

เดือนผู้ใช้คอมพิวเตอร์บ้านปี 52 ระวังภัยบริการออนไลน์

IT Digest สังเกตว่า ขณะนี้ ภัยจากอินเทอร์เน็ต และคอมพิวเตอร์ เริ่มเป็นข่าวตามสื่อต่างๆ มากขึ้น และเพิ่มขึ้นเป็นเงาตามตัว ผู้ใช้งานอินเทอร์เน็ตในประเทศไทย คล้ายกับตรงไหนมีคนมารวมตัวอยู่มากๆ เหล่ามีจมาชีพ และผู้ไม่ประสงค์ดี ต่างก็หวังจะหาผลประโยชน์จากผู้ใช้งานที่ยังรู้เท่าไม่ถึงการณ์ การล่อลวงผู้ใช้งานให้ดาวน์โหลดโปรแกรมเสริม เพื่อตกแต่งไฮไฟว์ แต่แฝงโทรจัน หรือไวรัสมา อีกทั้งยังหลอกให้โอนเงิน หรือ บอกให้เลขที่บัญชีเพื่อรับรางวัลจากการชิงโชค และการคืนภาษี โดยวิธีการที่เหล่าคนเหล่านี้มาใช้ มีรูปแบบที่อย่างหลากหลาย เพราะวิธีการต่างๆ มาผสมผสานเป็นเรื่องใหม่ๆ ที่ผู้ใช้งานทั่วไปไม่มีทางรู้ทัน

เมื่อเร็วๆ นี้ก็มีรายงานข่าวว่าเจ้าหน้าที่ตำรวจกองปราบปราม บุกจับชายชามาเลเซีย ผู้ต้องหาตามหมายจับของศาลในสหรัฐอเมริกา ที่ก่อคดีขโมยข้อมูลจากบัตรเครดิตมาทำบัตรใหม่เพื่อรูดซื้อสินค้า สร้างความเสียหายให้แก่ธนาคารเจ้าของบัตรกว่า 5,000 ล้านบาท แล้วแอบเข้ามาทอนเงินในเมืองไทย นอกจากนี้ปี 2551 ที่ผ่านมา มีหลายคดีที่ชาวต่างชาติเป็นผู้ก่อเหตุร่วมกับคนไทยแอบขโมยข้อมูลการใช้งานธนาคารออนไลน์ เนื่องจากมีความรู้และความเชี่ยวชาญ ขณะที่คนไทยที่ตามเล่ห์เหลี่ยมไม่ทันกลายเป็นเหยื่อแทบทุกครั้ง

นายปริญญา หอมเอนก ผู้เชี่ยวชาญด้านความปลอดภัยทางคอมพิวเตอร์ อธิบายว่า ขณะนี้การใช้งานระบบอินเทอร์เน็ตในประเทศไทย มีจำนวนผู้ใช้งานมากกว่า 10 ล้านคน (ข้อมูลของศูนย์เทคโนโลยีอิเล็กทรอนิกส์ และคอมพิวเตอร์แห่งชาติ หรือ เนคเทค และสำนักงานสถิติแห่งชาติ) ส่วนมากจะมีช่วงเด็กมัธยม และวัยรุ่น เช่น การเล่นเกมออนไลน์ ผ่านอินเทอร์เน็ตทุกคร่ำเรือน จากความนิยมของเทคโนโลยีอินเทอร์เน็ตความเร็วสูง (ADSL) ผู้ใช้งานอินเทอร์เน็ตส่วนใหญ่ในวันนี้กำลังเพลิดเพลินกับ เทคโนโลยี WEB2.0 ที่เรารู้จักกันดีว่าเป็นเครือข่ายสังคมออนไลน์ (Social Network) เช่น เว็บไซต์ Hi5, My Space และ Face Book เชื่อได้ว่าภัยอินเทอร์เน็ตสมัยใหม่ จึงมุ่งไปยังกลุ่มผู้ใช้งานตามบ้าน



ผู้เชี่ยวชาญด้านความปลอดภัยทางคอมพิวเตอร์ อธิบายต่อว่า ขณะที่ความนิยมชำระเงินและทำธุรกรรมผ่านทางระบบออนไลน์ เช่น ระบบ **Internet Banking** และระบบ **Online Payment** ก็ทำให้กลุ่มผู้ไม่หวังดี หันมาปล้นเงินผ่านทางระบบออนไลน์มากขึ้น ด้วยการล่อลวงแบบต่างๆ เช่น ฟิชซิง และฟาร์มมิง กล่าวได้ว่าปี 2552 เป็นยุคที่ผู้ใช้งานตามบ้าน ต้องตกเป็นเหยื่อของการหลอกลวง และโจมตีจากผู้ไม่ประสงค์ดี และเหล่าแฮกเกอร์มากขึ้น โอกาสนี้จึงอยากแจ้งเตือนถึงภัยคุกคามความปลอดภัยอินเทอร์เน็ตปี 2552 ว่ามีเรื่องใดต้องระมัดระวัง ให้ความสนใจในการป้องกันตัว เพื่อให้รอดพ้นไม่ตกเป็นเหยื่อของผู้ไม่หวังดี

นายปริญญา อธิบายอีกว่า ภัยจากการใช้เทคโนโลยี WEB2.0 และ Social Networking (Client Side Attack) ถือเป็นภัยอันดับต้นๆ ที่มีการหลอกลวงผ่านทางเว็บไซต์ยอดนิยม เช่น Hi5 หรือ Face Book นั้นกำลังเป็นที่นิยมไปยังหมู่แฮกเกอร์ ด้วยเทคนิคหลากหลายรูปแบบผสมผสานกัน เช่น การใช้ฟิชซิง ร่วมกับ Social Engineering เช่น การหลอกให้ผู้ใช้งานหลงเข้าไป ล็อกอินในเว็บไซต์ปลอมที่ดูเหมือนเว็บไซต์ยอดนิยม ทำให้ผู้ใช้งานถูก ขโมย Username และ Password หรือ ความเป็นตัวตน (Identity Theft) โดยไม่รู้ตัว ยิ่งไปกว่านั้นโปรแกรมประสงค์ร้าย เช่น โทรจันยังนิยมแพร่กระจายผ่านทางเว็บไซต์ Social Network ดังกล่าว



ผู้เชี่ยวชาญด้านความปลอดภัย อธิบายถึงการป้องกันไม่ให้ตกเป็นเหยื่อการล่อลวงอย่างทีกล่าวมา คือ ต้องคอยสังเกตเวลา Login เข้าเว็บไซต์ว่าเป็น เว็บไซต์จริงหรือเว็บไซต์ปลอม ต้องมีสติพึงระลึกให้รู้ก่อนคลิก หรือ ป้อนข้อมูลส่วนตัว ชื่อผู้ใช้ และรหัสผ่าน ลงในเว็บไซต์ที่กำลังใช้งานอยู่ นอกจากนี้ยังควรหมั่นอัปเดต

ข้อมูลข่าวสารให้ทันเหตุการณ์ โดยการเข้าไปอ่านข่าวเกี่ยวกับเรื่องความปลอดภัยในอินเทอร์เน็ต หรืออ่านจากแมกกาซีนต่างๆ เพื่อให้เข้าใจถึงเทคนิคการล่อลวงใหม่ๆ ที่อาจเกิดขึ้นได้ตลอดเวลา

นายปริญญาอธิบายถึงภัยจากการทำธุรกรรมออนไลน์ และการใช้อี-คอมเมิร์ซว่า ภัยลักษณะนี้กำลังมีอัตราการเพิ่มขึ้นตามความนิยม ที่ผู้คนชอบหันมาทำธุรกรรมออนไลน์มากขึ้น เช่น การโอนเงินเข้าบัญชีเงินฝากไม่จำเป็นต้องโอนเงินที่ตู้เอทีเอ็ม แต่เลือกโอนผ่าน Internet Banking ได้ เนื่องจากสะดวกสบาย รวดเร็ว และประหยัดค่าใช้จ่ายในการเดินทาง ที่สำคัญไม่ต้องใช้บัตรเอทีเอ็มในการโอน หรือการซื้อของผ่านทางอินเทอร์เน็ต โดยใช้เพียงแค่ข้อมูลในบัตรเครดิต ก็สามารถสั่งซื้อของได้อย่างง่ายดาย

ต่อต้านหลัง

ผู้เชี่ยวชาญด้านความปลอดภัย อธิบายเสริมว่า กลุ่มอาชญากรคอมพิวเตอร์รุ่นใหม่ นิยมเจาะระบบการทำธุรกรรมออนไลน์เป็นหลัก เนื่องจากมีผลประโยชน์จากการได้ขโมยเงินในบัญชีของเหยื่อ เรียกว่า **No Hack For Fun** แต่ **Hack For Money** คนเหล่านี้ดำรงชีวิตอยู่ได้ด้วยการ การเจาะระบบ อีกทั้งพบว่า แสกเกอร์บางคนทำงานแบบนี้เป็นอาชีพหลักด้วย นอกจากการเจาะระบบแล้ว ยังมีกลโกงโดยการปลอม และคัดลอกข้อมูลในบัตรเอทีเอ็มแบบผิดกฎหมายอีกด้วย ขณะเดียวกันเหยื่ออีกกลุ่มหนึ่ง มักถูกหลอกให้ติดตั้งโปรแกรมม้าโทรจัน โดยใช้เทคนิคทำฟิชซิง และฟาร์มมิง ผ่านทางเว็บเบราว์เซอร์ยอดนิยม เช่น Internet Explorer: IE และ Firefox

ผู้เชี่ยวชาญด้านความปลอดภัย อธิบายเพิ่มเติมว่า โปรแกรมม้าโทรจันดังกล่าว มักจะทำงานในลักษณะของโปรแกรมดักข้อมูลจากคีย์บอร์ด เคยมีตัวอย่างในประเทศไทยมาแล้ว โดยลูกค้าธนาคารแห่งหนึ่งถูกขโมยโอนเงินไปกว่า 800,000 บาท



จากวิธีดังกล่าว เทคนิคการหลอกหลวงนั้นยังพัฒนาเพื่อการขโมย Username และ Password ของเหยื่อ เช่น เทคนิค Fast Flux (DNS Hijacking) หรือเทคนิค TYPO-SQUATTING (URL Hijacking) ตลอดจนการโทรศัพท์หลอกหลวงให้บอกข้อมูลส่วนตัว หรือ เทคนิค **Vishing** ดังที่เป็นข่าวใหญ่ในหนังสือพิมพ์หลายฉบับ และการแอบคัดลอกข้อมูลบัตรเครดิต เพื่อทำบัตรปลอมที่เรียกว่า **Skimming**

รวมทั้งการหลอกหลวงโดยเทคโนโลยีเดิมที่เก่าแก่ที่สุดในโลก ได้แก่ เทคนิค Social Engineering โดยการหลอกอาเหยื่อเพียงแค่ส่งอีเมลมาหลอก นิยมเรียกเทคนิคนี้ว่า **Internet SCAM** เช่น **จดหมายหลอกหลวงในจีเรียสสแควม** (Internet SCAM) โดยหลอกหลวงว่า เราจะได้รับเงินก้อนใหญ่ แค่เพียงโอนเงิน

ค่าธรรมเนียมเล็กน้อยไปให้เขาก่อน เรียกว่าเป็น **"ตกทองยุคไฮเทค"**

สำหรับทางแก้ปัญหาทั้งหมดนี้ จากที่รับทราบข้อมูลมา ยังเป็นทางแก้เดิมๆ ด้วยการกำหนดสติ เวลาที่ทำธุรกรรมออนไลน์ ไม่หลงเชื่ออีเมลหลอกหลวงที่ทำให้ผู้ใช้งานเกิดความโลภ และตกเป็นเหยื่อโดยรู้เท่าไม่ถึงการณ์ ขณะเดียวกันผู้ใช้งานก็ต้องพยายามยับยั้งชั่งใจก่อนที่จะให้ข้อมูล แก่บุคคลแปลกหน้าที่เข้ามาเสนอให้เงิน หรือ มอบรางวัลที่ไม่เคยมีส่วนเกี่ยวข้องกับที่สำคัญไม่ควรดาวน์โหลดโปรแกรมแปลก หรือ ของตกแดง ที่เป็นแอดออนหน้าเว็บเพจ ที่ไม่รู้ที่มา หรือคนที่เขียนโปรแกรม

ส่วนกรณีที่ถูกแอบปลอมบัตรเครดิตนั้น ทางแก้ คือ ควรหมั่นตรวจเช็ค ใบแจ้งรายละเอียดการใช้งาน และถ้าพบปัญหาให้แจ้งไปยังธนาคารที่ตัวเองถือบัตรเครดิตอยู่ ขณะที่การใช้งานสังคมออนไลน์ ไม่ควรเปิดเผยข้อมูลส่วนตัว เช่น อีเมล เบอร์โทรศัพท์ เลขบัญชีธนาคาร รวมถึงหมายเลขบัตรเครดิต หากปฏิบัติตามอย่างเคร่งครัด เชื่อว่า น่าจะป้องกันและแก้ไขปัญหาดังกล่าวได้

จลดิศ รัตนคำแปง
itdigest@thairath.co.th

ที่มา : <http://www.thairath.co.th/news.php?section=technology03a&content=124787>