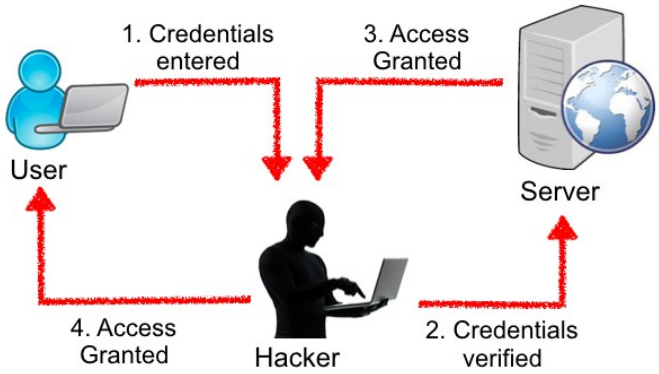
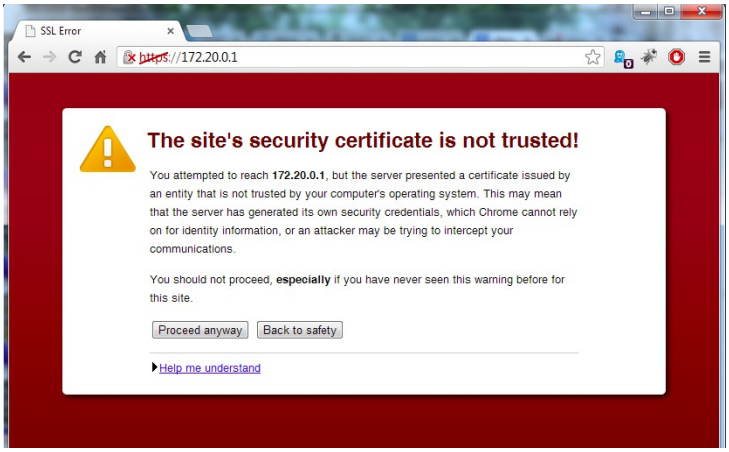
เรื่อง คำแนะนำในการใช้งานเครือข่ายไร้สายสาธารณะอย่างปลอดภัย
ทดสอบและเรียบเรียงโดย กิติศักดิ์ จิรวรรณกูล และ ปณิธาน เขินอำนวย
เรียบเรียงวันที่ 21 มิถุนายน 2559

ในปัจจุบันมีการให้บริการเครือข่ายไร้สายสาธารณะกันอย่างแพร่หลาย ทั้งตามสถานที่ต่างๆ ร้านอาหาร เครื่องดื่ม หรือแม้กระทั่งตามป้ายรถเมล์ ซึ่งเครือข่ายไร้สายเป็นการรับส่งข้อมูลในอากาศ ใครก็ตามสามารถเข้าถึงข้อมูลที่รับส่งได้อย่างง่ายดาย ดังนั้นหากมีผู้ประสงค์ร้ายสามารถใช้วิธีการต่างๆ เพื่อล่อลวง ขโมย ข้อมูลส่วนบุคคลของเรานั้น ในบทความนี้จึงอยากนำเสนอ**ตัวอย่างการโจมตีของเหล่าร้ายเพียงส่วนหนึ่งเท่านั้น** และตอนท้ายจะแนะนำ**วิธีการใช้งานเครือข่ายไร้สายสาธารณะอย่างปลอดภัย**

1. **การตั้งจุดเชื่อมต่อกระจายสัญญาณเครือข่ายไร้สายปลอม หรือการปลอม Access point** หากลองค้นหาสัญญาณไวไฟในที่สาธารณะ เราจะพบรายชื่อของจุดเชื่อมต่อกระจายสัญญาณไวไฟมากมาย อาจจะเป็นของผู้ให้บริการทางโทรคมนาคม ร้านอาหาร ร้านกาแฟ ห้างสรรพสินค้า หรือแม้กระทั่งสมาร์ทโฟนที่สามารถใช้กระจายสัญญาณไวไฟได้ เป็นต้น แต่รายชื่อที่พบตอนค้นหาสัญญาณนั้นไม่ได้การันตีได้ว่าจุดเชื่อมต่อกระจายสัญญาณไวไฟนี้เป็นของจริง เพราะไม่ว่าใครก็สามารถตั้งชื่อเป็นอะไรก็ได้ และแน่นอนว่าถ้าผู้ร้ายอยากได้ข้อมูลของเหยื่อ ก็ต้องปลอมชื่อจุดกระจายสัญญาณไวไฟให้เหมือนกับผู้ให้บริการทั่วไป หลอกเหยื่อจนตายใจและเชื่อมต่ออีกด้วย เมื่อเหยื่ออยู่ในระบบเครือข่ายเดียวกันกับผู้ประสงค์ร้ายแล้ว ก็อาจถูกสแกนหาช่องโหว่และเจาะระบบที่เครื่องของเหยื่อ เพื่อขโมยข้อมูลส่วนตัวได้
2. **การดักจับข้อมูลที่ถูกส่ง** ข้อมูลที่ถูกส่งในเครือข่ายไร้สายทั่วไปนั้น ทุกคนสามารถเข้าถึงได้ ทำให้ผู้ประสงค์ร้ายสามารถรู้ได้ว่าเหยื่อกำลังใช้งานอะไรบนระบบเครือข่ายอินเทอร์เน็ตอยู่ บ้างอาจจะใช้งานเครือข่ายสังคมออนไลน์ (Social media) รับส่งอีเมล์ (e-mail) โปรแกรมสนทนา (Chat) หรือแม้กระทั่งกำลังทำธุรกรรมการเงินกับธนาคารผ่านระบบอินเทอร์เน็ต เป็นต้น ผู้ประสงค์ร้ายอาจดักจับข้อมูลเพื่อจะดูว่ามีใครใช้งานและส่งข้อมูลโดยไม่เข้ารหัสหรือไม่ หากเหยื่อไม่ได้เข้ารหัสในการรับส่งข้อมูลไว้ ผู้ประสงค์ร้ายสามารถเห็นและเปิดอ่านข้อมูล หรือข้อความลับของเหยื่อได้
3. **การดักรหัสผ่าน** รหัสผ่านเป็นสิ่งที่สำคัญที่นิยมใช้แสดงความเป็นตัวตน ดังนั้นการขโมยรหัสผ่านจึงเป็นการโจมตีที่ผู้ประสงค์ร้ายนิยมกันอย่างแพร่หลาย ผู้ประสงค์ร้ายมีวิธีขโมยรหัสผ่านได้หลายวิธี แต่วิธีที่ทำให้เหยื่อรู้ตัวยากที่สุดคือการแอบมาอยู่ระหว่างกลางการส่งข้อมูล หรือที่เรียกว่า "Man in the Middle" ดังภาพที่ 1 และใช้วิธี SSLStrip เพื่อถอดฟังก์ชั่นการเข้ารหัสของเว็บนั้นออก (เปลี่ยนจาก HTTPS เป็น HTTP นั่นเอง) หรืออีกวิธีเหล่าร้ายจะส่งใบรับรองการเข้ารหัสปลอม (Faked certificate) มาให้ เพื่อหลอกว่าเรากำลังเชื่อมต่อกับเว็บด้วย HTTPS และเหยื่ออาจไม่ได้สังเกตว่าการใบรับรองการเข้ารหัสที่ใช้อยู่ในเว็บไซต์นั้นมีความผิดปกติ ซึ่งใบรับรองนี้ได้มาจากผู้ประสงค์ร้าย ทำให้ผู้ประสงค์ร้ายสามารถถอดรหัสและเปิดดูข้อมูลของเหยื่อได้ และลักษณะของหน้าเว็บไซต์ที่มีการแจ้งเตือนว่ามีใบรับรองที่ผิดปกติ ดังภาพที่ 2 หากท่านพบ ให้สอบถามไปยังเจ้าของเว็บไซต์ได้



ภาพที่ 1 แสดงกระบวนการโจมตีแบบ Man in the middle



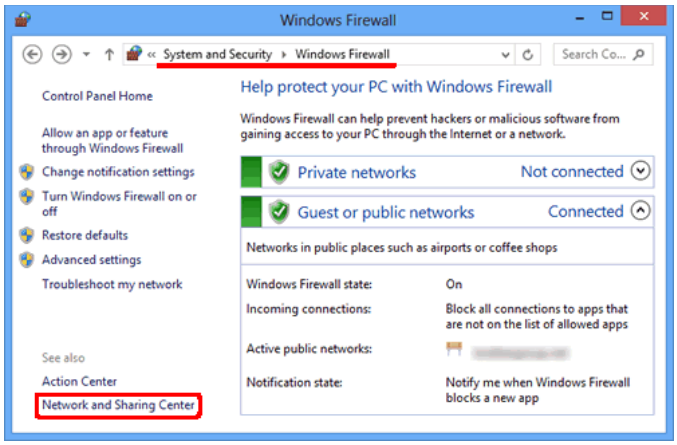
ภาพที่ 2 แสดงหน้าเว็บไซต์ที่มีใบรับรองการเข้ารหัสที่ผิดปกติ

วิธีการใช้งานระบบเครือข่ายไร้สายอย่างปลอดภัยดังต่อไปนี้

1. **หลีกเลี่ยงการเข้าถึงระบบที่สำคัญเมื่อใช้งานเครือข่ายไร้สายสาธารณะ** พึงระลึกไว้เสมอว่าไม่มีที่ไหนปลอดภัย ถ้าหากต้องการทำใช้งานอินเทอร์เน็ตที่มีความสำคัญมาก เช่นทำธุรกรรมบนอินเทอร์เน็ต ส่งเอกสารลับ ฯลฯ ให้หลีกเลี่ยงการใช้งานในเครือข่ายไร้สายสาธารณะ ให้กลับมาใช้งานอินเทอร์เน็ตจากที่บ้าน หรืออย่างน้อยให้ต่ออินเทอร์เน็ตจากโทรศัพท์มือถือของตนเอง ซึ่งควรตั้งระดับความปลอดภัยของการเข้ารหัสข้อมูลที่จุดเชื่อมต่อกระจายสัญญาณให้เป็น WPA2 เท่านั้น (ห้ามใช้ OPEN หรือ WEP) เพื่อป้องกันแอบดักจับข้อมูล และเปิดอ่านข้อมูลความลับได้
2. **พิจารณาชื่อจุดเชื่อมต่อกระจายสัญญาณที่พบ** เมื่อต้องการใช้งานระบบเครือข่ายไร้สายสาธารณะแล้วก็จำเป็นจะต้องรู้จักชื่อจุดเชื่อมต่อกระจายสัญญาณที่พบ และสังเกตชื่อดีๆ อาจจะถามจากผู้ให้บริการก็ได้ อย่างไรก็ตามเหล่าร้ายก็อาจจะปลอมชื่อจุดเชื่อมต่อกระจายสัญญาณก็ได้
3. **เมื่อเลิกใช้งานให้ลบรายชื่อจุดเชื่อมต่อกระจายสัญญาณทิ้ง** หลังจากหยุดเชื่อมต่อเครือข่ายไร้สาย ให้ลบรายชื่อจุดเชื่อมต่อกระจายสัญญาณออกจากเครื่อง เพื่อป้องกันไม่ให้เครื่องคอมพิวเตอร์ของเรานั้นเชื่อมต่อ

โดยอัตโนมัติ เนื่องจากถ้าหากเราอยู่ในบริเวณที่มีจุดเชื่อมต่อกระจายสัญญาณปลอม (ใช้ชื่อเดียวกับจุดเชื่อมต่อที่เราบันทึกไว้ก่อนหน้านี้แล้ว) เครื่องจะเชื่อมต่อทันที และมีความเสี่ยงที่เราจะถูกแอบดักขโมยข้อมูลด้วย

4. **เลือกใหม่ทุกครั้งเมื่อต้องการเชื่อมต่อกับจุดเชื่อมต่อกระจายสัญญาณเดิม** ทุกครั้งที่ต้องการเชื่อมต่อเครือข่ายไร้สาย ให้สังเกตดูว่าเป็นสิ่งผิดปกติหรือไม่ เช่นการเข้ารหัสเหมือนเดิมหรือไม่ (WEP หรือ WPA) เป็นต้น ถ้าหากไม่มีความผิดปกติ ก็ให้เลือกเชื่อมต่อด้วยตัวเองทุกครั้ง
5. **ไม่บันทึกรหัสผ่านหรือเปิดให้เข้าสู่ระบบในเว็บไซต์อย่างอัตโนมัติ** เนื่องจากหากเราบันทึกรหัสผ่านสำหรับการเข้าสู่ระบบไว้ เมื่อเราเปิดหน้าเว็บนั้นขึ้นมา ข้อมูลการเข้าสู่ระบบของเราจะถูกส่งออกจากเครื่องโดยทันที หากเราหลงเชื่อมต่อเครือข่ายไร้สายของผู้ไม่หวังดี จะทำให้เขาสามารถได้ข้อมูลการเข้าสู่ระบบของเราได้อย่างง่ายดาย
6. **เลือกเข้าเว็บไซต์ที่มีการเข้ารหัส** (สังเกตจากชื่อเว็บไซต์ว่าต้องมี "HTTPS" หรือมีรูปแม่กุญแจล็อก) หรือติดตั้งโปรแกรมเสริมชื่อ "HTTPS Everywhere" บน Firefox และ Chrome (ดาวน์โหลดได้จาก https://www.eff.org/https-everywhere)
7. **ติดตั้งโปรแกรมป้องกันมัลแวร์และอัพเดตซอฟต์แวร์ที่ใช้อย่างสม่ำเสมอ**
8. **ยกเลิกการแชร์ไฟล์** เนื่องจากเมื่อเชื่อมต่อเครือข่ายไร้สายแล้ว ก็ทำให้เครื่องคอมพิวเตอร์ที่เชื่อมต่อกับเครือข่ายไร้สายเดียวกันกับเรานั้นสามารถมองเห็นเครื่องของเราได้ ถ้าหากเปิดแชร์ไฟล์ไว้ ก็อาจทำให้ผู้ไม่หวังดี ได้ข้อมูลของเราไปโดยง่าย
9. **เลือกใช้งาน VPN ที่เชื่อถือได้** เมื่อจำเป็นต้องใช้เครือข่ายไร้สายสาธารณะเข้าถึงระบบสำคัญ ต้องใช้งาน Virtual Private Network (VPN) เพื่อเข้ารหัสการเชื่อมต่อไปยังระบบที่สำคัญ
10. **เปิดไฟร์วอลล์ของระบบปฏิบัติการ** โดยการเข้าไปใน Control Panel เลือก System and Security จากนั้นเลือก Windows Firewall ตามภาพที่ 3



ภาพที่ 3 แสดงภาพการใช้งานและปรับแต่ง Windows Firewall

สรุป

เนื่องจากบริการเครือข่ายไร้สายสาธารณะเปิดกว้างให้ทุกคนสามารถเข้าใช้งาน รวมไปถึงผู้ประสงค์ร้ายที่ต้องการขโมยข้อมูลส่วนตัวของผู้อื่น ด้วยวิธีการต่างๆ ซึ่งในบทความนี้ได้แสดงเพียงแค่ตัวอย่างเท่านั้น ดังนั้นเพื่อการรักษาความปลอดภัยของข้อมูลและไม่ให้ตกเป็นเหยื่อ จึงจำเป็นต้องปฏิบัติตามคำแนะนำในบทความนี้ ตลอดจนการติดตามข่าวสาร การแจ้งเตือนต่างๆ และต้องพึงระลึกไว้เสมอว่าเครือข่ายไร้สายสาธารณะมีความเสี่ยงสูง