื่อใจกัน ซึ่งเท่าที่ผ่านมานั้นมีการเปลี่ยนแปลงทางเทคโนโลยีในด้านนี้ซึ่งอาจช่วยให้เราสามารถเชื่อถือระบบอินเทอร์เน็ตได้มากกว่าเดิม แต่อย่างไรก็ตามเราควรพึงระลึกอยู่เสมอว่าก่อนที่จะเชื่อข้อมูลใดๆ ควรจะมีความสงสัยและใช้ความระมัดระวังอยู่เสมอ

การส่งข้อมูลไปโล่งๆ

หากท่านมีการสนทนากับอีกคนหนึ่งในบ้านของท่าน เป็นที่แน่นอนว่าทุกคนที่อยู่ในระยะที่ใกล้พอจะได้ยินและเข้าใจบทสนทนานั้น หากการสนทนานั้นใช้เสียงพูดที่ดังและท่านเปิดหน้าต่างหรือประตูไว้ ผู้คนที่ผ่านไปมาก็อาจได้ยินด้วย ซึ่งหากท่านต้องการความเป็นส่วนตัวท่านอาจต้องย้ายไปอยู่อีกห้องหนึ่งแล้วปิดประตูหน้าต่างเพื่อไม่ให้ใครได้ยินบทสนทนานี้

การสื่อสารผ่านทางระบบอินเทอร์เน็ตนั้นก็คล้ายกับการสนทนาในห้องที่กล่าวมาข้างต้น เพียงแต่ว่าห้องในกรณีนี้จะเป็นห้องที่ใหญ่มาก และการที่ท่านส่งข้อมูลใดๆ เช่น อีเมล์หรือข้อความ chat ไปยังผู้รับนั้น ข้อมูลของท่านไม่ได้ถูกส่งไปยังเครื่องคอมพิวเตอร์ของผู้รับโดยตรง แต่จะถูกส่งผ่านต่อไปยังเครื่องคอมพิวเตอร์ต่างๆมากมายก่อนที่จะถึงเครื่องคอมพิวเตอร์ของผู้รับ เราอาจเปรียบเทียบเครื่องคอมพิวเตอร์รายทางแต่ละเครื่องว่าเป็นห้องห้องหนึ่งได้

ดังนั้นใครก็ตามหรือโปรแกรมใดก็ตามที่อยู่ในเครื่องคอมพิวเตอร์หรือห้องเหล่านั้นจะสามารถ “ได้ยิน” คืออ่านและเข้าใจข้อมูลที่ท่านส่งได้ เนื่องจากการส่งข้อมูลในอินเทอร์เน็ตส่วนใหญ่นั้นเป็นการส่งไปโล่งๆ คือไม่มีการปกปิดใดๆ

ซึ่งที่กล่าวมาคือการหลักทำงานของระบบอินเทอร์เน็ตดังนั้นท่านควรจะต้องทราบถึงหลักการทำงานนี้ และตระหนักว่าการที่ท่านส่งข้อมูลผ่านทางอินเทอร์เน็ตนั้น จะมี **ความเสี่ยง** อยู่เสมอที่จะมีผู้ดักฟังหรือดักจับข้อมูลของท่านเพื่อนำไปใช้เป็นผลประโยชน์ของผู้นั้นเอง

สิ่งที่ท่านควรปฏิบัติเพื่อทำให้เครื่องคอมพิวเตอร์ของท่านปลอดภัย

การทำให้เครื่องคอมพิวเตอร์ของท่านมีความปลอดภัยนั้นมิใช่สิ่งที่กระทำได้โดยง่าย มีหัวข้อต่างๆมากมายที่ท่านต้องพิจารณาและมีขั้นตอนต่างๆมากมายที่ท่านจะต้องปฏิบัติ ซึ่งการสิ่งเหล่านี้จะต้องใช้เวลาในการเรียนรู้และปฏิบัติ หากเป็นไปได้โปรดอ่านเอกสารนี้ทั้งเอกสารก่อนที่ท่านจะเริ่มสร้างความปลอดภัยให้เครื่องของท่าน เพื่อที่ท่านจะได้มีความเข้าใจที่ดีขึ้นถึงสิ่งต่างๆที่ท่านต้องปฏิบัติ

ในส่วนต่อไปของเอกสารนี้จะอธิบายถึงกิจกรรมสองประเภทด้วยกันที่ท่านสามารถปฏิบัติเพื่อให้เกิดความปลอดภัยกับเครื่องคอมพิวเตอร์ของท่าน กิจกรรมประเภทแรกนั้นเป็นกิจกรรมที่ท่านสามารถปฏิบัติได้เลยโดยใช้โปรแกรมต่างๆที่อยู่ในเครื่องคอมพิวเตอร์ของท่านอยู่แล้ว เช่น การจัดการเรื่อง **รหัสผ่าน** การแนบไฟล์ไปกับอีเมล์ (email attachment) การสั่งโปรแกรมให้ทำงาน และการเก็บ**สำรอง**งานของท่าน ส่วนกิจกรรมอีกประเภทหนึ่งนั้นท่านอาจจะต้องใช้โปรแกรมพิเศษมาช่วยในการปฏิบัติ เช่น การอุดช่องโหว่ของโปรแกรม การใช้โปรแกรมป้องกันไวรัส การใช้ไฟร์วอลและการใช้โปรแกรมเข้ารหัสลับ เป็นต้น

ต่อไปนี้จะเป็นสิ่งต่างๆที่ท่านจะต้องปฏิบัติเพื่อที่จะให้เครื่องคอมพิวเตอร์ของท่านมีความปลอดภัย ข้อปฏิบัติเหล่านี้ถูกจัดเรียงตามพฤติกรรมของผู้บุกรุกโดยจะเริ่มจากวิธีโจมตีที่เกิดขึ้นบ่อยที่สุด ซึ่ง

หากท่านเริ่มปฏิบัติไปตามหัวข้อตามที่เรียงลำดับไว้นี้ท่านจะได้แก้ปัญหาใหญ่ที่สุดก่อนแล้วแก้ปัญหาอื่นๆลดหลั่นลงไปตามลำดับความสำคัญ

ข้อปฏิบัติที่ 1 – ติดตั้งและใช้โปรแกรมป้องกันไวรัส

หากมีคนมากดกริ่งที่ประตูบ้านท่านและต้องการที่จะเข้ามาในบ้านท่านเพื่อจะขายสินค้าหรือใช้โทรศัพท์ของท่าน ท่านคงต้องตัดสินใจว่าจะให้ผู้นั้นเข้ามาในบ้านหรือไม่ ซึ่งถ้าผู้นั้นเป็นคนรู้จักหรือเป็นเพื่อนบ้านท่านก็คงจะยอมให้เข้ามา หรือถ้าท่านเห็นว่าผู้นั้นมีความน่าเชื่อถือเพียงพอ ท่านก็อาจจะยอมให้ผู้นั้นเข้ามาในบ้านเช่นกัน แต่อาจจะเฝ้าดูผู้นั้นด้วยความระมัดระวังในขณะที่เขาอยู่ในบ้านท่าน

สิ่งที่ท่านปฏิบัติในที่นี้คือ ท่านสำรวจลักษณะของบุคคลที่มากดกริ่งที่ประตูบ้านท่าน และท่านตัดสินใจว่าจะให้ผู้นั้นเข้าบ้านหรือไม่โดยดูจากลักษณะที่ท่านสำรวจมาได้ เนื่องจากการที่จะอนุญาตให้ใครเข้ามาในบ้านนั้นเป็นความรับผิดชอบโดยตรงของท่าน นอกจากนี้ท่านยังอาจต้องสอนลูกหลานหรือคนอื่นๆในบ้านว่าจะปฏิบัติอย่างไรหากมีคนแปลกหน้ามากดกริ่งที่ประตูบ้าน

โปรแกรมป้องกันไวรัสมีหลักการทำงานคล้ายคลึงกับสถานการณ์ที่กล่าวมาข้างต้น ตัวโปรแกรมจะตรวจสอบเนื้อหาของไฟล์และมองหารูปแบบเฉพาะที่ตรงกับลักษณะของไวรัส เราเรียกรูปแบบเฉพาะนี้ว่า **“ลายมือของไวรัส”** (virus signature) เมื่อโปรแกรมป้องกันไวรัสตรวจพบไฟล์ที่มีลายมือของไวรัสอยู่ ตัวโปรแกรมก็จะมีหนทางปฏิบัติต่างๆให้ท่านเลือก เช่น ลบเฉพาะส่วนที่เป็นไวรัสของไฟล์นั้นหรือลบไฟล์นั้นทั้งไฟล์ เป็นต้น

เพื่อให้เกิดความเข้าใจในการทำงานของโปรแกรมป้องกันไวรัสเราอาจใช้การเปรียบเทียบโดยนึกภาพถึงพวกมิจฉาชีพที่หลอกหลวงคนทั่วไปหรือพวก 18 มงกุฎ พวกนี้จะมายังบ้านของท่านและพยายามจะขายสินค้าหลอกลวงให้ท่านหรือพยายามที่จะเข้ามาในบ้านของท่าน เมื่อสามารถเข้ามาในบ้านท่านได้แล้วก็อาจจะขโมยของท่านหรือทำอันตรายต่อท่าน

มีหลายวิธีด้วยกันที่ท่านจะสามารถทราบได้ว่ามีเหล่ามิจฉาชีพเหล่านี้อยู่ในบริเวณบ้านของท่านหรือไม่ เช่น ท่านอาจจะอ่านพบในข่าวหนังสือพิมพ์หรือดูจากข่าวในโทรทัศน์ โดยในข่าวจะมีรายละเอียดต่างๆเช่น รูปภาพ หรือวิธีการหลอกลวงของคนกลุ่มนี้ ซึ่งถือได้ว่าข่าวนั้นเป็นแหล่งบอกลักษณะเฉพาะของพวกมิจฉาชีพเหล่านี้ที่ท่านจะต้องมีความระมัดระวังเมื่อเจอคนที่มีลักษณะเหล่านี้ จนกระทั่งเวลาผ่านไปนานพอและเรื่องเงียบไปหรือจนกระทั่งท่านได้ข่าวว่าคนเหล่านี้ถูกจับได้แล้วท่านจึงอาจผ่อนคลายความระมัดระวังลงได้

โปรแกรมป้องกันไวรัสมีหลักการทำงานคล้ายคลึงกับสถานการณ์ที่กล่าวมาข้างต้น เมื่อใดก็ตามที่ผู้ขายโปรแกรมป้องกันไวรัสทราบถึงไวรัสตัวใหม่ๆ ผู้ขายจะออกรายชื่อทั้งหมดของลายมือไวรัสฉบับแก้ไขล่าสุดมาซึ่งจะรวมเอาลายมือของไวรัสตัวล่าสุดนี้ไว้ด้วย ซึ่งเมื่อโปรแกรมป้องกันไวรัสที่อยู่บนเครื่องของท่านได้รับรายชื่อฉบับใหม่นี้แล้ว (อาจโดยการที่ท่านนำมาติดตั้งหรือตัวโปรแกรมติดตั้งเองโดยอัตโนมัติ) ก็จะตรวจหาไฟล์ที่มีไวรัสใหม่นี้โดยอัตโนมัตินอกจากนั้นก็จะตรวจหาไวรัสตัวเก่าๆไปพร้อมกันด้วย แต่ไวรัสนั้นไม่เหมือนกับพวกมิจฉาชีพคือไม่มีทางที่ไวรัสจะหายไปโดยสิ้นเชิง ดังนั้นโปรแกรมป้องกันไวรัสจะยังคงเก็บลายมือของไวรัสเก่าๆไว้ทั้งหมด

ต่อไปขอให้ท่านนึกถึงสถานการณ์ว่าหากมีพวกมิจฉาชีพมาอยู่ที่หน้าประตูบ้านท่าน ท่านจะทำอย่างไร ท่านคงไม่ซื้อสินค้าหรือเชิญพวกนี้เข้าบ้านแต่ในขณะเดียวกันท่านก็อาจจะไม่อยากทำให้พวกนี้รู้ตัวหรือโมโห ดังนั้นท่านอาจจะรับฟังคำชักจูงต่างๆแล้วก็ปฏิเสธไป หลังจากที่พวกนี้ไปแล้วท่านก็อาจจะโทรศัพท์แจ้งตำรวจหรือหน่วยงานที่เกี่ยวข้อง

เช่นเดียวกันกับพวกมิจฉาชีพ ท่านจะมีทางเลือกว่าจะปฏิบัติอย่างไรเมื่อท่านพบไวรัสบนเครื่องคอมพิวเตอร์ของท่าน สำหรับไวรัสบางตัวท่านอาจจะสามารถลบไวรัสทิ้งจากไฟล์ที่ติดไวรัสได้ แต่สำหรับไวรัสบางตัวท่านอาจต้องลบไฟล์ทั้งไฟล์ทิ้งแล้วติดตั้งไฟล์นั้นใหม่ ทางเลือกของท่านนั้นจะขึ้นอยู่กับชนิดของไวรัสที่พบและชนิดของโปรแกรมป้องกันไวรัสของท่าน

สิ่งต่างๆ สามารถเข้ามาสู่บ้านท่านได้สองทางคือ คนที่มาหาท่านเข้าทางประตูบ้านและจดหมายหรือพัสดุที่ท่านได้รับทางไปรษณีย์ ก่อนที่ท่านจะยอมให้สิ่งเหล่านี้เข้ามาในบ้านท่านจะต้องตรวจสอบก่อน ซึ่งการตรวจสอบนี้ในบางกรณีท่านจะตรวจสอบโดยละเอียดส่วนบางกรณีท่านก็จะตรวจสอบโดยผ่านๆ

ส่วนไวรัสนั้นสามารถเข้ามาสู่เครื่องคอมพิวเตอร์ของท่านได้หลายทางด้วยกัน คือผ่านทางดิสเกตต์ **ซีดี-รอม** อีเมล์ เว็บต่างๆ และไฟล์ต่างๆที่ท่าน**ดาวน์โหลด**มา ซึ่งก่อนที่จะใช้งานท่านจะต้องตรวจสอบสิ่งเหล่านี้ก่อน กล่าวคือ ท่านต้องตรวจหาไวรัสที่แผ่นดิสเกตต์เมื่อนำดิสเกตต์มาใช้กับเครื่องคอมพิวเตอร์ของท่าน ท่านต้องตรวจหาไวรัสที่อีเมล์เมื่อได้รับอีเมล์ (รายละเอียดอยู่ในข้อปฏิบัติที่ 3) ตรวจหาไวรัสในทุกไฟล์ที่ท่านดาวน์โหลดมาจากอินเทอร์เน็ตซึ่งท่านอาจสามารถตั้งค่าในโปรแกรมป้องกันไวรัสของท่านให้ตรวจหาไวรัสในที่เหล่านี้ได้ ซึ่งตัวโปรแกรมจะสามารถตรวจหาไวรัสให้ได้โดยอัตโนมัติ

ท่านอาจเดินตรวจตรารอบๆ บ้านท่านเพื่อดูว่ามีอะไรผิดปกติหรือเสียหายหรือไม่เป็นครั้งคราว ในทำนองเดียวกันนี้ ท่านก็ควรจะต้อง “เดินตรวจตรา” ในเครื่องคอมพิวเตอร์ของท่านเพื่อตรวจดูว่ามีไวรัสซ่อนอยู่หรือไม่ โปรแกรมป้องกันไวรัสส่วนใหญ่จะสามารถถูกตั้งค่าให้ตรวจหาไวรัสโดย

อัตโนมัติเป็นประจำ เช่น ท่านอาจตั้งค่าให้มีการตรวจหาไวรัสทุกๆ 1 วัน ซึ่งถ้าท่านเปิดเครื่องคอมพิวเตอร์ของท่านไว้ในเวลากลางคืนท่านก็สามารถตั้งค่าให้มีการตรวจหาไวรัสทุกๆคืนได้

โปรแกรมป้องกันไวรัสบางโปรแกรมมีขีดความสามารถเพิ่มเติมพิเศษที่จะสามารถตรวจหาไวรัสได้โดยใช้วิธีอื่นนอกเหนือจากการตรวจสอบลายมือของไวรัส เนื่องจากไวรัสบางตัวจะไม่มีลายมือที่ชัดเจนหรือยังไม่มีการตรวจพบลายมือของไวรัสนั้นแต่จะมีพฤติกรรมที่เป็นไวรัสอยู่ โปรแกรมที่มีขีดความสามารถนี้จะสามารถเรียนรู้และตรวจจับพฤติกรรมนี้ได้และจะรายงานการตรวจพบให้ท่านทราบ ทั้งนี้ก็คล้ายกับการที่มีคนมากดกริ่งหน้าประตูบ้านท่านและถึงแม้ท่านจะไม่มีหลักฐานแน่ชัดว่าเขาเป็นพวกมิจฉาชีพแต่จากประสบการณ์และความรู้สึกของท่านแล้วท่านไม่อยากที่จะต้อนรับคนคนนั้น การตรวจหาไวรัสวิธีนี้เรียกว่าการตรวจหาแบบ **“การเรียนรู้”** (heuristics) ซึ่งจะช่วยให้มีการตรวจหาไวรัสชนิดใหม่ๆได้

โดยทั่วไปแล้วท่านจะต้องติดตั้งโปรแกรมป้องกันไวรัสเองหลังจากที่ท่านได้รับหรือซื้อเครื่องคอมพิวเตอร์เครื่องใหม่ ซึ่งในท้องตลาดจะมีโปรแกรมป้องกันไวรัสอยู่หลากหลายยี่ห้อ ดังนั้นในการเลือกซื้อโปรแกรมป้องกันไวรัสนั้นท่านควรจะประเมินแต่ละโปรแกรมโดยพิจารณาในหัวข้อต่างๆต่อไปนี้

1. ต้องการ – ท่านสามารถตรวจสอบไฟล์ใดๆได้เมื่อใดก็ตามที่ท่านต้องการหรือไม่
2. ปรับปรุง – ท่านสามารถตั้งค่าให้มีการปรับปรุงรายชื่อลายมือไวรัสได้โดยอัตโนมัติหรือไม่ หากปรับปรุงได้วันละครั้งจะเป็นการดีมาก
3. ทางเลือก – เมื่อพบไวรัสแล้ว ท่านมีทางเลือกใดบ้างที่จะจัดการกับไวรัสนั้น โปรแกรมสามารถขจัดไวรัสโดยไม่ต้องลบไฟล์หรือไม่
4. ตรวจสอบ – ท่านสามารถตรวจสอบไฟล์ทุกไฟล์ที่เข้ามายังเครื่องคอมพิวเตอร์ของท่านหรือไม่ (ไม่ว่าไฟล์นั้นจะเข้ามาทางช่องทางใด) และโปรแกรมสามารถตรวจสอบได้โดยอัตโนมัติหรือไม่
5. เรียนรู้ – โปรแกรมมีขีดความสามารถในการตรวจหาไวรัสใหม่ๆโดยวิธีการเรียนรู้หรือไม่

ท่านควรใช้ข้อพิจารณาเหล่านี้ในการเลือกซื้อโปรแกรมต่อต้านไวรัส เมื่อท่านได้ซื้อโปรแกรมมาแล้วท่านควรจะติดตั้งโปรแกรมลงบนเครื่องคอมพิวเตอร์ของท่านแล้วใช้โปรแกรมอย่างเต็มความสามารถของตัวโปรแกรม

โดยทั่วไปแล้วการโจมตีจากผู้บุกรุกโดยใช้ไวรัสและ**หนอน**นั้นจะเป็นการโจมตีที่ประสบผลสำเร็จมากที่สุด ดังนั้นการติดตั้งโปรแกรมป้องกันไวรัสและคอยปรับปรุงให้โปรแกรมทันสมัยล่าสุดนับว่าเป็นวิธีหนึ่งที่ดีที่สุดในการป้องกันเครื่องคอมพิวเตอร์ของท่านไม่ให้ถูกโจมตี โดยเฉพาะอย่างยิ่ง

ในกรณีที่มีงบประมาณอันจำกัดแล้ว การจ่ายเงินเพื่อซื้อโปรแกรมป้องกันไวรัสถือว่าเป็นการลงทุนที่คุ้มค่าที่สุด

ข้อปฏิบัติที่ 2 – อุดช่องโหว่ในเครื่องคอมพิวเตอร์ของท่าน

หากเครื่องใช้ในบ้านของท่านเสีย ท่านก็คงนำเครื่องใช้นั้นไปซ่อม ซึ่งท่านอาจนำเครื่องใช้นั้นไปที่ร้านหรือโทรศัพท์หาช่างแล้วถามราคาค่าซ่อมก่อน เมื่อทราบราคาแล้วท่านจะตัดสินใจว่าจะซ่อมเครื่องนั้นหรือจะเปลี่ยนเครื่องใหม่ ซึ่งผลลัพธ์สุดท้ายที่ท่านต้องการก็คือมีเครื่องใช้ในบ้านนั้นที่ทำงานได้เหมือนเดิม

นำแนวคิดนี้มาใช้กับเครื่องคอมพิวเตอร์ของท่าน ท่านควรจะทำอย่างไรเมื่อซอฟท์แวร์ โปรแกรม หรือ **ระบบปฏิบัติการ** ในเครื่องคอมพิวเตอร์ของท่าน (“เครื่องใช้ในบ้าน”) เสีย ท่านจะทำอย่างไรให้ซอฟท์แวร์ โปรแกรมหรือระบบปฏิบัติการกลับมาทำงานได้ดังเดิม ท่านจะหาช่างซ่อมได้จากที่ไหนหรือท่านจะหาข้อมูลได้จากที่ใดว่าจะทำอะไรต่อไป

ผู้ขายส่วนใหญ่จะแจกจ่ายโปรแกรมอุดช่องโหว่ที่ใช้แก้ไข **ข้อผิดพลาด** (bugs) ในผลิตภัณฑ์ของตน ซึ่งโดยทั่วไปแล้วโปรแกรมเหล่านี้จะสามารถแก้ไขข้อผิดพลาดได้อย่างเรียบร้อย แต่ในบางกรณีโปรแกรมอุดช่องโหว่จะแก้ปัญหาหนึ่งแต่เป็นต้นเหตุของอีกปัญหาหนึ่ง ยกตัวอย่างในชีวิตประจำวันเช่น เมื่อท่านให้ช่างมาซ่อมเครื่องใช้ที่บ้านแต่ขณะซ่อมช่างทำให้พื้นบ้านเป็นรอย สำหรับเครื่องคอมพิวเตอร์แล้วเราจะต้องลงโปรแกรมอุดช่องโหว่ไปเรื่อยๆจนกว่าจะแก้ปัญหาได้ทั้งหมด

โดยทั่วไปแล้วผู้ขายจะให้ท่านดาวน์โหลดโปรแกรมอุดช่องโหว่ได้ฟรีจากเว็บของผู้ขาย ดังนั้นเมื่อท่านซื้อโปรแกรมใดๆท่านควรจะตรวจสอบว่าผู้ขายมีโปรแกรมอุดช่องโหว่ให้หรือไม่และท่านจะนำโปรแกรมมาติดตั้งบนเครื่องของท่านได้อย่างไร นอกจากนั้นท่านควรตรวจสอบอีกด้วยว่าผู้ขายมีบริการตอบปัญหาหากท่านมีคำถามเกี่ยวกับผลิตภัณฑ์หรือไม่ ซึ่งในการนี้สำหรับผู้ขายบางรายท่านจะต้องซื้อบริการหลังการขายเป็นการเพิ่มเติม

ในกรณีที่ท่านซื้อสินค้าทั่วไป หากตัวสินค้ามีปัญหาด้านความปลอดภัย ทางบริษัทผู้ขายอาจเรียกสินค้าคืนเพื่อแก้ไขปัญหาหรือแลกเปลี่ยนสินค้าตัวใหม่ให้ ซึ่งบริษัทผู้ขายจะติดต่อกับท่านได้จากการที่ท่านกรอกข้อมูลในแบบฟอร์มที่มากับสินค้าแล้วส่งกลับไปยังผู้ขาย (คือการลงทะเบียนสินค้าที่ท่านซื้อ)

ผู้ขายซอฟท์แวร์ก็มีบริการคล้ายกันนี้ ท่านอาจได้รับข่าวเกี่ยวกับโปรแกรมอุดช่องโหว่ที่ออกใหม่ผ่านทางการสมัครเป็นสมาชิกข่าวทางอีเมล์ของผู้ขาย ซึ่งจะทำให้ท่านได้รับทราบถึงปัญหาของ

ซอฟท์แวร์ของท่านก่อนที่ท่านจะประสบกับปัญหาด้วยตัวเองและก่อนที่ผู้บุกรุกจะทราบและฉวยโอกาสเจาะช่องโหว่ที่เกิดขึ้น ท่านควรศึกษาเว็บของผู้ขายเพื่อหาวิธีรับทราบถึงโปรแกรมอุดช่องโหว่ล่าสุดที่ผู้ขายแจกจ่าย

ผู้ขายบางรายมีบริการที่ดีกว่าส่งข่าวทางอีเมล์กล่าวคือในตัวโปรแกรมที่ท่านซื้อจะมีโปรแกรมอีกโปรแกรมติดมาด้วยที่จะทำหน้าที่ติดต่อกับเว็บของผู้ขายและสามารถดาวน์โหลดโปรแกรมอุดช่องโหว่มาติดตั้งที่เครื่องของท่านโดยอัตโนมัติ ทั้งนี้ท่านสามารถตั้งค่าโปรแกรมนี้ไม่ให้ติดตั้งโปรแกรมอุดช่องโหว่โดยอัตโนมัติก็ได้โดยอาจจะให้โปรแกรมแจ้งข่าวให้ท่านทราบเท่านั้นและหากท่านต้องการที่จะติดตั้งโปรแกรมอุดช่องโหว่ด้วยตนเองก็จะสามารถกระทำได้

จะเห็นได้ว่ากระบวนการติดตั้งโปรแกรมอุดช่องโหว่นั้นง่ายขึ้นมากแต่ก็มิได้หมายความว่าจะปราศจากข้อผิดพลาด ในบางครั้งหลังจากที่เราติดตั้งโปรแกรมอุดช่องโหว่จะทำให้เกิดปัญหาอื่นขึ้นในเครื่องคอมพิวเตอร์ ดังนั้นท่านควรจะหาข้อมูลของโปรแกรมอุดช่องโหว่ที่ติดตั้งในเครื่องคอมพิวเตอร์ของท่านให้มากที่สุดเพื่อที่จะรับทราบว่าโปรแกรมนี้มีหน้าที่อะไรบ้างและปัญหาที่อาจจะเกิดจากโปรแกรมนี้มีอะไรบ้าง

การหาข้อมูลของโปรแกรมอุดช่องโหว่นั้นอาจกระทำไม่ได้ง่ายเสมอไป เนื่องจากโดยทั่วไปแล้วผู้ขายจะไม่บอกข้อมูลทั้งหมดของโปรแกรมอุดช่องโหว่ต่างๆเพราะผู้ขายเองก็ไม่สามารถทดสอบโปรแกรมอุดช่องโหว่ทั้งหมดเพื่อหาปัญหาที่อาจเกิดขึ้นได้ (โปรแกรมอุดช่องโหว่มีอยู่มากมาย) ซึ่งผู้ขายเองก็ต้องอาศัยลูกค้าของตนที่จะรายงานปัญหาต่างๆให้ผู้ขายทราบด้วย ดังนั้นหากท่านพบปัญหาจากโปรแกรมอุดช่องโหว่ที่ติดตั้งในเครื่องของท่านท่านควรรายงานให้ผู้ขายทราบด้วย

สมมุติว่าท่านทราบว่ามีโปรแกรมอุดช่องโหว่ออกใหม่ ท่านควรใช้หัวข้อพิจารณาต่อไปนี้ก่อนที่จะติดตั้งโปรแกรมอุดช่องโหว่นั้น

1. ผลกระทบ – โปรแกรมอุดช่องโหว่นั้นจะมีผลกระทบต่อโปรแกรมอื่นๆบนเครื่องคอมพิวเตอร์ของท่านหรือไม่
2. ผลเสียหาย – โปรแกรมอุดช่องโหว่นั้นก่อให้เกิดผลเสียหายใดๆหรือไม่ โดยท่านอาจทราบได้โดยศึกษาข้อมูลบนเว็บของผู้ขายเกี่ยวกับตัวโปรแกรมนี้ให้ได้มากที่สุดหรือใช้การค้นหาในเว็บต่างๆว่าผู้ใช้คนอื่นประสบปัญหากับโปรแกรมนี้หรือไม่
3. การยกเลิก – หลังจากที่ท่านติดตั้งโปรแกรมอุดช่องโหว่นั้นแล้วท่านสามารถยกเลิกหรือลบโปรแกรมนั้นออกภายหลังได้หรือไม่ กล่าวคือท่านสามารถทำให้เครื่องคอมพิวเตอร์ของท่านคืนสู่สภาพก่อนที่ท่านจะติดตั้งโปรแกรมนั้นได้หรือไม่ ซึ่งในปัจจุบันโปรแกรมอุดช่องโหว่ส่วนใหญ่จะมีคุณลักษณะในส่วนนี้ เพื่อให้ท่านสามารถ

ลบโปรแกรมออกได้หากโปรแกรมนั้นทำให้เกิดผลเสียหาย นอกจากนี้เครื่องคอมพิวเตอร์บางเครื่องมีขีดความสามารถที่จะคืนสภาพตัวเองสู่สถานะเดิมที่ตั้งไว้ได้ ทั้งนี้ท่านควรจะได้ทราบว่าเครื่องของท่านมีความสามารถนี้หรือไม่เพื่อที่ท่านจะสามารถปฏิบัติได้อย่างถูกต้อง

ในตอนกล่าวนำ เราได้กล่าวถึงว่าผู้บุกรุกจะสามารถโจมตีเครื่องคอมพิวเตอร์ของท่านโดยเจาะช่องโหว่ในโปรแกรมบนเครื่อง จึงมีคำถามอยู่ว่า แล้วผู้บุกรุกจะทราบได้อย่างไรว่าโปรแกรมใดมีช่องโหว่อยู่ที่ไหน? ซึ่งที่จริงแล้วผู้บุกรุกทราบถึงช่องโหว่ของโปรแกรมจากทางเว็บหรือการประกาศของผู้ขายนั่นเอง เพราะฉะนั้นเราอาจกล่าวได้ว่าผู้บุกรุกทราบถึงช่องโหว่ในเวลาไล่เลี่ยกับเรา ดังนั้นเมื่อท่านทราบถึงช่องโหว่ท่านควรจะปฏิบัติตามข้อพิจารณาด้านบนแล้วลงโปรแกรมอุดช่องโหว่ให้เร็วที่สุดเท่าที่จะทำได้ เนื่องจากยิ่งปล่อยช่องโหว่ไว้นานโอกาสที่ผู้บุกรุกจะเจาะเข้ามายังเครื่องคอมพิวเตอร์ของท่านโดยอาศัยช่องโหว่นั้นจะยิ่งมีมาก

ข้อควรระวังอีกข้อหนึ่งคือโปรแกรมอุดช่องโหว่นั้นก็ถือว่าเป็นโปรแกรมประเภทหนึ่งด้วย ดังนั้นในการที่ท่านจะดาวน์โหลดหรือติดตั้งโปรแกรมอุดช่องโหว่นั้นท่านควรใช้ข้อพิจารณาใน ข้อปฏิบัติที่ 7 – ใช้ความระมัดระวังในการดาวน์โหลดและติดตั้งโปรแกรม

ช่องโหว่ที่ผู้บุกรุกสามารถใช้เจาะเข้าในเครื่องคอมพิวเตอร์นั้นโดยมากแล้วจะเป็นช่องโหว่ที่มีโปรแกรมอุดช่องโหว่แจกจ่ายออกมาแล้วแต่ผู้ใช้เครื่องไม่ใส่ใจที่จะติดตั้งโปรแกรมอุดช่องโหว่นั้น ดังนั้นท่านควรติดตั้งโปรแกรมอุดช่องโหว่ทั้งหมดที่มีโดยเร็วที่สุดเท่าที่จะทำได้ หากโปรแกรมใดมีช่องโหว่แต่ไม่มีโปรแกรมอุดช่องโหว่แจกจ่ายออกมา ท่านควรหยุดใช้โปรแกรมนั้นไประยะหนึ่งจนกว่าจะมีโปรแกรมอุดช่องโหว่ออกมา หรือเปลี่ยนไปใช้โปรแกรมคล้ายๆ กันที่ผลิตโดยผู้ขายรายอื่นที่ไม่มีช่องโหว่นั้นอยู่

โดยปกติแล้วท่านจะไม่ต้องเสียค่าใช้จ่ายใดๆในการติดตั้งโปรแกรมอุดช่องโหว่ เพียงแต่ท่านต้องเสียเวลาไปบ้างเท่านั้น

ข้อปฏิบัติที่ 3 – ใช้ความระมัดระวังในการอ่านอีเมล์ที่มีสิ่งอื่นแนบมาด้วย (Attachments)

มีข่าวอยู่เสมอเกี่ยวกับผู้ที่ได้รับพัสดุหรือจดหมายทางไปรษณีย์แล้วได้รับอันตรายเนื่องจากพัสดุหรือจดหมายนั้นมีระเบิดหรือเชื้อโรคร้ายแรงอยู่ ถึงแม้ว่าเหตุการณ์ดังกล่าวจะไม่เกิดขึ้นบ่อยนักแต่เมื่อเกิดขึ้นแล้วก่อให้เกิดผลเสียหายแก่ผู้เสียหายอย่างมากและเป็นข่าวใหญ่ทุกครั้ง

พัสดุหรือจดหมายเหล่านี้ถูกส่งให้แก่ผู้เสียหายโดยที่ผู้เสียหายไม่ทราบล่วงหน้าก่อน (ไม่ได้ร้องขอ) ดังนั้นพัสดุหรือจดหมายเหล่านี้จะต้องมีอะไรบางอย่างที่ชักชวนผู้รับให้เปิดพัสดุหรือจดหมายนั้น เช่นมีที่อยู่ผู้ส่งที่ผู้รับอาจสนใจ มีข้อความบนซองจดหมายที่เชื้อเชิญให้เปิด มีการบรรจุหีบห่อที่สวยงามหรือแปลกประหลาด เป็นต้น วิธีการเหล่านี้จัดได้ว่าเป็นการทำ **“วิศวกรรมทางสังคม”** (social engineering) ซึ่งโดยทั่วไปแล้วจะประสบผลสำเร็จเนื่องจากโดยธรรมชาติแล้วคนเราจะเชื่อในสิ่งที่ได้พบเห็นและมีความอยากรู้อยากเห็น

ยกตัวอย่างเหตุการณ์จดหมายแพร่เชื้อแอนแทรกซ์ที่ผู้ก่อการร้ายส่งให้สมาชิกวุฒิสภาสหรัฐอเมริกานั้น ผู้ส่งปลอมที่อยู่ผู้ส่งเป็นที่อยู่ของโรงเรียนประถมแห่งหนึ่ง ซึ่งในสหรัฐอเมริกานั้นเป็นเรื่องปกติที่นักเรียนจะส่งจดหมายให้สมาชิกวุฒิสภา ดังนั้นเมื่อมีการเปิดซองจดหมายนี้จะทำให้เชื้อโรคแพร่กระจายออกมาเป็นไปตามวัตถุประสงค์ของผู้ส่ง เหตุการณ์ที่เกิดนี้ทำให้ในปัจจุบันมีความระมัดระวังในเรื่องสิ่งที่อยู่ในพัสดุหรือจดหมายและความน่าเชื่อถือของที่อยู่ผู้ส่งมากขึ้น โดยที่ก่อนหน้านี้แทบไม่มีความระมัดระวังหรือความสงสัยในเรื่องนี้เลย

ตัวท่านเองก็อาจจะได้รับจดหมายจำนวนหนึ่งในแต่ละวัน จดหมายบางฉบับถูกส่งมาโดยที่ท่านไม่ทราบล่วงหน้าก่อน (ท่านไม่ได้ร้องขอหรือส่งจดหมายไปก่อน) โดยอาจมีที่อยู่ผู้ส่งที่ท่านอาจจะไม่รู้จักแต่ดูน่าเชื่อถือ จดหมายเหล่านี้บางฉบับจะใช้วิศวกรรมทางสังคมชักชวนให้ท่านเข้าร่วมการแข่งขันหรือการเสี่ยงโชคบางอย่าง โดยจะชักจูงให้ท่านเปิดซอง อ่านจดหมาย และติดต่อกลับไป ซึ่งโดยมากจะทำให้เกิดผลประโยชน์ทางการค้า (ของผู้ส่ง) จดหมายในลักษณะนี้ใช้รางวัลล่อใจให้เราเปิดอ่านซึ่งโดยทั่วไปแล้วการเปิดอ่านจะไม่ก่อให้เกิดผลเสียมากมายนัก นอกจากการเสียเวลา

ไวรัสและหนอนที่มากับอีเมล์นั้นใช้หลักการคล้ายกับที่กล่าวมาข้างต้น เว้นแต่ว่าผลเสียหายที่เกิดอาจจะร้ายแรง อีเมล์เหล่านี้มักจะใช้ที่อยู่ผู้ส่งโดยเป็นคนที่ท่านรู้จักและมีชื่อเรื่อง (Subject) ที่น่าสนใจหรือแปลกใจ ซึ่งถือได้ว่าเป็นการทำวิศวกรรมทางสังคมที่แนบเนียนมากโดยหลอกลวงให้ท่านอ่านอีเมล์ที่ท่านคิดว่ามาจากคนที่ท่านรู้จักที่มีเรื่องที่น่าสนใจหรือแปลกใจ

การได้รับอีเมล์ที่มีไวรัสและหนอนนั้นเป็นเรื่องค่อนข้างปกติของผู้ที่ใช้อินเทอร์เน็ตซึ่งหากท่านยังไม่เคยได้รับอีเมล์ประเภทนี้ก็มีโอกาสสูงที่ท่านจะได้รับในเวลาอันใกล้นี้ ดังนั้นท่านควรใช้ความระมัดระวังในการเปิดและอ่านอีเมล์ที่มีสิ่งอื่นแนบมาด้วยโดยใช้ข้อพิจารณาต่อไปนี้

1. รู้จัก – อีเมล์นี้มาจากคนที่ท่านรู้จักหรือไม่
2. เคยได้รับ – ท่านเคยได้รับอีเมล์จากผู้ส่งคนนี้หรือไม่
3. คาดหวัง – ท่านคาดหวังหรือทราบมาก่อนว่าจะได้รับอีเมล์ (ที่มีสิ่งอื่นแนบมาด้วย)จากผู้ส่งคนนี้หรือไม่

4. สามัญสำนึก – ให้ท่านใช้สามัญสำนึกในการพิจารณาอีเมล์ที่ได้รับว่าผู้ส่ง ชื่อเรื่อง และสิ่งที่แนบมา มีความเกี่ยวเนื่องกันหรือไม่ เช่น หากชื่อผู้ส่งเป็นญาติผู้ใหญ่หรือเจ้านายของท่าน แต่ชื่อเรื่องเป็น “Here you have, ;o)” และสิ่งที่แนบมาเป็นไฟล์ AnnaKournikova.jpg.vbs เมื่อเราใช้สามัญสำนึกพิจารณาดูแล้วอีเมล์นี้ไม่น่าจะเป็นอีเมล์จริง แต่น่าจะเป็นอีเมล์ที่มีหนอนที่ชื่อ Anna Kournikova ซึ่งหากท่านเปิดอ่านจะสามารถทำอันตรายต่อเครื่องของท่านได้
5. ไวรัส – อีเมล์นี้มีไวรัสหรือไม่ ซึ่งการพิจารณาว่าอีเมล์นี้มีไวรัสหรือไม่นั้นท่านจะต้องติดตั้งและใช้โปรแกรมป้องกันไวรัสดังที่ได้อธิบายไว้ใน ข้อปฏิบัติที่ 1 – ติดตั้งและใช้โปรแกรมป้องกันไวรัส

หากอีเมล์ที่รับมาไม่ผ่านข้อพิจารณาข้อใดข้อหนึ่งด้านบน ท่านควรลบอีเมล์นั้นทิ้งไป และหากอีเมล์นั้นผ่านข้อพิจารณาทั้งหมดท่านก็ยังควรใช้ความระมัดระวังในการเปิดและอ่านและคอยเฝ้าดูสิ่งบอกเหตุหรือสิ่งผิดปกติที่เกิดขึ้นในขณะเปิดอ่าน

จากข้อพิจารณา 5 ข้อด้านบน จะเห็นได้ว่าผู้ที่ใช้ข้อพิจารณาเหล่านี้จะไม่เปิดอีเมล์ที่มีสิ่งแนบ ที่มาจากคนที่ไม่รู้จัก ดังนั้นถ้าท่านต้องการส่งอีเมล์ที่มีสิ่งแนบถึงผู้ที่ท่านไม่เคยติดต่อมาก่อน ท่านควรจะใช้ขั้นตอนด้านล่างนี้ในการติดต่อกับผู้นั้น

1. เนื่องจากผู้รับยังไม่รู้จักท่าน ดังนั้นท่านควรส่งอีเมล์แนะนำตัวเองก่อนโดยที่จะต้องไม่มีสิ่งใดๆแนบไปด้วย ซึ่งข้อความในอีเมล์นี้ควรจะประกอบด้วยการแนะนำตัวเองของท่าน วัตถุประสงค์ของการติดต่อ และการขออนุญาตส่งสิ่งแนบที่ท่านต้องการส่ง
2. การส่งอีเมล์แนะนำนี้ถือได้ว่าผู้รับเคยได้รับอีเมล์จากท่านแล้ว
3. หากผู้รับตอบกลับมา ท่านควรจะปฏิบัติตามความประสงค์ของผู้รับ โดยหากผู้รับไม่อนุญาตให้ท่านส่งสิ่งแนบนั้น ท่านก็ไม่ควรส่ง แต่ถ้าผู้รับไม่ได้ตอบกลับ ท่านอาจจะลองส่งอีเมล์แนะนำตัวเองอีกครั้ง
4. ถ้าผู้รับตอบกลับและอนุญาตให้ท่านส่งอีเมล์พร้อมสิ่งแนบ ก็จะถือว่าผู้รับรู้จักท่าน เคยได้รับอีเมล์จากท่าน และคาดหวังอีเมล์ที่มีสิ่งแนบจากท่าน ก็จะถือว่า
อีเมล์ จากท่านผ่านข้อพิจารณา 3 ข้อแรกในข้อพิจารณา 5 ข้อด้านบน
5. สิ่งที่ท่านส่งควรจะมีความเกี่ยวเนื่องกันในตัวเอง เพื่อให้ผ่านข้อพิจารณาเรื่องสามัญสำนึกด้านบน อย่าใช้ชื่อเรื่องที่เป็นเชิงโฆษณาชักชวน หรือที่คล้ายกับการทำวิศวกรรมสังคม
6. ตรวจสอบสิ่งที่ท่านแนบไปกับอีเมล์ว่ามีไวรัสหรือไม่ โดยใช้โปรแกรมป้องกันไวรัส

ข้อพิจารณาทั้ง 5 ข้อด้านบนช่วยให้ท่านพิจารณาเรื่องหลักๆ เกี่ยวกับไวรัสและหนอนที่มากับอีเมล์ ดังนั้นท่านควรใช้ข้อพิจารณาเหล่านี้ประกอบทุกครั้งที่มีการส่งและรับอีเมล์ที่มีสิ่งแนบ อย่างไรก็ตามท่านควรตระหนักว่าไม่มีข้อพิจารณาหรือสิ่งใดๆ ที่ช่วยให้มีความปลอดภัยอย่างเบ็ดเสร็จหรือเต็มที่ ถึงแม้จะใช้ข้อพิจารณาเหล่านี้แล้วท่านก็ควรจะใช้ความระมัดระวังด้วย โดยแม้โปรแกรมป้องกันไวรัสจะสามารถตรวจจับและทำลายไวรัสที่จะเข้าสู่เครื่องคอมพิวเตอร์ของท่านได้ แต่มักจะมีช่วงเวลาระหว่างการค้นพบไวรัสและการออกรายชื่อลายมือไวรัสใหม่จากผู้ผลิตโปรแกรมที่ไวรัสจะสามารถเข้ามาทำอันตรายต่อเครื่องของท่านได้ จะเห็นได้ว่าท่านไม่สามารถเชื่อถือโปรแกรมป้องกันไวรัสได้อย่างเบ็ดเสร็จหรือสมบูรณ์และท่านจะต้องใช้ความระมัดระวังทุกครั้งที่เปิดและอ่านอีเมล์ใดๆ

ข้อปฏิบัติที่ 4 – ติดตั้งและใช้โปรแกรมไฟร์วอล (Firewall)

ในหัวข้อนี้ท่านจะได้ทราบถึงสิ่งที่เรียกกันว่าไฟร์วอล ความสำคัญของไฟร์วอลต่อความปลอดภัยของเครื่องคอมพิวเตอร์ของท่านและสิ่งที่ต้องปฏิบัติในการใช้ไฟร์วอล ในการอธิบายสิ่งเหล่านี้เราจะไม่ใช้การเปรียบเทียบที่ว่า “เครื่องคอมพิวเตอร์เปรียบเสมือนบ้าน” เหมือนดังที่ผ่านมา แต่เราจะใช้การเปรียบเทียบอีกอย่างที่ท่านก็น่าจะมีความคุ้นเคยเช่นกันคือ “คอมพิวเตอร์เปรียบเสมือนอาคารสำนักงาน”

ท่านอาจจะเคยไปติดต่องานที่อาคารสำนักงานที่มีโต๊ะด้านหน้าที่มีเจ้าหน้าที่รักษาความปลอดภัยประจำอยู่ หน้าที่ของเจ้าหน้าที่รักษาความปลอดภัยนั้นคือตรวจสอบและประเมินผู้ที่จะเข้าและออกจากอาคารและตัดสินใจว่าควรอนุญาตผู้นั้นให้เข้าออกได้ตามประสงค์หรือไม่ เจ้าหน้าที่จะป้องกันไม่ให้บุคคลหรือสิ่งไม่พึงประสงค์เข้าในอาคารนั้น และจะอนุญาตเฉพาะบุคคลหรือสิ่งที่เหมาะสมเข้าและออกจากอาคารนั้นได้

ต่อไปลองพิจารณาในรายละเอียดของการเปรียบเทียบนี้ กล่าวคือ เมื่อใดที่มีผู้เข้าสู่ตัวอาคาร เจ้าหน้าที่รักษาความปลอดภัยจะมองเห็นผู้นั้น ซึ่งหากผู้นั้นมีบัตรประจำตัวที่แสดงต่อเจ้าหน้าที่หรือเป็นบัตรแม่เหล็กที่ใช้รูดกับเครื่องอ่าน ซึ่งหากผ่าน ผู้นั้นก็จะผ่านการตรวจสอบของเจ้าหน้าที่และผ่านเข้าไปในสำนักงานได้ แต่หากไม่ผ่านหรือผู้นั้นเป็นบุคคลภายนอกที่มาติดต่อ ผู้นั้นก็จะต้องหยุดติดต่อที่โต๊ะเจ้าหน้าที่รักษาความปลอดภัยก่อน

เจ้าหน้าที่ก็จะถามผู้นั้นว่าต้องการจะมาพบใคร และอาจจะขอดูบัตรประจำตัวของผู้นั้น โดยเจ้าหน้าที่อาจจะตรวจสอบกับรายชื่อของผู้ที่จะมาเยือนในวันนั้น (ที่ออกไว้ล่วงหน้า) และถ้าเจ้าหน้าที่เห็น

ว่าทุกอย่างถูกต้องเรียบร้อยก็จะอนุญาตให้ผู้นั้นผ่านเข้าไปได้ ซึ่งโดยปกติผู้นั้นจะต้องลงนามในสมุดเยี่ยมเพื่อระบุรายละเอียดต่างๆของตน เช่น ชื่อ หน่วยงาน ผู้ที่ตนติดต่อ และวันเวลาเข้าออก

ไฟร์วอลในเครื่องคอมพิวเตอร์นั้นทำหน้าที่คล้ายกับเจ้าหน้าที่รักษาความปลอดภัยดังที่กล่าวมา โดยไฟร์วอลจะตรวจสอบข้อมูลในเครือข่ายที่วิ่งออกไปยังและที่วิ่งเข้ามาจากเครื่องคอมพิวเตอร์อื่น ไฟร์วอลจะตัดสินใจว่าจะอนุญาตให้ข้อมูลนั้นดำเนินต่อไปถึงจุดหมายหรือไม่ ไฟร์วอลมีความสำคัญต่อความปลอดภัยของเครื่องของท่านเนื่องจากไฟร์วอลจะทำหน้าที่ป้องกันไม่ให้ข้อมูลที่ไม่ต้องการเข้ามาและอนุญาตเฉพาะข้อมูลที่เหมาะสมให้เข้าและออกจากเครื่องได้

ในการทำงานของไฟร์วอลนั้น ไฟร์วอลจะตรวจสอบข้อมูลทุกชิ้นที่วิ่งในเครือข่าย (แต่ละชิ้นเรียกว่าแพ็คเก็ต) ที่จะเข้ามาและออกจากเครื่องคอมพิวเตอร์ แต่ละแพ็คเก็ตจะมีข้อมูลกำกับว่ามาจากที่ใดและจะไปยังที่ใด แพ็คเก็ตบางตัวจะได้รับอนุญาตให้ไปที่ใดก็ได้ (เปรียบเสมือนพนักงานที่มีบัตรผ่าน) ส่วนแพ็คเก็ตบางตัวจะได้รับอนุญาตให้ไปเฉพาะบางที่เท่านั้น (เปรียบเสมือนผู้มาเยือน) ซึ่งหากไฟร์วอลอนุญาตให้แพ็คเก็ตดำเนินต่อไปได้ (ข้อมูลของแพ็คเก็ตเป็นไปตามกฎที่ตั้งไว้) ไฟร์วอลก็จะส่งแพ็คเก็ตให้เดินทางต่อไปยังที่หมาย พร้อมกันนั้นในกรณีส่วนใหญ่แล้วไฟร์วอลจะบันทึกข้อมูลของแพ็คเก็ตนั้นไว้ด้วยว่า มาจากที่ใด กำลังจะไปที่ใด และตรวจพบในเวลาใด ซึ่งก็เปรียบเสมือนกับการบันทึกข้อมูลของผู้เข้าออกตัวอาคารสำนักงานนั่นเอง

ในบางกรณี เจ้าหน้าที่รักษาความปลอดภัยของอาคารอาจต้องมีการปฏิบัติเพิ่มเติมในการที่จะตัดสินใจว่าควรอนุญาตให้ผู้มาติดต่อเข้าไปในสำนักงานหรือไม่ เช่นหากผู้ที่มาติดต่อนั้นไม่มีชื่ออยู่ในรายชื่อของผู้ของผู้ที่จะมาเยือนในวันนั้น เจ้าหน้าที่ก็อาจจะโทรศัพท์ติดต่อผู้ที่ผู้มาติดต่อต้องการพบเพื่อแจ้งว่ามีผู้ต้องการติดต่อและถามว่าจะอนุญาตให้ผู้นั้นเข้าพบหรือไม่ โดยหากได้รับอนุญาต ผู้ติดต่อก็สามารถเข้าไปยังสำนักงานได้ และเจ้าหน้าที่รักษาความปลอดภัยอาจมอบบัตรชั่วคราวให้ผู้ติดต่อติดไว้เพื่อแสดงว่าเป็นบุคคลภายนอกที่มาเยือน โดยที่อาจมีการจำกัดสิทธิของบัตรนั้นว่าให้เข้าได้เฉพาะบางส่วนของสำนักงาน หรือจะต้องมีผู้นำเยี่ยมชมสำนักงานเท่านั้น นอกจากนี้ ไม่ว่าผู้ที่จะเข้าสู่ตัวอาคารจะเป็นบุคคลภายในหรือภายนอก เจ้าหน้าที่รักษาความปลอดภัยยังอาจมีสิทธิที่จะตรวจสอบกระเป๋าเอกสารหรือคอมพิวเตอร์โน้ตบุ๊คของผู้นั้นได้

ในทำนองเดียวกันนี้ หากไฟร์วอลพบข้อมูลที่ไม่ได้คาดไว้ล่วงหน้า ไฟร์วอลสามารถถามผู้ใช้เครื่องคอมพิวเตอร์ได้ว่าจะอนุญาตให้ข้อมูลนี้เข้ามาในเครื่องหรือไม่ โดยอาจให้ผ่านเฉพาะแพ็คเก็ตที่กำลังพิจารณาอยู่เท่านั้นหรืออาจมีการตั้งค่าให้ผ่านแพ็คเก็ตประเภทเดียวกันนี้ตลอดไปในอนาคตก็ได้ ไฟร์วอลบางตัวสามารถส่งแพ็คเก็ตต่างกันไปยังที่หมายต่างกันได้หรือแม้แต่ซ่อนแพ็คเก็ตหนึ่งไว้ในอีกแพ็คเก็ตหนึ่ง (เปรียบเสมือนมีผู้นำเยี่ยมชมสำนักงาน) นอกจากนี้ไฟร์วอลบางตัวไม่ได้ตัด

สินใจโดยเพียงแค่ตรวจสอบที่หมายและแหล่งที่มาของแพ็คเก็ตเท่านั้น แต่ยังสามารถตรวจสอบข้อความภายในแพ็คเก็ตได้ด้วย (เปรียบเสมือนการตรวจสอบกระเป๋าเอกสารหรือคอมพิวเตอร์โน้ตบุ๊ค)

สำหรับอาคารสำนักงาน พนักงานอาจต้องรูดบัตรหรือลงบันทึกเมื่อออกจากอาคารเพื่อบันทึกเวลาออก บุคคลภายนอกผู้มาเยือนต้องลงบันทึกและคืนบัตรชั่วคราว และอาจจะมีการตรวจสิ่งของของทั้งพนักงานและบุคคลภายนอกก่อนที่จะได้รับอนุญาตให้ออกจากอาคาร

ในทำนองเดียวกัน ไฟร์วอลสามารถทราบได้เมื่อการเชื่อมต่อทางเครือข่าย (การแลกเปลี่ยนข้อมูล) สิ้นสุดลงและสามารถบันทึกข้อมูลการเชื่อมต่อไว้ได้ ซึ่งหากการเชื่อมต่อเป็นการเชื่อมต่อแบบชั่วคราว (เปรียบเสมือนบุคคลภายนอกที่มาเยือน) ไฟร์วอลจะไม่อนุญาตให้มีการเชื่อมต่อคล้ายกันนี้ในอนาคตอีก โดยจะถามผู้ใช้คอมพิวเตอร์เพื่อให้พิจารณาอนุญาตใหม่เป็นครั้งๆ ไป (เปรียบเสมือนการที่เจ้าหน้าที่รักษาความปลอดภัยโทรศัพท์ติดต่อผู้ที่มาเยือนต้องการพบทุกครั้ง) นอกจากนี้ไฟร์วอลยังสามารถตรวจสอบข้อความของแพ็คเก็ตใดๆ ที่เป็นส่งออกไปภายนอกได้ด้วย (เปรียบเสมือนการตรวจสิ่งของของผู้ที่จะออกจากอาคาร)

ที่กล่าวมาทั้งหมดข้างต้นนี้หมายความอย่างง่ายๆ ว่า ท่านสามารถควบคุมแพ็คเก็ตต่างๆ ที่จะเข้าสู่และออกจากเครื่องคอมพิวเตอร์ของท่านได้โดยใช้ไฟร์วอล

แต่สิ่งที่ค่อนข้างซับซ้อนที่ต้องพิจารณาก็คือ การกำหนดรายละเอียดว่าแพ็กเก็ตประเภทใดบ้างที่ควรได้รับอนุญาตให้เข้าสู่และออกจากเครื่องคอมพิวเตอร์ของท่าน และหากไฟร์วอลของท่านสามารถตรวจสอบข้อความที่อยู่ในแพ็คเก็ตได้ท่านก็ควรจะทราบด้วยว่าข้อความประเภทใดที่ควรอนุญาตและประเภทใดที่ไม่ควรอนุญาต เพื่อที่จะทำให้การปฏิบัติในส่วนนี้ง่ายขึ้น เราจะกลับไปพิจารณาเชิงเปรียบเทียบในเรื่องอาคารสำนักงานอีกครั้งหนึ่ง

ขอให้ท่านนึกภาพว่าท่านเป็นเจ้าหน้าที่รักษาความปลอดภัยที่มาปฏิบัติงานเป็นวันแรก และท่านมีหน้าที่ตัดสินใจว่าจะอนุญาตให้ใครเข้าออกอาคารได้บ้าง และจะอนุญาตให้มีการนำสิ่งของใดเข้าออกอาคารได้บ้าง ท่านจะมีข้อพิจารณาในการตัดสินใจอย่างไร?

วิธีตัดสินใจหนึ่งที่เป็นไปได้คือใช้หลักการปลอดภัยไว้ก่อน กล่าวคือ ไม่ยอมให้ผู้ใดหรือสิ่งใดเลยเข้าสู่หรือออกจากอาคารนั้น วิธีนี้เป็นวิธีที่ปฏิบัติได้ง่ายมากแต่เป็นที่แน่นอนว่าจะไม่เกิดผลดีต่อองค์กรนั้น เนื่องจากงานตามภารกิจขององค์กรย่อมจะไม่สามารถดำเนินไปได้ตามปกติ และท่านคงเป็นเจ้าหน้าที่รักษาความปลอดภัยขององค์กรนี้ได้อีกไม่นานนัก

ดังนั้นหลังจากใช้วิธีนี้ได้ไม่นานท่านก็คงต้องเปลี่ยนวิธีตัดสินใจใหม่ โดยอาจอนุญาตให้บุคคลและสิ่งของที่มีคุณสมบัติตามที่กำหนดไว้สามารถเข้าสู่และออกจากอาคารสำนักงานได้ และหากบุคคลหรือสิ่งของใดที่ไม่มีคุณสมบัติตามที่กำหนดจะไม่ได้รับอนุญาต

ท่านสามารถกำหนดวิธีตัดสินใจคล้ายกันนี้ให้กับไฟร์วอลบนเครื่องของท่านได้ โดยท่านสามารถกำหนดให้ไฟร์วอลไม่อนุญาตให้ข้อมูลใดๆ เข้าสู่หรือออกจากเครื่องคอมพิวเตอร์ของท่านเลยได้ เราเรียกกฎนี้ว่าการ “ปฏิเสธทั้งหมด” (deny all) ซึ่งเป็นการรักษาความปลอดภัยที่ได้ผลแต่กฎนี้จะทำให้ท่านไม่สามารถเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตได้ ซึ่งอาจไม่เป็นที่พึงประสงค์สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลทั่วไป

ท่านอาจจะใช้กฎคล้ายกับวิธีการตัดสินใจของเจ้าหน้าที่รักษาความปลอดภัยในอาคารสำนักงาน โดยตรวจสอบแพ็คเก็ตแต่ละแพ็คเก็ต (เปรียบเสมือนการตรวจสอบพนักงานหรือผู้มาเยือน) เพื่อดูแหล่งที่มาและที่หมายของแพ็คเก็ตนั้น ผลิตภัณฑ์ไฟร์วอลบางตัวสามารถให้ท่านตรวจสอบข้อมูลเหล่านี้ในแพ็คเก็ตได้โดยง่ายและจะทำให้การตัดสินใจในการอนุญาตแพ็คเก็ตนั้นง่ายขึ้น ดังนั้นหากท่านจะพิจารณาหาซื้อไฟร์วอลท่านควรเลือกไฟร์วอลที่มีคุณลักษณะนี้อยู่เพื่อให้งานการรักษาความปลอดภัยเครื่องคอมพิวเตอร์ของท่านง่ายขึ้น

ในขณะที่เจ้าหน้าที่รักษาความปลอดภัยจะยอมให้ผู้ใดที่ตามที่มีบัตรประจำตัวขององค์กรเข้าออกอาคารสำนังานขององค์กรนั้น ท่านก็สามารถสร้างกฎสำหรับไฟร์วอลให้อนุญาตแพ็คเก็ตบางประเภทผ่านเข้าออกได้โดยไม่ต้องตรวจสอบแพ็คเก็ตเหล่านั้นทุกครั้ง เช่น ท่านอาจจะสร้างกฎให้โปรแกรมท่องเว็บของท่านสามารถออกไปดูเว็บใดก็ได้ ดังนั้นกฎนี้จะยอมให้แพ็คเก็ตใดๆ ก็ตามที่มีที่มาจากโปรแกรมท่องเว็บของท่านและมีที่หมายเป็นเครื่องคอมพิวเตอร์ที่ให้บริการดูเว็บ (web server) และแพ็คเก็ตที่ตอบกลับมาจากเครื่องเหล่านั้นสามารถผ่านไปได้ ซึ่งจะทำให้ท่านสามารถใช้เครื่องคอมพิวเตอร์ของท่านในการดูเว็บทั่วไปที่อยู่บนเครือข่ายอินเทอร์เน็ตได้

จากเท่าที่กล่าวมา ขณะนี้ท่านคงได้แนวคิดในภาพรวมแล้วว่าไฟร์วอลมีหน้าที่อย่างไร ต่อไปนี้ท่านควรจะได้ทราบถึงข้อมูลต่างๆ ที่จำเป็นสำหรับการตั้งค่าไฟร์วอลของท่าน โดยข้อมูลเหล่านี้ได้ถูกรวบรวมไว้ในขั้นตอนการปฏิบัติด้านล่างนี้

1. โปรแกรม – โปรแกรมใดบ้างในเครื่องคอมพิวเตอร์ของท่านที่ต้องการการเชื่อมต่อออกไปยังเครือข่ายอินเทอร์เน็ตถึงแม้ว่าหลายๆ โปรแกรมจะใช้การเชื่อมต่อที่เหมือนกันออกไปยังที่หมายในเครือข่ายอินเทอร์เน็ตที่เดียวกัน แต่ท่านก็ควรจะทราบชื่อของโปรแกรมแต่ละโปรแกรมที่ต้องการการเชื่อมต่อนั้น โดยท่านควรหลีกเลี่ยงการ

อนุญาตให้โปรแกรมใดๆ ก็ได้ให้สามารถทำการเชื่อมต่อกับอินเทอร์เน็ตได้ ซึ่งอาจทำให้เกิดผลเสียที่ไม่ต้องการและไม่ได้รับการบันทึกไว้ได้

2. ที่หมาย – ที่หมายใดในเครือข่ายอินเทอร์เน็ตที่โปรแกรมของท่านต้องการเชื่อมต่อออกไป ที่หมายนี้จะประกอบด้วยที่อยู่ (address) และหมายเลข**พอร์ท** (port number) ในบางกรณีจะมีการอนุญาตให้โปรแกรมเชื่อมต่อกับที่หมายใดๆ ก็ได้บนอินเทอร์เน็ตเช่น การยอมให้โปรแกรมดูเว็บสามารถออกไปดูเว็บใดก็ได้ แต่ในบางกรณีหากเป็นไปได้ท่านก็ควรจำกัดการเชื่อมต่ออินเทอร์เน็ตของบางโปรแกรมให้เชื่อมต่อได้เฉพาะบางที่หมายเท่านั้น
3. อนุญาต – จะอนุญาตการเชื่อมต่อนี้หรือไม่ ข้อมูลนี้จะถูกนำไปกำหนดเป็นกฎของไฟร์วอลของท่าน
4. ชั่วคราว – การเชื่อมต่อนี้เป็นการเชื่อมต่อชั่วคราวหรือถาวร ยกตัวอย่างเช่น ท่านอาจตั้งค่าการเชื่อมต่อใดๆ ที่เกิดขึ้นบ่อยๆ เช่น 5 ครั้งต่อวัน เป็นการเชื่อมต่อแบบถาวรโดยกำหนดการเชื่อมต่อนี้เข้าไว้ในกฎของไฟร์วอล หากการเชื่อมต่อใดที่เกิดขึ้นนานๆ ครั้ง ท่านอาจกำหนดให้เป็นการเชื่อมต่อแบบชั่วคราว (โดยให้ไฟร์วอลขออนุญาตเป็นครั้งๆ ไป)

ท่านควรใช้ขั้นตอนเหล่านี้ในการพิจารณาการเชื่อมต่อแต่ละประเภทที่ท่านใช้เพื่อเป็นข้อมูลในการสร้างกฎของไฟร์วอล ซึ่งข้อมูลเหล่านี้จะเป็นตัวบอกว่าท่านควรสร้างกฎในไฟร์วอลเพิ่มหรือไม่ โดยที่ไฟร์วอลส่วนมากจะสามารถให้ท่านอนุญาตการเชื่อมต่อเป็นครั้งๆ ได้โดยตั้งค่าการเชื่อมต่อเป็นการเชื่อมต่อแบบชั่วคราวและไม่ต้องสร้างกฎในไฟร์วอลเพิ่ม ซึ่งหากเป็นไปได้ท่านควรให้มีการเชื่อมต่อแบบชั่วคราวให้มากที่สุด

เมื่อท่านใช้โปรแกรมที่เชื่อมต่อกับอินเทอร์เน็ตจากเครื่องของท่าน ท่านจะได้เรียนรู้ว่าโปรแกรมนั้นเชื่อมต่อกับอินเทอร์เน็ตอย่างไร และท่านจะสามารถสร้างกฎที่เหมาะสมสำหรับไฟร์วอลของท่านได้ โดยกฎที่เหมาะสมนี้จะเป็นความสมดุลย์ระหว่างการปิดไม่ให้ข้อมูลใดๆ ผ่านเข้าออกเลยและการยอมให้ข้อมูลทั้งหมดผ่านเข้าออกได้

ซึ่งในบางกรณีอาจจะมีข้อยกเว้นในกฎที่ท่านสร้างขึ้น เช่นท่านอาจจะต้องการให้โปรแกรมดูเว็บของท่านออกไปดูเว็บใดๆ ก็ได้ ยกเว้นเว็บบางเว็บ ซึ่งก็เปรียบเสมือนกับการที่เจ้าหน้าที่รักษาความปลอดภัยยอมให้พนักงานทุกคนเข้าออกอาคารได้เว้นพนักงานบางคนที่องค์กรมีคำสั่งให้มีความระมัดระวังเป็นพิเศษ

การสร้างข้อยกเว้นในกฎของไฟร์วอลนั้น จะต้องมีการระบุข้อยกเว้นขึ้นก่อนตัวกฎ ยกตัวอย่างเช่น จะต้องมีการกำหนดรายชื่อเว็บที่ห้ามออกไปดูไว้ก่อนการกำหนดกฎที่ยอมให้ออกไปดูเว็บใดก็ได้

ทั้งนี้เนื่องจากในการตรวจสอบแพ็คเก็ตโดยอ้างอิงจากกฎนั้น ไฟร์วอลจะใช้กฎจากบนลงล่างและเมื่อพบกฎที่เหมาะสมกับแพ็คเก็ตนั้นแล้วก็จะปฏิบัติตามกฎนั้นโดยไม่ดูกฎอื่นๆอีก ดังนั้นตามตัวอย่างด้านบน หากเรานำเอากฎที่ยอมให้ออกไปดูเว็บใดก็ได้มาวางไว้ก่อนกฎการห้ามออกไปดูบางเว็บ เมื่อไฟร์วอลตรวจสอบแพ็คเก็ตโดยอ้างอิงกฎ ไฟร์วอลจะพบกฎที่ยอมให้ออกไปดูเว็บใดก็ได้ก่อนและจะปฏิบัติตามกฎนั้น ดังนั้นไฟร์วอลจะไม่เคยมองลงไปถึงกฎที่ห้ามดูบางเว็บได้เลย เพราะฉะนั้นจะเห็นได้ว่าการเรียงลำดับกฎในไฟร์วอลนั้นมีความสำคัญมาก

ในไฟร์วอลหลายตัว เราสามารถตั้งค่าให้มีการถามรหัสผ่านทุกครั้งก่อนการเปลี่ยนแปลงหรือเพิ่มกฎของไฟร์วอลได้ ซึ่งนับเป็นการป้องกันอีกชั้นหนึ่งจากการเปลี่ยนแปลงกฎโดยที่ท่านไม่ได้ตั้งใจทั้งจากตัวท่านเอง ผู้ใช้คนอื่น หรือผู้บุกรุก ทั้งนี้การกำหนดรหัสผ่านนี้ท่านควรปฏิบัติตามข้อปฏิบัติที่ 6 – ใช้รหัสผ่านที่ยากต่อการเดา

โดยทั่วไปแล้วไฟร์วอลจะมีอยู่ 2 ประเภทคือ ฮาร์ดแวร์และซอฟท์แวร์ (ที่เป็นโปรแกรม) ไฟร์วอลที่เป็นซอฟท์แวร์โดยทั่วไปก็จะมีอีก 2 ประเภทคือ ที่เป็นของฟรี (freeware) และที่เป็นการค้า (ต้องซื้อ) อย่างน้อยที่สุดท่านควรจะใช้ไฟร์วอลที่เป็นของฟรีในเครื่องคอมพิวเตอร์ของท่าน โดยเฉพาะอย่างยิ่งถ้าเครื่องของท่านเป็นเครื่องคอมพิวเตอร์โน้ตบุ๊คที่ท่านนำไปเชื่อมต่อกับเครือข่ายในที่ต่างๆ เช่นในสำนักงานของท่าน ที่บ้านท่าน หรือในการประชุมต่างๆ

หากท่านมีงบประมาณเพียงพอที่จะจัดหาไฟร์วอลที่เป็นฮาร์ดแวร์มาได้ ท่านก็ควรติดตั้งไฟร์วอลที่เป็นฮาร์ดแวร์ด้วย แต่ทั้งนี้ถือว่าเป็นความเร่งด่วนอันดับหลังๆ โดยที่รายละเอียดของการติดตั้งไฟร์วอลที่เป็นฮาร์ดแวร์นี้อยู่ในข้อปฏิบัติที่ 8 เนื่องจากในเครือข่ายขององค์กรส่วนใหญ่จะมีไฟร์วอลประเภทนี้อยู่แล้ว

ไฟร์วอลเป็นสิ่งที่ใช้ในการรักษาความปลอดภัยเครื่องคอมพิวเตอร์ของท่าน โดยที่ตัวไฟร์วอลจะอยู่ระหว่างเครื่องของท่านและเครือข่ายอินเทอร์เน็ตท่านสามารถควบคุมข้อมูลที่ผ่านเข้าออกเครื่องของท่านและควบคุมโปรแกรมที่เชื่อมต่อกับอินเทอร์เน็ตได้โดยใช้ไฟร์วอล โดยการอนุญาตหรือปฏิเสธการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์ของท่านกับเครื่องอื่นที่อยู่ในเครือข่ายอินเทอร์เน็ต ทั้งนี้ท่านสามารถหาไฟร์วอลมาติดตั้งและใช้บนเครื่องคอมพิวเตอร์ของท่านได้โดยไม่เสียค่าใช้จ่ายใดๆ นอกจากนี้ยังมีไฟร์วอลประเภทที่ท่านต้องใช้งบประมาณในการซื้อมาติดตั้งและใช้ แต่ไฟร์วอล
ประเภทนี้จะมีขีดความสามารถเพิ่มขึ้นจากไฟร์วอลที่เป็นของฟรี

ข้อปฏิบัติที่ 5 – สำรองไฟล์ที่สำคัญ

ในชีวิตของคนเรานั้น โดยทั่วไปเราจะมีทรัพย์สินอยู่ 2 ประเภทคือ ทรัพย์สินที่เราสามารถหามาทดแทนได้ และทรัพย์สินที่เราไม่สามารถหามาทดแทนได้ สำหรับทรัพย์สินที่เราไม่สามารถหามาทดแทนได้นั้นเราอาจจะเก็บทรัพย์สินเหล่านี้ไว้ในที่ปลอดภัย เช่น ภายในบ้าน ในตู้นิรภัย หรือในธนาคาร เป็นต้น โดยนอกจากนี้เราอาจมีการประกันภัยทรัพย์สินเหล่านี้ในกรณีสูญหายหรือเสียหายเพื่อที่เราจะได้สามารถทดแทนทรัพย์สินเหล่านี้ได้

ท่านได้แบ่งสิ่งต่างๆ ที่อยู่ในเครื่องคอมพิวเตอร์ของท่านเป็น 2 ประเภทดังกล่าวด้านบนหรือไม่? ท่านได้มีการจัดการใดๆ กับสิ่ง (ในกรณีนี้คือไฟล์ต่างๆ) ที่ท่านไม่สามารถทดแทนได้หรือไม่? ยกตัวอย่างเช่น ไฟล์ที่ใช้เก็บข้อมูลสำคัญของตัวท่านเองหรือของงานท่าน รูปภาพที่ท่านถ่ายไว้โดยใช้กล้องดิจิตอล นิยายหรือบทความที่ท่านใช้เวลานานในการเขียน เป็นต้น จะเกิดอะไรขึ้นหากเครื่องคอมพิวเตอร์ของท่านเกิดผิดปกติหรือถูกทำลายโดยผู้บุกรุก ท่านจะสูญเสียไฟล์เหล่านั้นไปโดยไม่สามารถเรียกคืนกลับมาได้เลยหรือไม่

ในกรณีของรถยนต์ หากยางรถยนต์รั่วเราสามารถใช้ยางอะไหล่ทดแทนเพื่อให้รถยนต์วิ่งต่อไปได้ จะเกิดอะไรขึ้นหากรถยนต์ไม่มียางอะไหล่? ท่านจะซื้อรถยนต์คันหนึ่งหรือไม่หากรถคันนั้นไม่มียางอะไหล่? ถึงแม้ท่านจะซื้อรถยนต์ใช้แล้วที่ไม่มียางอะไหล่ ท่านก็คงจะซื้อยางอะไหล่สำหรับรถยนต์คันนั้นในไม่ช้า

เปรียบเทียบกรณีรถยนต์กับเครื่องคอมพิวเตอร์ของท่าน ท่านมี “ยางอะไหล่” คือ วิธีการที่จะดำเนินงานต่อไป ในกรณี “ยางรั่ว” หรือเครื่องคอมพิวเตอร์เสียหรือหรือถูกโจมตีหรือไม่ หรืออีกนัยหนึ่งคือ ท่านได้สำรองไฟล์ของท่านไว้ใน**สื่อ**อื่นเพื่อที่ท่านจะสามารถนำไฟล์นั้นกลับมาใช้ได้ใหม่หรือไม่? และหากท่านจะไม่ขับรถยนต์ที่ไม่มียางอะไหล่เพราะเหตุใดท่านจึงใช้เครื่องคอมพิวเตอร์ที่ไม่มีอุปกรณ์สำรองไฟล์?

ท่านควรใช้ข้อพิจารณาต่อไปนี้ประกอบการตัดสินใจในการสำรองไฟล์ที่สำคัญบนเครื่องคอมพิวเตอร์ของท่าน

1. อะไร – ท่านควรสำรองไฟล์ใดบ้าง ไฟล์ที่ท่านเลือกที่จะสำรองควรเป็นไฟล์ที่ท่านไม่สามารถสร้างใหม่หรือติดตั้งใหม่ได้โดยง่าย เช่น ซีดี-รอมหรือฟล็อปปี้ดิสค์ที่มากับเครื่องคอมพิวเตอร์ของท่าน หรือไฟล์ข้อมูลใดๆ ที่ท่านสามารถสร้างใหม่ได้แต่ต้องใช้เวลานาน

ในการสร้าง เช่นไฟล์เอกสารที่มีความยาวมากซึ่งหากสูญเสียไปท่านจะต้องเสียเวลาเป็นอันมากในการพิมพ์เข้าไปใหม่ เป็นต้น

2. เมื่อใด – ท่านควรสำรองไฟล์เหล่านั้นบ่อยเท่าใด ในอุดมคติท่านควรสำรองไฟล์ทุกครั้งที่มีการเปลี่ยนแปลงไฟล์นั้น มิฉะนั้นหากเกิดความเสียหายขึ้นท่านจะต้องกลับไปทำการเปลี่ยนแปลงใหม่ทั้งหมดที่ไม่ได้สำรองไว้หลังจากที่ได้นำไฟล์ที่สำรองไว้มาติดตั้งใหม่
3. อย่างไร – ท่านจะสำรองไฟล์ไว้ในสื่อชนิดใด ท่านควรสำรองไฟล์ไว้ในสื่อใดก็ได้ที่ท่านมีอยู่ ทั้งนี้ท่านควรได้พิจารณาความจุของสื่อนั้นและความสะดวกในการใช้สื่อนั้นด้วย ยกตัวอย่างเช่น เครื่องคอมพิวเตอร์ส่วนใหญ่จะมาพร้อมกับเครื่องฟล็อปปี้ไดร์ฟ ซึ่งท่านสามารถใช้ฟล็อปปี้ดิสค์ในการสำรองข้อมูลของท่านได้ แต่ท่านอาจจะต้องใช้แผ่นฟล็อปปี้ดิสค์จำนวนมากและใช้เวลามากในการสำรองข้อมูลและการสำรองข้อมูลอาจจะไม่สะดวกนัก ซึ่งหากท่านใช้ฮาร์ดดิสค์ที่พกพาได้หรือเครื่องอ่าน/เขียนซีดี-รอมอาจจะประหยัดเวลาได้มากกว่าและสะดวกกว่า

   ในกรณีที่ท่านไม่มีอุปกรณ์สำรองข้อมูล ท่านสามารถใช้บริการสำรองข้อมูลที่มีอยู่บนอินเทอร์เน็ตได้ โดยบริการนี้จะให้ท่านสามารถสำรองข้อมูลของท่านลงบนเครื่องคอมพิวเตอร์เครื่องอื่นที่อยู่บนเครือข่ายอินเทอร์เน็ตได้ โดยในบางบริการจะให้บริการโดยทำให้แหล่งสำรองข้อมูลนั้นเปรียบเสมือนเป็นฮาร์ดไดร์ฟอีกตัวหนึ่งบนเครื่องของท่าน (เรียกว่าเป็นการให้บริการแบบผู้รับบริการ “มองไม่เห็น” หรือ transparent) ท่านเพียงแต่สำเนาไฟล์ที่ท่านต้องการสำรองไปไว้บนฮาร์ดไดร์ฟตัวนั้นโดยใช้วิธีปกติของเครื่องของท่าน ก็จะเป็นการสำรองข้อมูลได้อย่างเรียบร้อย ท่านสามารถหาแหล่งที่ให้บริการเหล่านี้ได้โดยการสืบค้นจากอินเทอร์เน็ต
4. ที่ใด – หลังจากที่ท่านได้สำรองข้อมูลลงบนสื่อบันทึกข้อมูลแล้ว ท่านควรจะเก็บรักษาสื่อนั้นไว้ที่ใด? ไม่ว่าท่านจะสำรองข้อมูลโดยใช้สื่อประเภทใด ท่านควรให้ความสำคัญกับสถานที่เก็บรักษาสื่อเหล่านั้นด้วย

   ท่านได้ทราบแล้วว่าผู้บุกรุกจะพยายามที่เจาะเข้ามาในเครื่องคอมพิวเตอร์ของท่านเพื่อที่จะเข้าถึงข้อมูลและใช้ทรัพยากรในเครื่องของท่าน อีกวิธีหนึ่งที่ผู้บุกรุกจะสามารถเข้าถึงข้อมูลของท่านก็โดยการขโมยสื่อที่ท่านใช้สำรองข้อมูลของท่าน เป็นที่แน่นอนว่าการที่ผู้บุกรุกจะกระทำเช่นนี้ได้ผู้บุกรุกจะต้องสามารถเข้าถึงแหล่งสำรองข้อมูลได้ทางกายภาพ (คือตัวของผู้บุกรุกจะต้องไปอยู่ที่นั้น) จึงอาจกระทำได้ยาก แต่อย่างไรก็ตามท่านไม่ควรละเลยในข้อนี้และควรทราบอยู่เสมอว่าสื่อที่ท่านใช้ในการสำรองข้อมูลนั้นอยู่ที่ใด

เช่นเดียวกับการเก็บเอกสารสำคัญไว้ในตู้นิรภัยกันไฟ ท่านควรจะพิจารณาถึงการที่สื่อที่ท่านใช้สำรองข้อมูลจากเครื่องคอมพิวเตอร์ของท่านจะถูกทำลายหากสำนักงานหรือบ้านของท่านถูกทำลายหรือเสียหาย ซึ่งหมายความว่าท่านควรเก็บสื่อสำรองข้อมูลไว้ในตู้นิรภัยกันไฟและเก็บไว้ในสถานที่อื่นนอกเหนือจากที่ตั้งเครื่องคอมพิวเตอร์ของท่าน ซึ่งในการนี้จะเห็นได้ว่าเป็นความขัดแย้งระหว่างความปลอดภัยกับความสะดวก การเก็บสื่อสำรองข้อมูลไว้ในสถานที่อื่นนั้นมีความปลอดภัยสูงกว่า แต่เมื่อใดที่ท่านต้องการสำรองข้อมูลหรือนำข้อมูลสำรองกลับมาใช้อาจจะต้องเสียเวลาในการเดินทาง ดังนั้นท่านจึงควรพิจารณาประนีประนอมระหว่างความปลอดภัยกับความสะดวกนี้เพื่อหาหนทางปฏิบัติที่ดีที่สุด หรือท่านอาจสำรองข้อมูลไว้หลายชุดแล้วเก็บรักษาไว้ในที่ต่างๆ ก็ได้

หากท่านมียางอะไหล่สำหรับรถยนต์ของท่านหรือมีตู้นิรภัยที่ใช้เก็บของมีค่าของท่าน ก็ถือได้ว่าท่านได้เตรียมพร้อมสำหรับความเสียหายที่อาจเกิดขึ้นในชีวิตประจำวันของท่านแล้ว นอกจากนี้แล้วท่านควรจะได้เตรียมพร้อมสำหรับความเสียหายที่อาจเกิดขึ้นกับเครื่องคอมพิวเตอร์ของท่านโดยการสำรองข้อมูลที่สำคัญในเครื่องคอมพิวเตอร์ของท่านแล้วเก็บไว้ในที่ปลอดภัย และทำการสำรองข้อมูลให้บ่อยที่สุดเท่าที่จะทำได้

ทั้งนี้ท่านควรใช้ข้อพิจารณาทั้ง 4 ข้อข้างต้นในการสำรองข้อมูล และถึงแม้ท่านไม่สามารถปฏิบัติตามคำแนะนำได้ทั้งหมด เช่น ท่านอาจไม่สามารถเก็บข้อมูลสำรองในตู้นิรภัยได้ ท่านก็ควรสำรองข้อมูลของท่านเท่าที่ทำได้ เนื่องจากการสำรองข้อมูลใดๆ ก็ยังดีกว่าการไม่สำรองข้อมูลเลย

ข้อปฏิบัติที่ 6 – ใช้รหัสผ่านที่ยากต่อการเดา

ที่พักอาศัยของท่านจะต้องมีประตูและหน้าต่าง ซึ่งตามปกติแล้วในเวลาส่วนใหญ่ท่านจะล็อคประตูและหน้าต่างเหล่านี้ นอกจากนี้หากเป็นการล็อคโดยใช้กุญแจ ท่านก็คงจะใช้กุญแจที่ต่างกันสำหรับประตูและหน้าต่างแต่ละบาน ท่านจะต้องทราบว่าเมื่อใดควรล็อคประตูหน้าต่าง และคงจะไม่แจกจ่ายกุญแจให้คนแปลกหน้าหรือแม้แต่เพื่อนส่วนใหญ่ และท่านควรจะเก็บลูกกุญแจไว้ในที่ปลอดภัย

หลักการล็อคประตูหน้าต่างตามที่กล่าวมานี้ก็จะคล้ายคลึงกับหลักการใช้รหัสผ่านในเครื่องคอมพิวเตอร์ ท่านจะต้องมีรหัสผ่านสำหรับเครื่องคอมพิวเตอร์แต่ละเครื่องหรือบริการบนเครือข่ายแต่ละบริการ (เช่น การใช้ อีเมล์, การเป็นสมาชิกเว็บต่างๆ) ซึ่งรหัสผ่านแต่ละตัวไม่ควรจะเหมือนกันและไม่ควรมีความเกี่ยวข้องกัน ท่านควรเก็บรหัสผ่านไว้ในที่ปลอดภัย (ที่ที่ปลอดภัยที่สุดก็คือ

การจำรหัสผ่านไว้ ท่านไม่ควรจดรหัสผ่านไว้ในที่ใดๆ) และท่านไม่ควรบอกรหัสผ่านให้ผู้อื่นทราบ (ไม่ควรบอกแม้แต่เพื่อนของท่านเอง)

เปรียบเทียบกับลูกกุญแจไขประตูที่พักของท่าน ลุกกุญแจนี้จะค่อนข้างซับซ้อน โดยจะมีบากและร่องต่างๆ ที่สร้างขึ้นได้ไม่ง่ายนักและมีความหลากหลายมาก ซึ่งหากบากและร่องเหล่านี้สร้างขึ้นได้โดยง่ายหรือไม่มีความหลากหลายก็จะทำให้เป็นการง่ายต่อพวกมิจฉาชีพที่จะสร้างกุญแจขึ้นมาหลายๆ แบบแล้วลองใช้กุญแจเหล่านั้นไขประตูของท่านทีละดอกจนกระทั่งประสบความสำเร็จ วิธีนี้เป็นวิธีแบบลองผิดลองถูก (ศัพท์ในวงการคอมพิวเตอร์เรียกว่าเป็นวิธี **“ใช้กำลัง”** (brute force)) ซึ่งสามารถประสบความสำเร็จได้ถึงแม้อาจจะต้องใช้เวลานาน แต่อย่างไรก็ตามไม่ว่าลูกกุญแจของท่านจะมีความซับซ้อนเพียงใด หากพวกมิจฉาชีพสามารถครอบครองลูกกุญแจของท่านได้แม้เพียงชั่วคราวพวกเขาก็จะสามารถสร้างกุญแจเลียนแบบและใช้ลูกกุญแจเลียนแบบนั้นปลดล็อคประตูท่านได้

รหัสผ่านสามารถมีความซับซ้อนได้เช่นกัน ในกรณีส่วนใหญ่ท่านสามารถใช้ตัวอักษร (ทั้งตัวเล็กและใหญ่) และตัวเลขใดๆ รวมถึงสัญญลักษณ์ต่างๆ (เช่น !@#$%) ท่านสามารถกำหนดรหัสผ่านของท่านให้มีความซับซ้อนเพียงใดก็ได้ แต่ท่านจะต้องสามารถจำรหัสผ่านนี้ได้โดยไม่ต้องจดลงไว้ที่ใดที่หนึ่ง

ผู้โจมตีเครื่องคอมพิวเตอร์ก็ใช้วิธีลองผิดลองถูกหรือวิธีใช้กำลังในการเดารหัสผ่านของท่าน ผู้โจมตีจะใช้คำต่างๆที่อาจจะมาจากพจนานุกรมมาเดาเป็นรหัสผ่านของท่านที่ละคำจนกระทั่งประสบความสำเร็จ ถ้าผู้โจมตีทราบข้อมูลส่วนตัวของท่าน ผู้โจมตีอาจจะนำข้อมูลเหล่านั้นมาเดาเป็นรหัสผ่านของท่านด้วย เช่น ชื่อคู่สมรสของท่าน ที่ทำงานของท่าน วันเดือนปีเกิดของท่าน เป็นต้น ซึ่งโดยทั่วไปแล้วผู้โจมตีมักจะประสบความสำเร็จ ถึงแม้ท่านจะแปลงรหัสผ่านโดยเพิ่มตัวเลขหรือตัวอักษรเข้าที่ด้านหน้าหรือด้านหลังหรือแปลงตัวอักษร o ด้วยตัวเลข 0 ก็จะไม่เป็นผลเนื่องจากผู้โจมตีย่อมทราบถึงวิธีการเหล่านี้และสามารถเดารหัสผ่านในแนวทางนั้นได้เช่นกัน

เช่นเดียวกันกับลูกกุญแจที่ใช้ไขประตู รหัสผ่านที่ซับซ้อนก็สามารถถูกลอกเลียนแล้วนำไปใช้ได้ดังที่ได้กล่าวไว้ในหัวข้อต้นๆ ในเรื่องของการส่งข้อมูลไปในเครือข่ายอินเทอร์เน็ตนั้นเป็นการส่งข้อมูลไปแบบเปิดเผยสามารถเห็นได้ ไม่ว่ารหัสผ่านของท่านจะซับซ้อนเพียงใดหากมีการส่งรหัสผ่านไปแบบเปิดเผยสามารถเห็นได้ ผู้โจมตีก็สามารถมองเห็นและสำเนารหัสผ่านนั้นไว้ได้เพื่อนำไปใช้ภายหลัง การกระทำเช่นนี้เรียกว่าการ **“ดมกลิ่น”** (sniffing) และเป็นวิธีการที่ใช้กันแพร่หลายในหมู่ผู้โจมตี

หลักการในที่นี้ก็คือ ท่านจะต้องใช้รหัสผ่านที่แตกต่างกันสำหรับเครื่องคอมพิวเตอร์หรือบริการ (อาจเรียกได้ว่า account) ที่ต่างกัน โดยท่านสามารถใช้ข้อพิจารณาด้านล่างช่วยในการกำหนดรหัสผ่านของท่านได้

1. ยากต่อการเดา – รหัสผ่านนี้ยากต่อการเดา (หมายถึงว่ามีความยาวและมีความซับซ้อนมากเท่าที่ระบบนั้นๆ จะยินยอมหรือไม่
2. ซ้ำซ้อน – รหัสผ่านนี้ซ้ำซ้อนหรือเกี่ยวข้องกับรหัสผ่านสำหรับเครื่องหรือบริการอื่นหรือไม่
3. จำได้ – ท่านสามารถจำรหัสผ่านนี้ได้โดยไม่ต้องจดลงไว้ที่ใดได้หรือไม่
4. เวลา – ท่านใช้รหัสผ่านนี้มานานเท่าใด (หากนานมากควรเปลี่ยนรหัสผ่าน)

แม้ท่านจะใช้ข้อพิจารณาเหล่านี้ในการกำหนดรหัสผ่านแล้ว แต่ท่านก็ควรตระหนักว่าผู้โจมตีสามารถใช้การดมกลิ่นแล้วดักจับรหัสผ่านของท่านได้

ท่านควรใช้รหัสผ่านกับเครื่องคอมพิวเตอร์และบริการบนเครือข่ายทั้งหมดของท่าน รหัสผ่านทุกตัวควรเป็นรหัสผ่านที่ยากต่อการเดาและที่ท่านสามารถจำได้ด้วย และรหัสผ่านแต่ละตัวไม่ควรซ้ำหรือเกี่ยวเนื่องกัน รหัสผ่านที่ยากต่อการเดาจะเป็นรหัสผ่านที่ยาวและใช้การผสมผสานกันของตัวอักษรเล็กและใหญ่รวมทั้งตัวเลขและสัญญลักษณ์ต่างๆและไม่เป็นคำศัพท์ในพจนานุกรม นอกจากนี้ท่านควรตระหนักว่าหากมีการส่งรหัสผ่านไปแบบเปิดเผยสามารถเห็นได้ ในเครือข่ายอินเทอร์เน็ตแล้วผู้โจมตีจะสามารถดักจับและนำรหัสผ่านนั้นไปใช้ได้ไม่ว่ารหัสผ่านนั้นจะยากต่อการเดาเพียงใด (รายละเอียดตามหัวข้อ การส่งข้อมูลไปโล่งๆ)

ข้อปฏิบัติที่ 7 – ใช้ความระมัดระวังเมื่อดาวน์โหลดและติดตั้งโปรแกรม

ก่อนที่ท่านจะซื้อเครื่องใช้ใดๆ เข้าบ้าน โดยทั่วไปแล้วท่านมักจะไม่คิดถึงอันตรายของเครื่องใช้นั้นที่อาจมีต่อท่านในการใช้ ทั้งนี้เนื่องจากจะมีองค์กรควบคุมมาตรฐานการผลิดเครื่องใช้นั้นอยู่แล้ว เช่นมาตรฐานของกระทรวงอุตสาหกรรม และหากเครื่องใช้นั้นมีตรามาตรฐานติดอยู่ท่านก็จะค่อนข้างมั่นใจได้ว่าเครื่องใช้นี้จะไม่มีอันตราย

แต่สำหรับเครือข่ายอินเทอร์เน็ตนั้นไม่ได้มีมาตรฐานหรือองค์กรหนึ่งองค์กรใดที่ทำหน้าที่ในการตรวจสอบโดยเฉพาะ ดังนั้นใครก็ตามที่เขียนโปรแกรมขึ้นมาก็สามารถแจกจ่ายโปรแกรมนั้นได้โดยอิสระ ท่านเคยได้ติดตั้งโปรแกรมที่มากับซีดี-รอมแจกฟรีหรือไม่ และท่านจะทราบได้อย่างไรว่าโปรแกรมที่ท่านติดตั้งนั้นเป็นไปตามสลากที่ติดไว้กับซีดี-รอม คำตอบก็คือท่านไม่ทราบและการที่จะทราบได้นั้นจะต้องใช้วิธีที่ค่อนข้างลำบากและซับซ้อน

ไม่ว่าท่านจะได้โปรแกรมมาโดยวิธีใด ความเป็นจริงก็คือเมื่อท่านใช้โปรแกรมนั้นจะเป็นการเปิดเครื่องคอมพิวเตอร์ของท่านให้แก่โปรแกรมนั้นโดยแล้วแต่ที่ผู้เขียนโปรแกรมจะกำหนด กล่าวคือ กิจกรรมใดก็ตามที่ท่านสามารถทำได้บนเครื่องคอมพิวเตอร์ของท่าน โปรแกรมนั้นก็สามารถทำได้ เช่น หากท่านสามารถลบไฟล์บนเครื่องของท่านได้ โปรแกรมนั้นก็สามารถลบไฟล์บนเครื่องของท่านได้ (โดยที่ท่านอาจจะไม่ทราบ) หากท่านสามารถส่งอีเมล์ได้ โปรแกรมนั้นก็สามารถส่งอีเมล์ในนามของท่านได้ หากท่านสามารถติดตั้งโปรแกรมอื่นๆ ได้ โปรแกรมนั้นก็สามารถติดตั้งโปรแกรมอื่นๆ เพิ่มเติมได้เช่นเดียวกัน ที่กล่าวมานี้หมายความว่า สิ่งใดก็ตามที่ท่านสามารถทำได้บนเครื่องของท่าน ผู้บุกรุกก็สามารถทำได้โดยผ่านทางโปรแกรมที่ท่านติดตั้งและใช้งาน

ในบางกรณีโปรแกรมที่ท่านได้มาจะไม่มีคำอธิบายหรือไม่มีคู่มือการใช้ใดๆ แนบมาด้วย อาจไม่มีชื่อหรือวิธีการติดต่อผู้เขียนโปรแกรม ดังนั้นท่านจะต้องตัดสินใจด้วยตัวเองว่าการใช้โปรแกรมนั้นจะประโยชน์ที่ได้จะคุ้มกับการเสี่ยงต่ออันตรายที่อาจเกิดขึ้นหรือไม่

ดังนั้นสิ่งที่ท่านจะต้องทำก็คือ จะต้องตัดสินใจว่าโปรแกรมที่ท่านได้มาจะทำประโยชน์ได้ตามที่ท่านหวังหรือไม่โดยในขณะเดียวกันจะต้องไม่ทำอันตรายต่อเครื่องคอมพิวเตอร์และข้อมูลบนเครื่องคอมพิวเตอร์ของท่านด้วย ท่านจะต้องตรวจสอบว่าโปรแกรมนี้จะทำงานได้ตรงตามที่อ้างหรือไม่ ท่านจะต้องประเมินความเสี่ยงที่มีต่อเครื่องคอมพิวเตอร์ของท่านและตัวท่านในการที่จะใช้โปรแกรมนี้

ซึ่งก็เป็นกระบวนการเดียวกันกับเมื่อท่านจะซื้อเครื่องใช้มาใช้ในบ้านของท่าน เพียงแต่ท่านอาจกระทำไปโดยไม่รู้ตัว เมื่อท่านซื้อเครื่องใช้ ท่านจะซื้อจากร้านในละแวกบ้านที่ท่านคุ้นเคยหรือจากร้านตัวแทนบริษัทใหญ่ที่เป็นที่น่าเชื่อถือ ซึ่งหากมีปัญหาใดๆ เกิดขึ้น ท่านสามารถนำเครื่องใช้นั้นกลับไปเปลี่ยนหรือซ่อมแซมได้ หากเครื่องใช้นั้นทำให้ท่านได้รับอันตรายท่านก็อาจได้รับการชดใช้ความเสียหายตามกฎหมายได้ ซึ่งความน่าเชื่อถือของผู้ขาย การรับประกันสินค้า และกฎหมายที่เกี่ยวกับการชดใช้ความเสียหายนั้น เป็นปัจจัยที่ลดความเสี่ยงของท่านลงจนกระทั่งท่านตัดสินใจที่จะซื้อเครื่องใช้นั้นๆ ในที่สุด

ดังนั้นท่านควรใช้กระบวนการคล้ายกันนี้เมื่อใดก็ตามที่ท่านจะซื้อโปรแกรมมาใช้งาน กล่าวคือ

1. เรียนรู้ – เรียนรู้เกี่ยวกับโปรแกรมที่ท่านจะซื้อให้มากที่สุดเท่าที่จะทำได้ โดยท่านควรจะทราบอย่างแน่ชัดว่าตัวโปรแกรมนั้นทำอะไรได้บ้าง
2. เข้าใจ – ศึกษานโยบายการรับประกันและการคืนสินค้าของผู้ขายให้เข้าใจก่อนที่ท่านจะซื้อโปรแกรมนั้น

3. ซื้อ - ซื้อจากร้านค้าในละแวกบ้านท่านที่ท่านรู้จักและคุ้นเคยหรือจากร้านตัวแทนบริษัทใหญ่ที่เป็นที่น่าเชื่อถือ

ในปัจจุบันอาจจะยังไม่มีตัวกฎหมายที่ชัดเจนเกี่ยวกับอันตรายของโปรแกรมที่อาจเกิดกับผู้ใช้ อย่างไรก็ตามในระหว่างนี้ท่านควรใช้ข้อพิจารณาทั้ง 3 ข้อด้านบนเป็นพื้นฐานในการพิจารณาก่อนจะซื้อโปรแกรมใดๆ

เครือข่ายอินเทอร์เน็ตนั้นมีจุดเด่นอยู่อย่างหนึ่งคือการที่ผู้ใช้สามารถดาวน์โหลดโปรแกรมที่มีอยู่มากมายมาใช้ฟรีได้ โปรแกรมเหล่านี้มีความหลากหลายสูง มีให้ใช้กับระบบหรือเครื่องคอมพิวเตอร์ทุกรูปแบบ และนับวันจะยิ่งทวีจำนวนมากขึ้น ดังนั้นสิ่งที่ท้าทายคือจะทำอย่างไรท่านจึงจะสามารถตัดสินใจว่าโปรแกรมใดที่น่าเชื่อถือพอที่ท่านจะยอมรับความเสี่ยงในการดาวน์โหลดและนำมาติดตั้งและใช้ในเครื่องคอมพิวเตอร์ของท่านได้

ในการตัดสินใจดังกล่าวนี้ ท่านควรใช้ข้อพิจารณาดังต่อไปนี้

1. สิ่งที่ทำ – โปรแกรมนี้ทำอะไรได้บ้าง ควรจะมีคำอธิบายอย่างชัดเจนว่าโปรแกรมนี้ทำอะไรได้บ้าง คำอธิบายนี้อาจจะอยู่ในเว็บที่ท่านดาวน์โหลดโปรแกรมนี้มาหรือในไฟล์ที่มากับโปรแกรมนี้ แต่ท่านควรจะได้ตระหนักว่าหากโปรแกรมนี้ถูกเขียนขึ้นมาโดยมีวัตถุประสงค์อันมิชอบแล้ว ผู้เขียนหรือผู้บุกรุกจะไม่บอกการว่าโปรแกรมนี้จะเป็นผลร้ายต่อเครื่องของท่าน และจะพยายามหลอกลวงท่านให้เชื่อใจและทำการติดตั้ง ดังนั้นสิ่งที่ท่านทำได้คือเรียนรู้เกี่ยวกับโปรแกรมนี้ให้มากที่สุดและใช้วิจารณญาณประกอบการตัดสินใจว่าท่านจะเชื่อแหล่งที่มาของโปรแกรมหรือไม่
2. สิ่งที่เปลี่ยนแปลง - เมื่อท่านติดตั้งและใช้โปรแกรมจะมีการติดตั้งไฟล์ใดลงบนเครื่องของท่านบ้างและจะมีการเปลี่ยนแปลงใดเกิดขึ้นกับเครื่องหรือระบบของท่านบ้าง ซึ่งท่านจะทราบได้จากการศึกษาจากเว็บของแหล่งที่มาของโปรแกรมหรือถามจากผู้เขียนโปรแกรม (อาจเป็นผู้บุกรุก) ในที่นี้ท่านก็จะต้องใช้วิจารณญาณประกอบการตัดสินใจว่าท่านจะเชื่อแหล่งที่มาของโปรแกรมหรือไม่
3. ผู้เขียน – ท่านควรหาข้อมูลว่าผู้เขียนโปรแกรมเป็นใคร และสามารถติดต่อผู้เขียนโปรแกรมได้อย่างไร เมื่อท่านทราบข้อมูลนี้แล้วท่านอาจพยายามติดต่อผู้เขียนเพื่อตรวจสอบความถูกต้องของข้อมูลซึ่งเป็นอีกวิธีหนึ่งที่ท่านจะสามารถประเมินความเชื่อถือของแหล่งที่มาของโปรแกรมได้
4. เรียนรู้ – ท่านสามารถเรียนรู้เกี่ยวกับโปรแกรมนี้จากผู้ใช้อื่นๆ ได้อย่างไรบ้าง โดยท่านอาจใช้โปรแกรมท่องเว็บของท่านสืบค้นข้อมูลเกี่ยวกับโปรแกรมนี้ได้

หากท่านไม่สามารถหาคำตอบที่ชัดเจนสำหรับข้อพิจารณาทั้ง 4 ข้อด้านบนได้ ท่านควรจะเพิ่มความระมัดระวังและความสงสัยเกี่ยวกับตัวโปรแกรมให้มากขึ้นและตัดสินใจอย่างดีที่สุดเท่าที่ข้อมูลจะอำนวย แต่ไม่ว่าจะอย่างไรก็ตามท่านควรที่จะเตรียมพร้อมที่จะติดตั้งระบบของท่านใหม่ทั้งหมดเสมอในกรณีที่โปรแกรมที่ท่านดาวน์โหลดมาทำลายระบบเก่าของท่าน รายละเอียดการเตรียมพร้อมในส่วนนี้อยู่ในข้อปฏิบัติที่ 5 – สำรองไฟล์ที่สำคัญ

ตามปกติแล้วโปรแกรมป้องกันไวรัสของท่านจะสามารถป้องกันปัญหาบางปัญหาที่อาจเกิดขึ้นจากการดาวน์โหลดและติดตั้งโปรแกรม แต่ท่านก็ควรระลึกอยู่เสมอว่ามักจะมีช่วงเวลาระหว่างการเกิดของไวรัสและการหาวิธีแก้ไวรัสได้ที่เครื่องของท่านอาจถูกโจมตีได้ และถึงแม้โปรแกรมที่ท่านดาวน์โหลดมาจะไม่มีไวรัสแต่โปรแกรมนั้นอาจมีลักษณะการทำงานที่ก่อให้เกิดความเสียหายได้ ดังนั้นท่านควรจะค้นคว้าหาข้อมูลให้ได้มากที่สุดและใช้ความระมัดระวังเมื่อดาวน์โหลด ติดตั้งและใช้โปรแกรมใหม่ๆ

ข้อปฏิบัติที่ 8 – ติดตั้งและใช้ไฟร์วอลที่เป็นฮาร์ดแวร์

เสริมความแข็งแรงของโปรแกรมไฟร์วอล (ที่เป็นซอฟท์แวร์) ของท่านด้วยการติดตั้งไฟร์วอลที่เป็นฮาร์ดแวร์ ไฟร์วอลทั้งสองชนิดนี้จะอยู่ระหว่างเครื่องคอมพิวเตอร์ของท่านและเครือข่ายอินเทอร์เน็ตและจะสามารถป้องกันเครื่องของท่านจากผู้บุกรุก โดยการใช้ไฟร์วอลนี้ถือได้ว่าเป็นการลงทุนที่คุ้มค่าอีกอย่างหนึ่ง

ในข้อปฏิบัติที่ 4 – ติดตั้งและใช้โปรแกรมไฟร์วอล จะมีรายละเอียดเกี่ยวกับไฟร์วอลอยู่ ซึ่งรายละเอียดเหล่านั้นจะเน้นไปทางโปรแกรมไฟร์วอลแต่ก็สามารถนำมาใช้กับไฟร์วอลที่เป็นฮาร์ดแวร์ได้ด้วยเช่นกัน ท่านสามารถสืบค้นในเว็บเพื่อหารายละเอียดเกี่ยวกับไฟร์วอลที่เป็นฮาร์ดแวร์ได้

ข้อปฏิบัติที่ 9 – ติดตั้งและใช้โปรแกรมเข้ารหัสไฟล์และการควบคุมการเข้าถึง

เราจะกลับไปใช้การเปรียบเทียบที่ว่าเครื่องคอมพิวเตอร์เปรียบเสมือนบ้านอีกครั้งหนึ่ง โดยหากเรานึกถึงเอกสารสำคัญที่เราเก็บไว้ในบ้าน เช่น ทะเบียนบ้าน กรมธรรม์ประกันภัย หรือ หนังสือเดินทาง ตามปกติแล้วเราจะเก็บเอกสารเหล่านี้ไว้ในตู้เอกสารหรือตู้นิรภัยที่สามารถล็อคได้แน่นหนาและเราสามารถตรวจสอบได้ตลอดเวลา

การปฏิบัติดังที่กล่าวมานั้นเป็นการทำให้เกิดความปลอดภัยขึ้นในส่วนหนึ่งของสามส่วนของความปลอดภัยของข้อมูล ซึ่งก็คือในส่วนของความลับ (confidentiality) ซึ่งความลับนี้คือการที่สิ่งที่ไม่ควรได้รับการเปิดเผยไม่ได้รับการเปิดเผย ผู้ที่เหมาะสมหรือได้รับอนุญาตเท่านั้นที่จะสามารถเข้าถึง

ข้อมูลที่เป็นความลับได้ ซึ่งตามที่กล่าวข้างต้นนั้นเราเก็บเอกสารที่สำคัญของเราไว้ในที่ที่เข้าถึงได้เฉพาะตัวเราเองเท่านั้น ดังนั้นจึงเก็บไว้เป็นความลับได้ นอกจากนี้ส่วนประกอบอีกสองส่วนของความปลอดภัยในข้อมูลก็คือ ความสมบูรณ์-Integrity (ข้อมูลที่เรามีอยู่นั้นถูกต้องสมบูรณ์และไม่ได้ถูกเปลี่ยนแปลงโดยไม่ได้รับอนุญาต) และความพร้อมใช้งาน-Availibility (เราสามารถเข้าไปตรวจสอบหรือใช้ข้อมูลที่เรามีอยู่เมื่อใดก็ตามที่เราต้องการ)

ท่านสามารถเสริมการปกป้องความลับของข้อมูลของท่านได้โดยการใช้อุปกรณ์ควบคุมการเข้าถึง (access control device) เช่นการใช้กุญแจล็อคตู้เอกสารหรือการล็อคตู้นิรภัยของท่าน อุปกรณ์นี้จะอยู่ระหว่างตัวข้อมูลและผู้ที่ต้องการจะเข้าถึงข้อมูลนั้น อุปกรณ์นี้จะอนุญาตให้ผู้ที่มีกุญแจ รหัสกุญแจ หรือเครื่องมือที่ใช้เปิดล็อคได้ สามารถเข้าถึงข้อมูลได้ ในบางกรณีจะมีการใช้อุปกรณ์ควบคุมการเข้าถึงหลายๆ ชั้น (เรียกว่า “การป้องกันทางลึก”) โดยท่านอาจจะเก็บตู้เอกสารหรือตู้นิรภัยไว้ในห้องที่มีการล็อคประตูอีกชั้นหนึ่ง ผู้ที่ต้องการจะบุกรุกจะต้องผ่านการป้องกันหลายชั้นก่อนที่จะสามารถเข้าถึงข้อมูลที่ตนต้องการได้

เมื่อเปรียบเทียบกับเครื่องคอมพิวเตอร์ของท่านแล้ว สิ่งที่ท่านจะต้องทำคือ มีวิธีการในการควบคุมการเข้าถึงไฟล์ต่างๆ ซึ่งเรียกกันว่า access control list – ACL วิธีการควบคุมการเข้าถึงจะกำหนดว่าใครสามารถทำอะไรกับไฟล์ใดได้ เช่น การอ่านและเปลี่ยนแปลงไฟล์เป็นต้น วิธีการนี้เปรียบเสมือนตู้ใช้เก็บเอกสารที่ได้รับการล็อคกุญแจไว้

คอมพิวเตอร์ระบบต่างๆ ก็จะมีวิธีการควบคุมการเข้าถึงในรูปแบบที่แตกต่างกัน บางระบบจะมีวิธีการควบคุมการเข้าถึงที่มีรายละเอียดมากโดยสามารถปรับค่าได้มากมาย บางระบบก็จะมีวิธีการควบคุมที่ปรับแต่งได้น้อยหรือแทบไม่ได้เลย แต่อย่างไรก็ตามท่านควรจะใช้การควบคุมการเข้าถึงทั้งหมดที่มีอยู่บนเครื่องคอมพิวเตอร์ของท่าน

โดยทั่วไปแล้วผู้ขายจะกำหนดการควบคุมการเข้าถึงมาให้ในระดับหนึ่งก่อน ซึ่งจะเป็นการกำหนดค่าที่อ่อนเกินไป (คือยอมให้แทบทุกคนสามารถเข้าถึงได้) ซึ่งจะมีผลดีที่ทำให้ระบบใช้ได้ง่าย แต่สิ่งที่ท่านควรทำคือ ปรับแต่งค่าเพื่อควบคุมการเข้าถึงให้เหมาะสม โดยให้ผู้ที่ได้รับอนุญาตเท่านั้นสามารถเข้าถึงระบบได้ ซึ่งจะได้มีการกล่าวถึงเรื่องนี้ในรายละเอียดต่อไป

กลับไปสู่การเปรียบเทียบคอมพิวเตอร์กับบ้านอีกครั้ง ในบางกรณีเมื่อผู้ใหญ่ต้องการจะปรึกษากันโดยไม่ต้องการให้เด็กได้ทราบความหมายแต่ไม่ต้องการหรือไม่สามารถที่จะไปปรึกษากันในที่ลับ ผู้ใหญ่ก็อาจจะพูดโดยใช้รหัสบางอย่างที่เป็นที่รู้กันเอง โดยที่เด็กได้ยินแต่ไม่เข้าใจ การกระทำเช่นนี้จะได้ผลในช่วงระยะเวลาหนึ่งจนกระทั่งเด็กโตขึ้นและอาจเรียนรู้รหัสนี้

เช่นเดียวกับการส่งข้อมูลผ่านทางเครือข่ายอินเทอร์เน็ตที่เป็นการส่งข้อมูลไปแบบเปิดเผยสามารถเห็นได้ ซึ่งผู้ใดก็ตามที่อยู่ในที่ข้อมูลนั้นผ่านไปสามารถดักดูข้อมูลนั้นได้ การปกปิดข้อมูลสำหรับการสื่อสารบางประเภทเช่นการซื้อขายสินค้าผ่านทางอินเทอร์เน็ตนั้นกระทำโดยการใช้กระบวนการทางคณิตศาสตร์มาเข้ารหัสข้อมูลนั้น การเข้ารหัสนี้แปลงข้อมูลที่เป็นตัวอักษรธรรมดาที่ใครก็อ่านได้ (readable text) ให้เป็นข้อมูลที่ถูกเข้ารหัสแล้ว (encrypted text) วัตถุประสงค์ในการนี้ก็คือเพื่อซ่อนข้อมูลจากผู้ที่ไม่ทราบวิธีการแปลงข้อมูลหรือไม่มีสิ่งที่นำมาแปลงข้อมูลกลับเป็นตัวอักษรธรรมดา (มักเรียกว่ากุญแจถอดรหัส) ข้อมูลที่ถูกเข้ารหัสจะเป็นตัวอักษรที่ยุ่งเหยิงและผู้ที่ไม่ทราบวิธีหรือผู้ที่ไม่มีกุญแจถอดรหัสจะไม่สามารถอ่านเข้าใจได้

กลับไปพิจารณาการสนทนาระหว่างผู้ใหญ่ในบ้าน เมื่อเด็กโตขึ้นและเรียนรู้วิธีการพูดแบบ “เข้ารหัส” ก็จะสามารถเข้าใจบทสนทนาของผู้ใหญ่ได้หากมีการสนทนาเกิดขึ้นในขณะนั้น ส่วนบทสนทนาที่เกิดขึ้นในอดีตนั้นเราจะถือว่าเด็กไม่ได้เข้าใจในขณะเกิดการสนทนาและข้อมูลในอดีตไม่มีความสำคัญหรือไม่เป็นที่น่าสนใจอีกต่อไป ดังนั้นเราจะถือว่าการเข้ารหัสของผู้ใหญ่นี้มีความแข็งแรงพอที่จะปกป้องความลับในช่วงระยะเวลาหนึ่งซึ่งเรียกว่าเป็นอายุการใช้งานของวิธีการเข้ารหัสนี้

การเข้ารหัสข้อมูลในคอมพิวเตอร์นั้นจะต้องแข็งแรงพอภายในอายุการใช้งานด้วย ยกตัวอย่างเช่นหากมีการเข้ารหัสหมายเลขบัตรเครดิตโดยใช้วิธีการเข้ารหัสวิธีหนึ่ง โดยบัตรเครดิตนี้มีกำหนดหมดอายุภายใน 5 ปี แต่ผู้บุกรุกสามารถใช้เครื่องคอมพิวเตอร์มาคำนวณทางคณิตศาสตร์เพื่อถอดรหัสนี้ได้โดยใช้เวลาเพียง 6 เดือน ผู้บุกรุกจะสามารถนำเอาข้อมูลหมายเลขบัตรเครดิตไปใช้ประโยชน์ได้ ดังนั้นในที่นี้เราจะถือว่าวิธีการเข้ารหัสนี้ไม่มีความแข็งแรงเพียงพอที่จะปกป้องความลับภายในอายุการใช้งาน

สิ่งที่ท่านควรปฏิบัติคือปรับแต่งการควบคุมการเข้าถึงข้อมูลในเครื่องคอมพิวเตอร์ของท่านให้เหมาะสมกับสภาพแวดล้อมในการปฏิบัติงานของท่าน โดยอนุญาตให้ผู้ใช้เข้าถึงไฟล์ที่ตนเองจำเป็นต้องใช้เท่านั้นและไม่สามารถเข้าถึงไฟล์อื่นๆ ได้ โดยท่านควรใช้ข้อพิจารณาดังนี้

1. ใคร – ผู้ใช้ใดบ้างที่มีความจำเป็นต้องเข้าถึงไฟล์ต่างๆ
2. การเข้าถึง – ผู้ใช้เหล่านั้นต้องการเข้าถึงในระดับใด เช่น อ่าน หรือ เขียน
3. ไฟล์ – ไฟล์ใดที่จำเป็นต้องมีการกำหนดการเข้าถึงเป็นพิเศษ โดยท่านควรกำหนดให้มีการเข้าถึงไฟล์ได้โดยตัวท่านเองเท่านั้นก่อน แล้วจึงกำหนดการเข้าถึงเป็นพิเศษสำหรับไฟล์บางไฟล์ที่ผู้ใช้อื่นจำเป็นจะต้องเข้าถึง (คล้ายกับการกำหนดกฎในไฟร์วอล)

เมื่อท่านใช้ข้อพิจารณา 3 ข้อข้างต้นท่านจะสามารถจำกัดการเข้าถึงไฟล์ในเครื่องคอมพิวเตอร์ของท่านให้เฉพาะผู้ที่จำเป็นจะต้องเข้าถึงเท่านั้น

การควบคุมการเข้าถึงให้เหมาะสมนั้นไม่ได้เป็นงานที่ง่าย ท่านอาจจะต้องปรับแต่งค่าที่ตั้งไว้หลายครั้งจนกระทั่งค่านั้นเหมาะสมกับสภาพแวดล้อมในการปฏิบัติงานของท่าน แต่เวลาที่เสียไปในการตั้งค่านี้จะคุ้มค่ากับความปลอดภัยที่เกิดขึ้น

สำหรับไฟล์สำคัญที่เป็นความลับและไฟล์ที่อยู่บนเครื่องโน้ตบุ๊คนั้น การควบคุมการเข้าถึงอย่างเดียวอาจจะไม่เพียงพอ ท่านอาจจะต้องใช้การเข้ารหัสเสริมด้วย

ระบบคอมพิวเตอร์บางระบบจะมาพร้อมกับระบบเข้ารหัสอยู่แล้ว ดังนั้นท่านสามารถทำตามคำแนะนำของผู้ขายเกี่ยวกับการเข้ารหัสได้ทันที ซึ่งหากระบบของท่านมีระบบเข้ารหัสอยู่แล้วท่านควรใช้การเข้ารหัสนั้น

สำหรับระบบคอมพิวเตอร์ที่ไม่ได้ให้ระบบการเข้ารหัสมาด้วยนั้นท่านจะต้องติดตั้งโปรแกรมเข้ารหัสเพิ่มเติมเข้าไป ซึ่งหากท่านดาวน์โหลดโปรแกรมเข้ารหัสจากเครือข่ายอินเทอร์เน็ตท่านควรปฏิบัติตามข้อปฏิบัติที่ 7 ด้วย (ใช้ความระมัดระวังเมื่อดาวน์โหลดและติดตั้งโปรแกรม) และสำหรับการกำหนดรหัสผ่านในโปรแกรมเข้ารหัส ท่านควรปฏิบัติตามข้อปฏิบัติที่ 6 (ใช้รหัสผ่านที่ยากต่อการเดา)

โปรแกรมเข้ารหัสนั้นมีอยู่ทั้งที่เป็นประเภทที่ท่านสามารถดาวน์โหลดมาใช้ได้ฟรีและที่ท่านจะต้องซื้อมาใช้ ซึ่งในกรณีส่วนใหญ่แล้วโปรแกรมฟรีก็เพียงพอสำหรับการใช้งานแล้ว โดยโปรแกรมที่ต้องซื้อนั้นโดยทั่วไปจะมีลักษณะการทำงานที่หลากหลายกว่าและอาจสามารถปรับปรุงตัวเองโดยใช้วิธีการเข้ารหัสใหม่ๆ ที่ยากต่อการเดากว่า อนึ่ง หากท่านปฏิบัติงานส่วนใหญ่โดยใช้เครื่องโน้ตบุ๊ค ท่านควรจะพิจารณาซื้อโปรแกรมเข้ารหัสมาใช้งาน

ท่านควรจะใช้การควบคุมการเข้าถึงเอกสารต่างๆ ของท่าน ไม่ว่าจะเป็นเอกสารที่เป็นกระดาษหรือเอกสารที่อยู่บนเครื่องคอมพิวเตอร์ สำหรับเอกสารบนเครื่องคอมพิวเตอร์ของท่านนั้นท่านควรใช้โปรแกรมเข้ารหัสเพื่อเสริมความปลอดภัยหรือเมื่อท่านเห็นว่าการควบคุมการเข้าถึงเพียงอย่างเดียวอาจไม่มีความปลอดภัยเพียงพอ

บทสรุป

จากการที่ท่านได้เติบโตจากเด็กเป็นผู้ใหญ่ท่านได้เรียนรู้วิธีรักษาความปลอดภัยของที่อยู่อาศัยโดยการสังเกตุจากผู้ใหญ่ การเรียนรู้นี้เป็นการเรียนรู้ทีละน้อยอย่างช้าๆ ซึ่งอาจจะช้าเสียจนท่านไม่ได้

ตระหนักว่าท่านกำลังเรียนรู้วิธีการเหล่านั้นอยู่ แต่เมื่อท่านโตเป็นผู้ใหญ่ท่านก็สามารถรักษาความปลอดภัยที่อยู่อาศัยของท่านได้ด้วยตัวเอง

แต่ในกรณีของการรักษาความปลอดภัยในเครื่องคอมพิวเตอร์นั้น ท่านไม่มีเวลาที่จะเรียนรู้ไปทีละน้อยเช่นดังท่านเรียนรู้วิธีรักษาความปลอดภัยของที่อยู่อาศัย ทั้งนี้เนื่องจากในขณะที่ท่านเชื่อมต่อเครื่องของท่านกับเครือข่ายอินเทอร์เน็ต เครื่องของท่านจะกลายเป็นเป้าหมายของผู้บุกรุกทันที ท่านจึงต้องมีความพร้อมในเรื่องความปลอดภัยตั้งแต่ต้น

สำหรับที่พักอาศัยของท่าน ท่านจะต้องใช้ทั้งเวลาและเงินในการที่จะซ่อมแซมและเปลี่ยนแปลงสิ่งต่างๆ ในที่พักอาศัย ท่านจะต้องใช้ทั้งเวลาและเงินในการที่จะปรับแต่งที่พักอาศัยให้เหมาะสมกับการใช้ชีวิตของท่านและทำให้ท่านและผู้พักอาศัยคนอื่นปลอดภัย ซึ่งท่านยอมรับในความรับผิดชอบนี้และยอมรับว่าเวลาและเงินที่เสียไปนั้นเป็นส่วนหนึ่งของค่าใช้จ่ายที่ท่านจะต้องเสียในฐานะเจ้าของที่พักอาศัย

ซึ่งเครื่องคอมพิวเตอร์ของท่านก็มีลักษณะคล้ายกัน ในขั้นแรก ท่านจะต้องจ่ายเงินเพื่อที่จะซื้อเครื่องคอมพิวเตอร์นั้นมา จากนั้นก็จะมีค่าใช้จ่ายเพิ่มเติมเพื่อปรับแต่งเครื่องและเพื่อให้ท่านและผู้ใช้เครื่องคนอื่นมีความปลอดภัยจากการใช้งานได้อย่างเพียงพอ ค่าใช้จ่ายเพิ่มเติมเหล่านี้เป็นความรับผิดชอบของท่านเช่นกันและเป็นส่วนหนึ่งของค่าใช้จ่ายที่ท่านจะต้องเสียในฐานะเป็นเจ้าของเครื่องคอมพิวเตอร์

หวังเป็นอย่างยิ่งว่าเอกสารนี้สามารถมีส่วนช่วยให้ท่านมองปัญหาที่เกิดขึ้นในการเป็นเจ้าของหรือผู้รับผิดชอบเครื่องคอมพิวเตอร์ได้ชัดเจนขึ้นและได้ทราบถึงการปฏิบัติต่างๆ ในการแก้ปัญหาเหล่านั้น ซึ่งจากการที่ท่านสละเวลาในการอ่านเอกสารนี้นั้น ผลตอบแทนที่ท่านได้รับคือท่านได้มีความรู้เพิ่มเติมในการที่จะทำให้เครื่องคอมพิวเตอร์ของท่านมีความปลอดภัยและทราบถึงค่าใช้จ่ายเพิ่มเติมที่ท่านจะต้องใช้ไปในการนี้ ขอแนะนำให้ท่านปฏิบัติตามคำแนะนำในเอกสารนี้ และโปรดแจกจ่ายหรือบอกต่อเอกสารนี้กับคนที่ท่านรู้จักเพื่อให้เครือข่ายอินเทอร์เน็ตในภาพรวมมีความปลอดภัยที่สูงขึ้น ซึ่งในที่สุดแล้วก็จะเป็นผลดีต่อผู้ใช้ทุกคนที่อยู่บนเครือข่ายนี้

รวมคำศัพท์ที่ใช้ในบทความ

คำศัพท์ภาษาไทย	*คำศัพท์ภาษาอังกฤษ*	คำอธิบาย
การค้าทางอิเล็กทรอนิกส์	***Electronic Commerce, E-Commerce***	การทำธุรกรรมบนเครือข่าย (on-line) ยกตัวอย่างเช่น การซื้อและขายของโดยใช้เงินแบบ “ดิจิตอล” บัตรเครดิต หรือ ระบบแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ (Electronic Data Interchange – EDI)
การเรียนรู้	***Heuristics***	วิธีการแก้ปัญหาโดยใช้การสำรวจแบบหนึ่งที่ใช้เทคนิคของการเรียนรู้ด้วยตัวเอง (โดยใช้การประเมินข้อมูลป้อนกลับหรือ feedback) เพื่อให้สามารถแก้ปัญหาได้อย่างมีประสิทธิภาพมากขึ้น
ข้อความฉับพลัน, ข้อความอิเล็กทรอนิกส์	***Instant Messaging***	บริการการสื่อสารแบบหนึ่งที่ท่านสามารถสร้างห้องสนทนาส่วนตัวเพื่อสนทนากับอีกคนหนึ่ง โดยทั่วไปแล้วระบบนี้จะแจ้งให้ท่านทราบเมื่อบุคคลที่อยู่ในรายชื่อคนรู้จักของท่านกำลังอยู่บนเครือข่าย ท่านก็จะสามารถเริ่มการสนทนากับบุคคลนั้นได้ มีระบบข้อความอิเล็กทรอนิกส์นี้อยู่หลายระบบที่แข่งขันกันอยู่ แต่ไม่ได้มีการกำหนดมาตรฐานใดๆ ดังนั้นบุคคลที่ท่านต้องการสนทนาด้วยจะต้องใช้ระบบข้อความอิเล็กทรอนิกส์ระบบเดียวกับท่าน
ข้อผิดพลาด	***Bug***	ความผิดพลาดหรือจุดด้อยที่อยู่ในซอฟท์แวร์หรือฮาร์ดแวร์ที่ทำให้โปรแกรมทำงานผิดพลาด โดยตามตำนานที่เล่าขานกันนั้น ข้อผิดพลาด (bug) แรกของคอมพิวเตอร์นั้นเกิดจากตัวแมลง (bug) จริงๆ โดยในปี ค.ศ.1945 ที่มหาวิทยาลัยฮาวาร์ดนั้นได้มีผีเสื้อกลางคืนเข้าไปติดอยู่ในวงจรของเครื่องคำนวณมาร์ค ทู ไอเคน (Mark II Aiken) ทำให้เครื่องหยุดทำงาน
การเข้ารหัส	***Encryption***	การแปลงข้อมูลให้อยู่ในรูปของรหัสลับ การเข้ารหัสเป็นวิธีที่ทำให้เกิดความปลอดภัยของข้อมูลที่ได้ผลที่สุด หากท่านต้องการอ่านไฟล์ที่ถูกเข้ารหัสไว้ ท่านจะต้องมีกุญแจลับหรือรหัสผ่านที่จะช่วยให้ท่านสามารถถอดรหัสไฟล์นั้นได้ เราเรียกข้อมูลที่ไม่ได้รับการเข้ารหัสว่าข้อความธรรมดา (plain text) ส่วนข้อมูลที่ได้รับการเข้ารหัสแล้ว เราเรียกว่าข้อความเข้ารหัสหรือข้อความปิดซ่อน (cipher text)
ความเสี่ยง	***Risk***	ความเป็นไปได้ของการสูญเสียหรือการบาดเจ็บ
เคเบิ้ล โมเด็ม	***Cable Modem***	โมเด็มที่ได้รับการออกแบบให้ทำงานกับสายเคเบิ้ลโทรทัศน์ เคเบิ้ลโมเด็มนั้นมีความเร็วสูงกว่าโมเด็มธรรมดาในการท่องเว็บมากเนื่องจากใช้สายเคเบิ้ลแบบร่วมแกน (coaxial) ที่มีความกว้างของช่องสัญญาณมากกว่าสายโทรศัพท์มาก

อย่างไรก็ตามมีปัญหาทางเทคนิคอยู่บ้าง กล่าวคือ โครงสร้างพื้นฐานของของระบบโทรทัศน์ผ่านสายเคเบิ้ลนั้นได้รับการออกแบบให้เป็นการส่งสัญญาณโทรทัศน์แบบทางเดียว คือจากบริษัทผู้ให้บริการไปสู่บ้านของผู้รับชม แต่ระบบอินเทอร์เน็ตนั้นเป็นการส่งข้อมูลสองทาง นอกจากนี้ยังไม่เป็นที่ทราบแน่ชัดว่าหากผู้ใช้เป็นจำนวนมากต้องการใช้เคเบิ้ลโมเด็มในการเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตแล้วระบบเคเบิ้ลจะสามารถรองรับการใช้งานเป็นจำนวนมากได้หรือไม่

ไปรษณีย์อิเล็กทรอนิกส์, อีเมล์ ***E-mail, Electronic Mail***

การส่งข้อความไปในเครือข่ายการสื่อสาร ข้อความนี้อาจเป็นข้อความที่ใช้แป้นพิมพ์พิมพ์เข้าไป หรือเป็นไฟล์ที่เก็บอยู่บนดิสค์ เครือข่ายคอมพิวเตอร์ มินิคอมพิวเตอร์ และเมนเฟรมส่วนใหญ่จะมีระบบอีเมล์อยู่ ระบบอีเมล์บางระบบสามารถใช้ได้กับระบบหรือเครือข่ายคอมพิวเตอร์เพียงระบบหรือเครือข่ายเดียวเท่านั้น ส่วนอีเมล์บางระบบมีเกทเวย์ที่ทำให้ทำงานร่วมกับระบบหรือเครือข่ายอื่นได้ซึ่งจะทำให้ผู้ใช้สามารถส่งข้อความไปได้ทั่วโลก บริษัทที่ใช้เครื่องคอมพิวเตอร์เป็นหลักนั้นล้วนจะใช้ระบบอีเมล์เนื่องจากมีข้อดีที่ความเร็ว ความยืดหยุ่น และความน่าเชื่อถือของระบบนี้

ระบบอีเมล์ส่วนใหญ่จะมีโปรแกรมแก้ไขข้อความมาพร้อมกับระบบเพื่อให้ผู้ใช้สามารถสร้างข้อความขึ้นได้ แต่สำหรับระบบอีเมล์หลายๆ ระบบนั้นผู้ใช้สามารถใช้โปรแกรมสร้างข้อความใดๆ ก็ได้ ผู้ใช้สามารถส่งข้อความไปยังผู้รับได้โดยการระบุที่อยู่ของผู้รับ ผู้ส่งสามารถส่งข้อความไปยังผู้รับหลายคนได้ในเวลาเดียวกัน การกระทำเช่นนี้เรียกว่าการกระจายการส่งข้อมูล (broadcasting)

เมื่อข้อความถูกส่งไปถึงผู้รับ ข้อความจะไปอยู่ในตู้จดหมาย (mailbox) ของผู้รับ จนกระทั่งผู้รับนั้นมารับเอาข้อความนั้นไป ท่านอาจจะต้องตรวจสอบตู้จดหมายของท่านเป็นระยะๆ เพื่อดูว่าท่านได้รับอีเมล์หรือไม่ แต่ระบบหลายๆ ระบบก็จะสามารถเตือนท่านโดยอัตโนมัติเมื่อมีอีเมล์มาถึงท่าน หลังจากที่ท่านได้อ่านอีเมล์แล้วท่านอาจจะบันทึกเก็บไว้เป็นไฟล์ข้อความ (text file) ส่งต่อให้ผู้อื่น หรือลบทิ้งไป ท่านสามารถพิมพ์ข้อความออกมาโดยใช้เครื่องพิมพ์ได้ด้วย

ผู้ให้บริการเครือข่ายและผู้ให้บริการอินเทอร์เน็ตต่างๆ มีการให้บริการอีเมล์และส่วนใหญ่จะมีเกทเวย์ ดังนั้นท่านสามารถแลกเปลี่ยนอีเมล์กับผู้ใช้ในระบบอื่นได้

โดยทั่วไปแล้วการที่อีเมล์จะเดินทางจากผู้ส่งไปยังผู้รับนั้นจะใช้เวลาไม่กี่วินาทีหรือไม่กี่นาที ดังนั้นการสื่อสารแบบนี้จึงเป็นการสื่อสารที่มีประสิทธิภาพสูงโดยเฉพาะกับกลุ่มคนเนื่องจากท่านสามารถส่งข้อความไปให้ทุกๆ คนในกลุ่มได้พร้อมๆ กัน

		แม้ว่าระบบอีเมล์ต่างระบบจะใช้รูปแบบข้อความที่ไม่เหมือนกัน แต่ก็เริ่มจะมีมาตรฐานสำหรับรูปแบบข้อความเกิดขึ้นเพื่อให้ผู้ใช้ในทุกระบบสามารถแลกเปลี่ยนข้อความกันได้ มาตรฐานของข้อความที่ใช้กันบนเครื่องคอมพิวเตอร์ส่วนตัวคือ MAPI ส่วนองค์กรมาตรฐาน CCITT นั้นก็ได้กำหนดมาตรฐาน X.400 ขึ้นซึ่งเป็นความพยายามที่จะให้มีการใช้ข้อความที่เป็นมาตรฐานสากล แต่ทุกวันนี้มาตรฐานอย่างไม่เป็นทางการที่มีการยอมรับใช้กันทั่วไปคือมาตรฐานที่ใช้บนระบบอินเทอร์เน็ต เนื่องจากระบบอีเมล์ส่วนใหญ่นั้นจะมีเกทเวย์ที่ใช้เชื่อมต่อกับอินเทอร์เน็ต
การโจมตี	***Attack***	การกระทำที่กระทำโดยปรปักษ์ ผู้ไม่หวังดี ผู้โจมตี ที่กระทำกับผู้ที่อาจตกเป็นเหยื่อหรือถูกกระทำ
ช่องโหว่, จุดอ่อน	***Vulnerability***	ลักษณะหนึ่งหรือหลายลักษณะของระบบที่ยอมให้ปรปักษ์ ผู้บุกรุกทำให้ระบบอยู่ในสถานะที่ผู้รับผิดชอบระบบไม่ต้องการและทำให้เพิ่มความเสี่ยงที่ระบบจะปฏิบัติงานไม่ถูกต้อง ลักษณะหนึ่งหรือหลายลักษณะของระบบที่ไม่ยอมให้มีการกำหนดหรือรักษาความปลอดภัยที่เหมาะสมของระบบ โปรแกรมที่มีบัฟเฟอร์ที่อาจเกิดการล้นได้จากการที่ผู้บุกรุกส่งข้อมูลจำนวนมากเข้ามาก็ถือได้ว่าเป็นโปรแกรมที่มีช่องโหว่
การใช้กำลัง	***Brute Force***	การเขียนโปรแกรมที่ไม่ได้ใช้วิธีลัดใดๆ ช่วยในการเพิ่มประสิทธิภาพของโปรแกรมนั้น แต่ใช้พลังการคำนวณที่มีอยู่ในการลองหาคำตอบทุกคำตอบที่เป็นไปได้จนกระทั่งค้นพบคำตอบ ตัวอย่างหนึ่งที่มักใช้ในการอธิบายคำนี้กันคือการแก้ปัญหาการเดินทางของพนักงานขาย กล่าวคือ พนักงานขายคนหนึ่งจะต้องเดินทางไปใน 10 จังหวัดทั่วประเทศ ปัญหาคือจะต้องหาว่าพนักงานขายคนนี้ควรจะเดินทางไปยังจังหวัดใดก่อน/หลังเพื่อที่จะให้ระยะทางการเดินทางน้อยที่สุด การแก้ปัญหาโดยวิธีใช้กำลังนั้นจะคำนวณระยะทางรวมสำหรับทุกกรณีที่เป็นไปได้ของลำดับการเดินทางทั้งหมดแล้วจึงเลือกเอาลำดับการเดินทางที่ใช้ระยะทางน้อยที่สุด การคำนวณแบบนี้มีประสิทธิภาพไม่สูงนัก เนื่องจากหากมีการใช้กระบวนการที่มีความฉลาดขึ้นเราสามารถกำจัดลำดับการเดินทางบางลำดับได้โดยไม่ต้องคำนวณระยะทางรวมของลำดับนั้น ถึงแม้วิธีนี้จะไม่มีประสิทธิภาพมากนัก แต่ก็มีประโยชน์ในสาขาวิชาวิศวกรรมซอฟท์แวร์ เนื่องจากวิธีนี้จะให้คำตอบที่ถูกต้องเสมอ (แม้จะช้า) เราจึงสามารถใช้วิธีนี้ในการตรวจความถูกต้องของวิธีอื่นที่เร็วกว่าได้

ซีดี-รอม	***CD-ROM (Compact Disk – Read Only Memory)***	แผ่นดิสค์แบบลำแสงแบบหนึ่งที่สามารถเก็บข้อมูลได้เป็นจำนวนมาก โดยสามารถจุได้สูงสุดถึง 1 GB แต่ขนาดที่ใช้กันทั่วไปคือ 650 MB ซึ่งแผ่นซีดี-รอมที่ใช้กันทั่วไปนั้นมีความจุเทียบเท่ากับแผ่นฟล็อปปี้ดิสค์จำนวน 700 แผ่น ซึ่งเป็นหน่วยความจำที่สามารถเก็บเอกสารที่เป็นตัวอักษรได้ประมาณ 300,000 หน้า
การดมกลิ่น	***Sniffing***	โปรแกรมและ/หรืออุปกรณ์ที่ใช้เฝ้าดูข้อมูลที่เดินทางไปในเครือข่าย เครื่องดมกลิ่นหรือสนิฟเฟอร์ (sniffer) นี้สามารถใช้ได้ทั้งกับงานสุจริตในการบริหารเครือข่ายและกับงานทุจริตในการขโมยข้อมูลจากเครือข่าย การใช้สนิฟเฟอร์โดยไม่ได้รับอนุญาตนั้นถือว่าก่อให้เกิดอันตรายอย่างยิ่งกับความปลอดภัยของเครือข่ายเนื่องจากแทบจะเป็นไปไม่ได้ที่จะตรวจจับสนิฟเฟอร์ได้และสามารถใช้สนิฟเฟอร์ได้แทบจะทุกที่ในเครือข่ายใดๆ จึงทำให้สนิฟเฟอร์นั้นเป็นอาวุธยอดนิยมของเหล่าแฮ็คเกอร์
การดาวน์โหลด	***Download***	การสำเนาข้อมูล (โดยทั่วไปจะเป็นไฟล์ทั้งไฟล์) จากแหล่งแจกจ่ายหลักไปยังอุปกรณ์ข้างเคียง คำนี้มักใช้อธิบายการสำเนาไฟล์จากบริการที่อยู่บนเครือข่ายหรือจากบริการกระดานข่าว (bulletin board service – BBS) มายังเครื่องคอมพิวเตอร์ของผู้ใช้ นอกจากนี้การดาวน์โหลดยังหมายความถึงการสำเนาไฟล์จากไฟล์เซิร์ฟเวอร์ (file server) ไปยังเครื่องคอมพิวเตอร์ที่อยู่บนเครือข่าย
ดีเอสแอล โมเด็ม	***DSL (Digital Subscriber Lines) Modem***	หมายความรวมถึงระบบดีเอสแอลแบบต่างๆ โดยจะมีสองระบบหลักๆ คือ เอดีเอสแอล (ADSL) และ เอสดีเอสแอล (SDSL) ส่วนอีกสองระบบจะเป็นระบบดีเอสแอลความเร็วสูง (High-data-rate DSL – HDSL) และระบบดีเอสแอลความเร็วสูงมาก (Very-high-data-rate DSL – VDSL) เทคโนโลยีดีเอสแอลนั้นใช้วิธีการปรุงคลื่นที่ซับซ้อนในการบีบอัดข้อมูลลงในเส้นลวดทองแดง บางครั้งเราเรียกเทคโนโลยีนี้ว่าเทคโนโลยีกิโลเมตรสุดท้าย (last-mile technologies) เนื่องจากใช้ในการเชื่อมต่อระหว่างตู้สลับสายโทรศัพท์กับบ้านเรือนหรือสำนักงานและไม่ได้เป็นการเชื่อมต่อระหว่างตู้สลับสายด้วยกันเอง ระบบดีเอสแอลนั้นคล้ายกับระบบไอเอสดีเอ็นตรงที่ว่าเป็นระบบที่ใช้เส้นลวดทองแดงของเครือข่ายโทรศัพท์ดั้งเดิมเหมือนกัน และระยะทางไปยังสำนักงานโทรศัพท์กลางจะต้องไม่ไกลนัก (ควรจะน้อยกว่า 6,000 เมตร) แต่ระบบดีเอสแอลนั้นสามารถให้ความเร็วได้สูงกว่า คือ รับข้อมูลได้เร็วสูงสุดถึง 32 Mbps และส่งข้อมูลได้เร็วสูงสุดจาก 32kbps ถึงมากกว่า 1 Mbps
หน่วยประมวลผล	***Processor***	ชิปที่ทำจากซิลิกอนที่มีซีพียู (central processing unit – CPU) อยู่ข้างใน ในวงการเครื่องคอมพิวเตอร์ส่วนตัวนั้นคำว่าไมโครโปรเซสเซอร์และซีพียูนั้นมีความหมายเหมือนกัน ไมโครโปรเซสเซอร์

		นั้นถือว่าเป็นหัวใจของเครื่องคอมพิวเตอร์ส่วนตัวและเครื่องคอมพิวเตอร์ลูกข่ายส่วนใหญ่ นอกจากนี้ไมโครโปรเซสเซอร์ยังมีหน้าที่ในการควบคุมกระบวนการทางตรรกทั้งสิ้นของอุปกรณ์ดิจิตอลส่วนใหญ่ ตั้งแต่นาฬิกา ไปจนถึงระบบหัวฉีดน้ำมันของรถยนต์
ประตูลับ	***Backdoor, Trapdoor***	วิธีหนึ่ง (ที่ไม่เป็นทางการ) ที่ใช้ในการเข้าถึงโปรแกรม บริการบนเครือข่าย หรือระบบคอมพิวเตอร์ทั้งระบบ ประตูลับนี้ถูกสร้าง (เขียน) โดยผู้เขียนโปรแกรมนั้นๆ ซึ่งโดยทั่วไปจะมีเพียงผู้เขียนโปรแกรมเท่านั้นที่ทราบว่ามีประตูลับอยู่ ประตูลับถือว่าเป็นความเสี่ยงทางความปลอดภัยของระบบคอมพิวเตอร์
การปลอมแปลง	***Spoofing***	การใช้ข้อมูลการพิสูจน์ตัวตนและการตรวจสอบตัวจริงไปในทางที่ผิด ซึ่งโดยทั่วไปแล้วจะใช้ในการปลอมผู้โจมตีว่าเป็นผู้ใช้ที่ถูกต้อง ตัวอย่างเช่น การปลอมแปลงการส่งอีเมล์แทนเจ้าของอีเมล์ที่แท้จริง เป็นต้น คำศัพท์อื่นที่ใช้อาจมีดังนี้ impersonating, masquerading, piggybacking, และ mimicking
โปรแกรม	***Program***	ชุดของคำสั่งต่างๆที่เรียบเรียงไว้ซึ่งเมื่อได้รับการสั่งให้ทำงานจะทำให้เครื่องคอมพิวเตอร์ปฏิบัติงานตามที่ได้กำหนดไว้ เครื่องคอมพิวเตอร์จะไร้ประโยชน์หากไม่มีโปรแกรม เราสามารถมองโปรแกรมว่าเหมือนกับสูตรปรุงอาหาร โดยจะมีรายชื่อของส่วนผสมอยู่ (เราเรียกว่าตัวแปร) และมีขั้นตอนการทำ (เราเรียกว่า statement) ที่บอกคอมพิวเตอร์ว่าควรจะทำอย่างไรกับตัวแปร ตัวแปรนั้นอาจจะใช้ในการแสดงตัวเลข ข้อความ หรือรูปภาพก็ได้ มีภาษาโปรแกรมอยู่หลายภาษาด้วยกัน เช่น C, C++, ปาสคาล, เบสิค, ฟอร์แทรน, โคบอล และ ลิสป์ เป็นต้น ภาษาเหล่านี้เป็นภาษาขั้นสูง เราสามารถเขียนโปรแกรมโดยใช้ภาษาขั้นต่ำได้โดยใช้ภาษาแอสเซ็มบลี้ แต่จะยากกว่า ภาษาระดับต่ำนั้นมีความใกล้เคียงกับภาษาที่คอมพิวเตอร์ใช้มากกว่าภาษาขั้นสูงซึ่งมีความใกล้เคียงกับภาษาที่มนุษย์ใช้ ในที่สุดแล้วทุกโปรแกรมจะต้องถูกแปลงให้เป็นภาษาเครื่องที่เครื่องคอมพิวเตอร์สามารถเข้าใจได้ การแปลงนี้กระทำโดยคอมไพเลอร์ อินเทอร์พริตเตอร์ และเอสเซ็มเบลอ เมื่อท่านซื้อซอฟท์แวร์มา โดยทั่วไปแล้วท่านจะได้รับโปรแกรมที่ท่านสามารถสั่งให้ทำงานได้ทันที ซึ่งก็หมายความว่าตัวโปรแกรมนั้นเป็นภาษาเครื่องที่ได้รับการคอมไพล์และเอสเซ็มเบิลแล้ว และพร้อมทำงานได้ทันที

โปรแกรมอุดช่องโหว่	***Patch***	การแก้ไขข้อผิดพลาดของโปรแกรมแบบชั่วคราว โปรแกรมอุดช่องโหว่ที่แท้จริงแล้วก็คือออบเจ็กโค้ดที่ใส่แทรกเข้าไป (เข้าไปอุด) ในโปรแกรมที่ปกติทำงานอยู่
ผู้บุกรุก	***Intruder***	ปรปักษ์ ผู้ไม่หวังดี ที่กำลังกระทำ หรือได้กระทำการบุกรุกหรือโจมตีต่อเครื่อง ระบบ เครือข่าย หรือองค์กรที่เป็นเหยื่อหรือที่ถูกกระทำ ไม่มีคำจำกัดความที่แน่นอนสำหรับการกระทำที่ถือว่าเป็นการบุกรุกเนื่องจากการให้คำจำกัดความนั้นจะขึ้นอยู่กับเหยื่อหรือผู้ถูกบุกรุกในแต่ละรายซึ่งก็จะแตกต่างกันออกไป ซึ่งในมุมมองของผู้ถูกบุกรุกนั้นผู้บุกรุกมักจะเป็นบุคคลหรือองค์กรที่โจมตีผู้ถูกบุกรุกแล้วได้รับความสำเร็จ แต่ไม่มีความแน่ชัดว่าหากการโจมตีไม่ประสบความสำเร็จจะถือว่าเป็นการบุกรุกหรือไม่ หากเราจะถือว่าต้องเกิดการบุกรุกขึ้น (โจมตีสำเร็จ) จึงจะถือว่าผู้กระทำเป็นผู้บุกรุกดังนั้นผู้บุกรุกทุกคนก็จะเป็นผู้โจมตี แต่ผู้โจมตีไม่จำเป็นจะต้องเป็นผู้บุกรุก
พอร์ท	***Port***	เป็นช่องทางการสื่อสารบนระบบเครือข่าย ทั้งแบบ TCP/IP และ UDP เราใช้หมายเลขของพอร์ทในการกำหนดชนิดของพอร์ทนั้นๆ เช่น พอร์ทหมายเลข 80 เป็นพอร์ทสำหรับข้อมูล HTTP (ข้อมูลเว็บ)
แพ็คเก็ต	***Packet***	หน่วยของข้อความที่ใช้ส่งกันในระบบเครือข่าย ชนิดสลับแพ็คเก็ต (packet switching network) คุณลักษณะสำคัญประการหนึ่งของแพ็คเก็ตคือภายในแพ็คเก็ตนั้นนอกจากจะมีข้อมูลแล้วยังจะมีที่อยู่ของผู้รับอยู่ สำหรับเครือข่ายประเภท IP (อินเทอร์เน็ต) นั้นเราอาจเรียกแพ็คเก็ตว่า “ดาต้าแกรม”
ไฟร์วอล	***Firewall***	ระบบหนึ่งที่ได้รับการออกแบบมาเพื่อป้องกันการเข้าถึงเครือข่ายที่ไม่ได้รับอนุญาต ไฟร์วอลนั้นมีอยู่ทั้งแบบที่เป็นฮาร์ดแวร์และซอฟท์แวร์หรือทั้งสองแบบรวมกัน โดยทั่วไปแล้วไฟร์วอลจะถูกใช้ในการป้องกันมิให้ผู้ใช้จากเครือข่ายอินเทอร์เน็ตที่ไม่ได้รับอนุญาตสามารถเข้าถึงเครือข่ายส่วนบุคคลที่เชื่อมต่ออยู่กับเครือข่ายอินเทอร์เน็ตโดยเฉพาะอย่างยิ่งเครือข่ายอินทราเน็ท ข้อมูลทั้งหมดที่เข้าสู่หรือออกจากเครือข่ายอินทราเน็ทจะต้องผ่านไฟร์วอล ซึ่งไฟร์วอลจะตรวจสอบข้อมูลทั้งหมดและหากข้อมูลใดไม่ผ่านเกณฑ์การรักษาความปลอดภัยไฟร์วอลก็จะไม่อนุญาตให้ผ่านไป ไฟร์วอลมีอยู่หลายชนิดด้วยกัน กล่าวคือ • ไฟร์วอลแบบกรองแพ็คเก็ต (packet filter) - ไฟร์วอลจะตรวจสอบแพ็คเก็ตแต่ละแพ็คเก็ตที่เข้าสู่และออกจากเครือข่าย และใช้กฎที่ผู้ใช้ตั้งขึ้นเป็นเกณฑ์พิจารณาในการอนุญาตแพ็คเก็ตนั้นๆ วิธีนี้ค่อนข้างได้ผล แต่การตั้งค่าไฟร์วอลกระทำได้ยากและซับซ้อน นอกจากนี้วิธีนี้อ่อนแอต่อการโจมตีแบบปลอมแปลงหมายเลข IP (IP spoofing)

- ไฟร์วอลแบบกรองโปรแกรม (application gateway) - ไฟร์วอลจะใช้มาตรการรักษาความปลอดภัยกับโปรแกรมแต่ละโปรแกรมโดยเฉพาะไป เช่น เทลเน็ต หรือ เอฟทีพี เซิร์ฟเวอร์ วิธีนี้มีประสิทธิผลสูงแต่อาจทำให้ประสิทธิภาพในการสื่อสารต่ำลง
- ไฟร์วอลแบบกรองวงจร (circuit-level gateway) – ไฟร์วอลจะใช้มาตรการรักษาความปลอดภัยขณะที่กำลังมีการจัดตั้งการเชื่อมต่อแบบ TCP หรือ UDP ซึ่งเมื่อจัดตั้งเรียบร้อยแล้วแพ็คเก็ตจะสามารถเดินทางได้โดยไม่ต้องได้รับการตรวจสอบอีก
- ไฟร์วอลแบบพร็อกซี่เซิร์ฟเวอร์ (proxy server) – จะตรวจจับแพ็คเก็ตทั้งหมดที่เข้าสู่และออกจากเครือข่ายและสร้างแพ็คเก็ตใหม่ขึ้น ถือได้ว่าพร็อกซี่เซิร์ฟเวอร์นั้นซ่อนที่อยู่ที่แท้จริงของเครือข่ายไว้

ในทางปฏิบัติแล้ว ไฟร์วอลโดยมากจะใช้หลายวิธีดังกล่าวด้านบนผสมกัน

เราถือว่าไฟร์วอลเป็นแนวป้องกันแนวแรกในการปกป้องข้อมูลส่วนบุคคล เราสามารถเสริมความปลอดภัยให้สูงยิ่งขึ้นโดยการเข้ารหัสข้อมูล

ไฟล์ ***File*** ข้อมูลกลุ่มหนึ่งที่อยู่รวมกันแล้วมีชื่อเรียกเป็นชื่อไฟล์ (filename) ข้อมูลเกือบทั้งหมดที่อยู่ในเครื่องคอมพิวเตอร์จะต้องอยู่ในรูปของไฟล์ ไฟล์นั้นมีอยู่หลายชนิดด้วยกัน เช่น ไฟล์ข้อมูล (data file) ไฟล์ข้อความ (text file) ไฟล์โปรแกรม (program file) และ ไฟล์รายชื่อ (directory file) เป็นต้น ไฟล์ต่างชนิดกันจะเก็บข้อมูลต่างชนิดกัน ยกตัวอย่างเช่น ไฟล์โปรแกรมจะมีตัวโปรแกรมอยู่ส่วนไฟล์ข้อความก็จะบรรจุข้อความ

รหัสผ่าน ***Password*** กลุ่มตัวอักษรลับที่ผู้ใช้ใช้ในการเข้าถึงไฟล์ คอมพิวเตอร์ หรือโปรแกรม สำหรับระบบที่มีผู้ใช้หลายคน ผู้ใช้จะต้องระบุรหัสผ่านของตัวเองก่อนที่เครื่องคอมพิวเตอร์จะยอมทำตามคำสั่งของผู้ใช้นั้น การให้รหัสผ่านนั้นช่วยให้มั่นใจได้ว่าผู้ใช้ที่ไม่ได้รับอนุญาตจะไม่สามารถเข้าถึงเครื่องคอมพิวเตอร์ได้ นอกจากนี้เราอาจต้องใช้รหัสผ่านในการเข้าถึงไฟล์ข้อมูลบางไฟล์และโปรแกรมบางโปรแกรม

รหัสผ่านตามอุดมคตินั้นควรจะเป็นสิ่งที่ไม่มีใครเดาได้ถูก แต่โดยทั่วไปแล้วคนส่วนใหญ่จะเลือกรหัสผ่านที่ง่ายต่อการจำเช่นชื่อหรือชื่อเล่นของตัวเอง ซึ่งก็เป็นเหตุผลหนึ่งที่ทำให้การเจาะเข้าสู่ระบบคอมพิวเตอร์ส่วนใหญ่นั้นทำได้ง่าย

ระบบปฏิบัติการ ***Operating System***

เป็นโปรแกรมที่สำคัญที่สุดในเครื่องคอมพิวเตอร์ โดยเครื่องคอมพิวเตอร์อเนกประสงค์ทุกเครื่องจะต้องมีระบบปฏิบัติการทำงานอยู่เพื่อควบคุมการทำงานของโปรแกรมอื่นในระบบ ระบบปฏิบัติการจะทำงานพื้นฐานต่างๆ เช่น รับข้อมูลที่ป้อนเข้าจากแป้นพิมพ์ ส่งข้อมูลออกไปแสดงผลบนจอภาพ สร้างระบบจัดเก็บไฟล์และรายชื่อไฟล์ลงบนดิสค์ และควบคุมอุปกรณ์ข้างเคียงต่างๆ เช่น ดิสค์ไดร์ฟ และเครื่องพิมพ์

เราสามารถแบ่งประเภทของระบบปฏิบัติการออกได้เป็นหลายประเภทด้วยกันคือ

- แบบผู้ใช้หลายคน (multi-user) – ยอมให้ผู้ใช้สองคนหรือมากกว่าสั่งใช้โปรแกรมได้พร้อมกัน ระบบปฏิบัติการบางระบบสามารถรองรับผู้ใช้ได้พร้อมกันถึงเป็นพันคน
- แบบหน่วยประมวลผลหลายหน่วย (multiprocessing) – สามารถให้โปรแกรมทำงานโดยใช้หน่วยประมวลผลหลายตัวได้
- แบบหลายหน้าที่ (multitasking) – ยอมให้โปรแกรมมากกว่าหนึ่งโปรแกรมสามารถทำงานพร้อมกันได้
- แบบหลายส่วน (multithreading) – ยอมให้หลายส่วนในโปรแกรมเดียวกันสามารถทำงานพร้อมกันได้
- แบบเวลาจริง (real time) – ปฏิบัติตามคำสั่งในทันที ซึ่งระบบปฏิบัติการอเนกประสงค์ต่างๆ เช่น ดอส และ ยูนิกซ์ นั้นไม่ใช่ระบบปฏิบัติการแบบเวลาจริง

บนตัวระบบปฏิบัติการนั้นจะให้โปรแกรมอื่นเข้ามาทำงานได้ เราเรียกโปรแกรมเหล่านั้นว่าโปรแกรมประยุกต์ (application programs) ซึ่งโปรแกรมใช้งานเหล่านี้จะต้องถูกเขียนมาให้ทำงานกับระบบปฏิบัติการระบบใดระบบหนึ่งโดยเฉพาะ ดังนั้นระบบปฏิบัติการที่ท่านเลือกใช้จะเป็นตัวกำหนดว่าท่านจะสามารถใช้โปรแกรมประยุกต์ใดได้บ้าง ระบบปฏิบัติการสำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่เป็นที่นิยมมากที่สุดได้แก่ ดอส โอเอสทู และ วินโดวส์ แต่ก็มีระบบปฏิบัติการอื่นๆ อีก เช่น ลินุกซ์

ในส่วนของผู้ใช้จะติดต่อทำงานกับระบบปฏิบัติการโดยใช้คำสั่ง (command) ต่างๆ ยกตัวอย่างเช่น สำหรับระบบปฏิบัติการดอสจะมีคำสั่งเช่น COPY และ RENAME เพื่อใช้สำหรับการสำเนาและเปลี่ยนชื่อไฟล์ ตามลำดับ ซึ่งระบบปฏิบัติการในส่วนของตัวประมวลคำสั่ง (command processor) หรือตัวแปลคำสั่ง (command line interpreter) จะเป็นตัวรับคำสั่งและทำงานตามคำสั่งนั้น บางระบบปฏิบัติการจะมีส่วนที่เป็นรูปภาพให้ผู้ใช้ได้ชี้ที่ภาพแล้วกดปุ่มเพื่อเป็นการสั่งให้ระบบปฏิบัติการทำงาน เราเรียกส่วนนี้ว่าส่วนเชื่อมต่อกับผู้ใช้โดยใช้รูปภาพ (graphical user interface – GUI)

ลายมือของไวรัส	***Virus Signature***	บิทหรือตัวเลขฐานสองชุดหนึ่งที่เป็นเอกลักษณ์ของไวรัส ลายมือไวรัสนั้นก็เหมือนกับลายนิ้วมือของคนที่สามารถนำมาใช้ตรวจจับและพิสูจน์ทราบไวรัสตัวหนึ่งๆ ได้ โปรแกรมป้องกันไวรัสใช้ลายมือไวรัสในการตรวจหาโค้ดที่มีลักษณะพึงประสงค์ร้าย
วิศวกรรมทางสังคม	***Social Engineering***	การวิศวกรรมทางสังคมนั้นเป็นทั้งศิลป์และศาสตร์ในการที่จะชักจูงหรือหลอกล่อให้ผู้ใดผู้หนึ่งทำในสิ่งที่เราต้องการ แต่วิธีนี้ไม่เกี่ยวกับการสะกดจิตและไม่สามารถทำให้คนผู้นั้นทำอะไรที่ผิดแปลกไปจากวิสัยปกติอย่างมากมาย วิธีนี้ไม่จำเป็นจะต้องได้ผลเสมอไป
ไวรัส	***Virus***	โปรแกรมหรือโค้ดที่ถูกส่งมาที่เครื่องคอมพิวเตอร์ของท่านโดยที่ท่านไม่ทราบแล้วทำงานในลักษณะที่ท่านไม่ต้องการ ไวรัสนั้นยังสามารถแบ่งตัวเองได้ด้วย ไวรัสในเครื่องคอมพิวเตอร์ทั้งหมดล้วนถูกสร้างขึ้นมาโดยมนุษย์ เป็นการง่ายมากที่จะสร้างไวรัสแบบที่ไม่ซับซ้อนที่แบ่งตัวเองออกไปเรื่อยๆ ซึ่งแม้แต่ไวรัสธรรมดาเช่นนี้ก็มีอันตรายเนื่องจากมันจะใช้หน่วยความจำของระบบจนหมดทำให้ระบบหยุดทำงาน ไวรัสชนิดที่อันตรายกว่านี้คือไวรัสที่สามารถแบ่งตัวเอง เจาะผ่านระบบรักษาความปลอดภัยและส่งตัวเองข้ามเครือข่ายให้ไปติดเครื่องอื่นๆ
การทำสำรอง	***Backup***	การสำเนาไฟล์หรือโปรแกรมเพื่อไว้ใช้ในการเรียกคืนหากเกิดการเสียหายหรือสูญหาย
สื่อ	***Media***	สิ่งที่สามารถใช้เก็บข้อมูลได้ รวมถึง ฮาร์ดดิสค์ ฟล็อปปี้ดิสค์ ซีดี-รอม และแถบแม่เหล็ก
หนอน	***Worm***	โปรแกรมหรือชุดคำสั่งที่สำเนาตัวเองและส่งตัวเองออกไปทั่วเครือข่ายและโดยมากจะทำกิจกรรมที่มีวัตถุประสงค์อันมิชอบ เช่นใช้ทรัพยากรของเครื่องคอมพิวเตอร์จนกระทั่งอาจทำให้เครื่องต้องหยุดทำงาน (อ่านเพิ่มเติมที่ “ไวรัส”)
อาร์พาเน็ต	***ARPAnet***	ต้นตระกูลของอินเทอร์เน็ต อาร์พาเน็ตเป็นเครือข่ายขนาดใหญ่ (wide area network) ที่หน่วยงานโครงการวิจัยขั้นสูงกระทรวงกลาโหม สหรัฐอเมริกา (United States Defense Advanced Research Project Agency – ARPA) สร้างขึ้นในปี ค.ศ.1969 อาร์พาเน็ตถูกใช้เป็นสนามทดลองสำหรับเทคโนโลยีใหม่ๆ ทางเครือข่าย และเชื่อมต่อมหาวิทยาลัยและศูนย์วิจัยต่างๆ เข้าด้วยกัน จุดเชื่อมต่อสองจุดแรกของเครือข่ายนี้คือการเชื่อมต่อระหว่างมหาวิทยาลัยแคลิฟอร์เนียที่ลอสแองเจลิสกับสถาบันวิจัยสแตนฟอร์ดซึ่งหลังจากนั้นไม่นานก็ตามมาด้วยการเชื่อมต่อกับมหาวิทยาลัยยูท่าห์
อินเทอร์เน็ต	***Internet***	เครือข่ายที่โยงใยไปทั่วโลกเชื่อมต่อเครื่องคอมพิวเตอร์นับล้าน

เครื่องจากประเทศต่างๆ กว่า 100 ประเทศเข้าด้วยกันเพื่อแลกเปลี่ยนข้อมูล ข่าวสาร และความเห็น

อินเทอร์เน็ตนั้นแตกต่างจากบริการเครือข่ายอื่นๆ ที่มีการควบคุมจากศูนย์กลาง อินเทอร์เน็ตนั้นได้รับการออกแบบให้มีลักษณะกระจาย เครื่องคอมพิวเตอร์ในอินเทอร์เน็ตแต่ละเครื่องนั้นเรียกว่า โฮ้ส (host) จะเป็นอิสระต่อกัน ผู้รับผิดชอบโฮ้สนั้นจะตัดสินใจว่าจะเปิดบริการใดให้กับเครื่องอื่นในอินเทอร์เน็ตและจะออกไปใช้บริการใดที่มีอยู่ในอินเทอร์เน็ต การออกแบบในลักษณะนี้ทำงานได้ผลอย่างน่าทึ่ง

การเข้าถึงหรือเชื่อมต่อกับอินเทอร์เน็ตนั้นสามารถทำได้หลายวิธี บริการเครือข่าย (เช่น America Online ในสหรัฐอเมริกา) ส่วนใหญ่จะให้บริการในการเชื่อมต่อกับอินเทอร์เน็ตด้วย นอกจากนี้ยังมีผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider – ISP) ที่ให้บริการการเชื่อมต่อกับอินเทอร์เน็ตโดยเฉพาะ

ฮาร์ดดิสค์ ***Harddisk***

แผ่นแม่เหล็กที่สามารถนำข้อมูลคอมพิวเตอร์มาบรรจุไว้ได้ คำว่า “ฮาร์ด” หรือแข็งนั้นถูกนำมาใช้เพื่อให้เกิดความแตกต่างจาก “ซอฟท์” หรือ “ฟล็อปปี้” ที่แปลว่าอ่อน เนื่องจากฮาร์ดดิสค์สามารถจุข้อมูลได้มากกว่าและมีความเร็วสูงกว่าฟล็อปปี้ดิสค์ โดยฮาร์ดดิสค์ตัวหนึ่งนั้นอาจเก็บข้อมูลได้ตั้งแต่ 10 MB ถึงหลาย GB ส่วนฟล็อปปี้ดิสค์นั้นมีความจุสูงสุดได้เพียง 1.4 MB

ฮาร์ดดิสค์ตัวหนึ่งนั้นโดยทั่วไปจะมีแผ่นแม่เหล็กอยู่หลายแผ่น ซึ่งสำหรับแต่ละแผ่นจะต้องมีหัวอ่าน/เขียนสองหัว โดยจะมีหัวอ่าน/เขียนหน้าละหนึ่งหัว หัวอ่าน/เขียนทั้งหมดจะถูกเชื่อมกันด้วยแขนกล ดังนั้นแต่ละหัวจะไม่เป็นอิสระต่อกัน แผ่นดิสค์แต่ละแผ่นจะมีจำนวนร่องหรือแทร็ค (track) เท่ากัน แทร็คแต่ละแทร็คที่อยู่ตรงกันในแผ่นดิสค์ทั้งหมดจะถูกเรียกว่ากระบอกหรือไซลินเดอร์ (cylinder) ยกตัวอย่างเช่นฮาร์ดดิสค์ของเครื่องคอมพิวเตอร์ส่วนบุคคลที่มีความจุ 83 MB อาจจะมีแผ่นแม่เหล็กสองแผ่น (สี่หน้า) และมี 1,053 ไซลินเดอร์

แหล่งอ้างอิง

Roger, Lawrence R., Home Computer Security, Computer Emergency Response Team/ Coordination Center, http://www.cert.org/homeusers/HomeComputerSecurity/

แปลและเรียบเรียงโดย พ.ต.ปนิวัธน์ ทรัพย์รุ่งเรือง, ที่ปรึกษาโครงการ, ศูนย์ประสานงานรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย