

ระวัง! ใช้ Wi-Fi ทำธุรกรรมการเงินออนไลน์ เสี่ยงโดนแฮ็ค

นำเสนอเมื่อ : 6 พ.ย. 2555

[เรียบเรียงข้อมูลโดยกระปุกดอทคอม](#)

ขอขอบคุณภาพประกอบจาก [รายการเจาะข่าวเด่น](#) โพสต์โดย [คุณ DuangAesthetic](#) สมาชิกเว็บไซต์ยูทูปดอทคอม

สมัยนี้การทำธุรกรรมการเงินออนไลน์หรือผ่านอินเทอร์เน็ตกำลังเป็นที่นิยมอย่างสูง เนื่องจากสามารถทำได้ง่ายตาย อีกทั้งยังสะดวกรวดเร็ว ได้ทุกที่ทุกเวลา แต่รู้หรือไม่ว่าการทำธุรกรรมการเงินผ่านระบบออนไลน์ขณะนี้กำลังเสี่ยงอันตรายจากการแฮ็คข้อมูลของกลุ่มมิจฉาชีพเป็นอย่างมาก

เกี่ยวกับเรื่องนี้ รายการเจาะข่าวเด่น (5 พฤศจิกายน) จึงได้เชิญ นายปริญญา หอมเอนก ผอ.สถาบันฝึกอบรมความมั่นคงปลอดภัยทางข้อมูลสารสนเทศ (ACIS professional center) มาให้คำแนะนำถึงกรณีดังกล่าว

โดย นายปริญญา กล่าวว่า การเปิด Wi-Fi ในโทรศัพท์ มิจฉาชีพจะใช้อุปกรณ์ปล่อยสัญญาณพร้อมกับตั้งชื่อเหมือนกับ Wi-Fi ของสถานที่ดังกล่าว เมื่อผู้ใช้กดรับเพราะเข้าใจว่าเป็น Wi-Fi ของสถานที่นั้น ๆ มิจฉาชีพก็สามารถดูข้อมูล username และ password ของ Gmail, Hotmail, Facebook, Twitter, Instagram ฯลฯ ได้เลยทีเดียว



ทั้งนี้ นายปริญญา ได้แนะนำสำหรับการทำธุรกรรมการเงินออนไลน์อย่างปลอดภัย ว่า เพื่อป้องกันไม่ให้ถูกมิจฉาชีพแฮ็คข้อมูลจากคอมพิวเตอร์, โน้ตบุ๊ค และสมาร์ตโฟน เวลาที่เข้าหน้าหลักเพื่อใส่ username และ password นั้น ก่อนที่จะกรอกข้อมูลให้สังเกตโดเมนทางด้านขวาสุด จะขึ้นว่า <https://> (s ย่อมาจาก secure) แต่หากถูกอุปกรณ์ปล่อยสัญญาณจากมิจฉาชีพ โดเมนทางด้านขวาจะขึ้น <http://> (ไม่มี s) ซึ่งสมาร์ตโฟนจะต้องระวังเป็นพิเศษเนื่องจากหน้าจอเล็กกว่า ดังนั้นเพื่อความปลอดภัยควรกดเลื่อนไปดูโดเมนให้ครบถ้วนก่อนที่จะกรอกรหัสต่าง ๆ

นอกจากนี้ นายปริญญา กล่าวต่อไปว่า สำหรับวิธีป้องกันอีกอย่างหนึ่งคือ โหลดโปรแกรม **SSL STRIP Guard** ซึ่งตนเป็นคนเขียนเองสามารถดาวน์โหลดได้โดยไม่เสียค่าใช้จ่าย โดยเมื่อเขาไปแล้วจะมีคำว่า **Check now** ซึ่งระบบก็จะเช็คสมาร์ตโฟนให้ว่าเครื่องถูกแฮ็คอยู่หรือไม่ โดยจะมีคำว่า **Pass** และ **Warning**



นายปริญญา กล่าวเตือนผู้ใช้สมาร์ทโฟนด้วยว่า **อย่ากดรับ Socialcam** ที่เพื่อนส่งมาให้เราในขอความเด็ดขาด เพราะมันจะโหลด Trojan โดยอัตโนมัติ และมันจะส่ง SMS โดยที่เราไม่ได้อนุญาต ซึ่งเสีย SMS ละ 3 บาท และส่งไปในเพื่อนทุกคนที่เราบันทึกเบอร์เอาไว้ ซึ่งกรณีนี้ส่วนใหญ่จะเกิดกับเครื่อง iPhone ที่ทำ Jailbreak และ Android ซึ่งแฮ็คเกอร์จะนำข้อมูลความลับเหล่านี้ไปขายต่อ ถ้าเป็น username และ password ของธนาคาร มันจะเข้าไปเปลี่ยนรหัสผ่านและโอนเงิน ซึ่งผู้เสียหายบางรายสูญเงินกว่า 8 แสนบาทเลยทีเดียว โดยแฮ็คเกอร์เหล่านี้เป็นพวกรัสเซียที่อยู่แถวพัทยา และสุดท้ายนี้ขอเตือนด้วยว่า **ผู้ใช้ควรปิด location service** มิฉะนั้น มันจะรู้ความเคลื่อนไหวของผู้ใช้โดยตลอด

[ระวัง! ทำธุรกรรมการเงิน Online 1/2 : เครดิต รายการเจาะข่าวเด่น โพสต์โดย คุณ DuangAesthetic](#)

[ระวัง! ทำธุรกรรมการเงิน Online 2/2 : เครดิต รายการเจาะข่าวเด่น โพสต์โดย คุณ DuangAesthetic](#)