โพสต์ทูเดย์
Post Today
Circulation: 320,000
Ad Rate: 1,100

Section: First Section/สกู๊ป
วันที่: อาทิตย์ 18 กันยายน 2559
ปีที่: 14 ฉบับที่: 4973 หน้า: A2(กลาง)
Col.Inch: 99.49 Ad Value: 109,439 PRValue (x3): 328,317 คลิป: สี่สี
หัวข้อข่าว: ดิจิทัลฟรีไม่มีในโลก 70%โดนฉกข้อมูล

ดิจิทัลฟรีไม่มีในโลก 70%โดนฉกข้อมูล

ทุกคนที่มีโทรศัพท์เคลื่อนที่ หรือมือถือ ชาวเน็ตที่ออนไลน์เกือบตลอดเวลา เชื่อแน่ว่าคงต้องได้รับโทรศัพท์ หรือข้อมูล ขายสินค้าหรือบริการต่างๆ โดยเฉพาะบัตรเครดิต ประกัน พวกปล่อยเงินกู้รวมหนี้ล้างหนี้ พิเศษต่างๆ หลายคนสงสัยปนรำคาญว่าพวกนี้ได้เบอร์อีเมล หรืออื่นๆ ติดต่อมาถึงได้อย่างไร บางครั้งเป็นเบอร์ลับเฉพาะ แต่ก็มีการโทรเข้ามาเรียกชื่อได้ถูกต้อง และบางทีรู้ข้อมูลส่วนตัวหลายอย่างจนผวาถึงภัยหากฝ่ายที่ติดต่อเข้ามาต้องการจะโจรกรรม

ด้วยการที่ข้อมูลมันมีราคา มีการเล่ากันว่าเบอร์โทรศัพท์ พร้อมชื่อผู้เป็นเจ้าของ ซื้อขายกันที่ชื่อละ 3 บาท หากข้อมูลนั้นพัฒนาให้สมบูรณ์ขึ้น รู้ว่ามีรายได้เท่าไร ชอบใช้จ่ายอย่างไร ชอบกินดื่มเที่ยวแบบไหน ว่ากันว่าราคาของข้อมูลจะสูงขึ้นเป็นชื่อละหลายสิบหลายร้อยบาท

ด้วยราคาค่างวดดังกล่าว จึงทำให้มีการขายข้อมูลกันอย่างคึกคัก รวมทั้งกรณีล่าสุด ซึ่งลูกค้าที่ชื่อว่า "พล" มัณฑนากร วัย 41 ปี ที่ถูกพนักงานของเอไอเอสนำข้อมูลการโทรเข้าและออก ตำแหน่งและเสาสัญญาณที่อยู่รอบตัว รวมทั้งระบุการเดินทาง ในไฟล์ข้อมูลที่ถูกส่งมาจากผู้หวังดีชี้ให้เห็นว่ามีข้อมูลย้อนหลังประมาณ 3-4 เดือน และมีหมายเลขโทรศัพท์ย้อนหลังไปถึงปี 2556 ซึ่งหลังจากที่ลูกค้ารายนี้ได้แจ้งเรื่องร้องเรียนไปยังเอไอเอส เซเรเนด และพบผู้จัดการสาขาของเอไอเอสแห่งหนึ่ง แต่กลับไม่ได้ความชัดเจน ภรรยาของ "พล" จึงได้นำเรื่องดังกล่าวไปโพสต์ในกระทู้เว็บไซต์พันทิป จากนั้นจึงมีการติดต่อกลับจากทางผู้บริหารและเดินทางไปเจรจากันที่สำนักงานใหญ่ และเมื่อทราบเรื่องบริษัทได้จัดการลงโทษขั้นสูงสุดคือ ไล่พนักงานคนดังกล่าวออกแล้ว

วิไล เดียงประดู่ ผู้ช่วยกรรมการผู้อำนวยการอาวุโส ส่วนงานประชาสัมพันธ์ บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส หรือเอไอเอส กล่าวว่า เรื่องดังกล่าวเป็นการกระทำผิดของพนักงานต่อ "นโยบายการคุ้มครองสิทธิและการรักษาข้อมูลส่วนบุคคลของผู้ใช้บริการ" และ "ประมวลจริยธรรมทางธุรกิจ" ของบริษัท ซึ่งเอไอเอสรู้สึกเสียใจและขออภัยลูกค้า ซึ่งเมื่อทราบเรื่องดังกล่าวบริษัทได้ตรวจสอบอย่างเข้มข้นทันที โดยสิ่งสำคัญในกระบวนการทำงาน คือ การกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของลูกค้าตามอำนาจหน้าที่ความรับผิดชอบ และกำหนดให้มีรหัสผ่านในการเข้าถึงข้อมูลทุกครั้ง มีการจัดให้มีการตรวจสอบโดยส่วนงานตรวจสอบภายในและโดยผู้เชี่ยวชาญอิสระจากภายนอกเป็นประจำ

โพสต์ทูเดย์
Post Today
Circulation: 320,000
Ad Rate: 1,100

Section: First Section/สกู๊ป
วันที่: อาทิตย์ 18 กันยายน 2559
ปีที่: 14 ฉบับที่: 4973 หน้า: A2(กลาง)
Col.Inch: 99.49 Ad Value: 109,439 PRValue (x3): 328,317 คลิป: สี่สี
หัวข้อข่าว: ดิจิทัลฟรีไม่มีในโลก 70%โดนฉกข้อมูล

ปริญญา หอมเอนก ผู้เชี่ยวชาญด้านระบบคอมพิวเตอร์และความมั่นคงปลอดภัยสารสนเทศ กล่าวว่า มีความเป็นได้ที่ปัญหาเหล่านี้อาจกลายเป็นปัญหาใหญ่ระดับโลก เหตุการณ์ลักษณะดังกล่าวมักเกิดขึ้นในต่างประเทศเป็นส่วนมาก แม้ว่าหลายบริษัทหน่วยงานราชการจะมีมาตรการดูแลที่เข้มงวดแล้วก็ตาม เพราะการนำข้อมูลออกมาไม่ได้มีกลวิธีที่ซับซ้อนยุ่งยากแต่อย่างใด สามารถทำกันได้ดื้อๆ เช่น พนักงานคนนั้นกดคิวรี (Query) สืบค้นข้อมูลได้ เพราะคนเหล่านั้นได้รับหน้าที่ให้เข้าถึงข้อมูลได้ ซึ่งปัญหาอยู่ที่เมื่อมีพนักงานจำนวนมาก การควบคุมจะทำอย่างไร บริษัทต้องตรวจสอบว่าพนักงานมีการเข้าไปถึงข้อมูลกี่ลำดับชั้น

อย่างไรก็ตาม สำหรับการเข้าถึงข้อมูลส่วนตัวของบุคคลไม่ใช่เฉพาะหน่วยงานของเอกชนเพียงอย่างเดียว แต่ยังรวมถึงหน่วยงานภาครัฐก็สามารถเข้าถึงข้อมูลได้ เช่น ข้อมูลทะเบียนราษฎร์ ข้อมูลตำรวจ ข้อมูลกรมการปกครอง ฯลฯ สามารถเข้าได้เช่นกันเพียงมีเลขบัตรประจำตัวประชาชน ก็สืบค้นข้อมูลได้ ดังนั้นในอนาคตเวลาพนักงานหรือเจ้าหน้าที่จะเข้าไปดูข้อมูลสำคัญของลูกค้าหรือประชาชน ควรจะต้องใส่ไอดีส่วนตัว และหากพบว่านำข้อมูลลูกค้าไปหาประโยชน์ ควรลงโทษหนักไล่ออกและดำเนินคดีอาญา

✓ **ด้าน กมล เกียรติเรืองกมล** ผู้ช่วยอธิการบดีฝ่ายสารสนเทศและการเงิน สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง อธิบายถึงสถานการณ์ความไม่ปลอดภัยในโลกไซเบอร์ ไม่ว่าจะเป็นการใช้งานผ่านเว็บไซต์หรือแอพพลิเคชั่นต่างๆ ว่า จากสถิติและประสบการณ์ที่คลุกคลีในวงการไอทีบอกได้เลยว่า มากกว่า 70% ผู้บริโภคมีความสุ่มเสี่ยงที่ข้อมูลส่วนตัวจะไปตกอยู่กับผู้ไม่หวังดี

"ถ้าเป็นขององค์กรหรือบริษัทใหญ่ จะมีความปลอดภัยสูงกว่าองค์กรขนาดกลางและขนาดเล็ก เพราะเว็บไซต์หลักจะได้รับการตรวจสอบรับรองความปลอดภัยจากองค์กรตรวจสอบระดับโลกโดยเฉพาะ ซึ่งข้อมูลของผู้ใช้งานที่อยู่ในเว็บไซต์ต่างๆ จะมีการเก็บบันทึกข้อมูลส่วนตัวผู้ใช้เอาไว้ทั้งหมด เช่น ชื่อ เบอร์โทรศัพท์ เลขที่บัญชีธนาคาร ข้อมูลส่วนตัวอื่นๆ ตามที่เราเคยกรอกข้อมูลเอาไว้ รวมทั้งประวัติการใช้งานและพ่วงท้ายด้วยไอพีแอดเดรส ซึ่งสามารถระบุได้ถึงที่อยู่ที่เราใช้งานอยู่ติดเข้าไปด้วย"

จากนั้นขึ้นอยู่กับนโยบายในการรักษาข้อมูลลูกค้า และระบบรักษาความปลอดภัยของบริษัทว่าแข็งแกร่งพอจะป้องกันได้มากน้อยแค่ไหนในการโจรกรรมข้อมูลวิธีแรกคนร้ายมักจะใช้กลวิธีการใช้เว็บฟิชชิ่ง เว็บเหล่านี้จะทำการก๊อบปี้หน้าเว็บจนแยกไม่ออก จนเหยื่อหลงเชื่อว่ากำลังเข้าเว็บไซต์จริง หลอกเอาล็อกอินพาสเวิร์ดของผู้ใช้งานเข้าไปเอาข้อมูลหรือส่งคำสั่งโอนเงินไปเข้าอีกบัญชีหนึ่ง

ต่อมาคือวิธีการส่งมัลแวร์เข้าไปฝังไว้ในเครื่อง ชนิดที่โปรแกรมแอนตี้ไวรัสบางตัวก็ไม่สามารถตรวจจับได้ว่ามีการทำงานเบื้องหลังหรือหลบซ่อนตัวอยู่ที่ไหน มัลแวร์เหล่านี้ส่วนมากจะได้มาจากการที่เราเข้าใช้งานเว็บไซต์ผิดกฎหมาย มัลแวร์ที่ฝังตัวเข้ามาจะตรวจจับการทำงานของคีย์บอร์ดแล้วส่งข้อมูลกลับไปที่ต้นทาง ซึ่งข้อมูลสำคัญเหล่านี้ก็คือล็อกอินและพาสเวิร์ด เลขที่บัตรประชาชน เบอร์โทรศัพท์ นั่นหมายความว่าแม้ว่าเราจะเข้าเว็บไซต์ที่มีระบบรักษาความปลอดภัยสูง ก็ไม่สามารถป้องกันการล้วงข้อมูลออกไปได้ เพราะเว็บไซต์กับการทำงานของคีย์บอร์ดในเครื่องเราเป็นคนละส่วนกัน

อีกวิธีหนึ่งก็คือการส่งไวรัสหรือมัลแวร์ในเครื่องสมาร์ทโฟน ซึ่งต่อไปเราจะได้ยินข่าวเกี่ยวกับการโจรกรรมข้อมูลในสมาร์ทโฟนมากขึ้น พวกนี้สามารถทำได้โดยการสร้างแอพพลิเคชั่นที่ผ่านการตรวจสอบความปลอดภัยให้เราดาวน์โหลด เช่น ฟรีเกม หรือแอพใช้งานฟรีต่างๆ โดยเบื้องหลังแอพเหล่านี้จะคอยดักจับข้อมูลในเครื่องส่งกลับไปที่ต้นทาง

วิธีการป้องกันไม่ว่าจะเป็นการใช้งานเว็บไซต์โซเชียลมีเดีย หรือแอพพลิเคชั่น สิ่งแรกที่ต้องทำก็คือให้สงสัยไว้ก่อนว่าเป็นเว็บหรือแอพที่มีจุดประสงค์ไม่ดี เวลาใช้งานเว็บไซต์ไม่ว่าจะเป็นเว็บอะไรก็ตาม ในขั้นตอนการกรอกล็อกอิน พาสเวิร์ด หรือกรอกข้อมูลส่วนตัว ให้ดูที่ช่องแอดเดรสของเว็บไซต์ว่ามี https:// นำหน้าชื่อเว็บไซต์และมีสัญลักษณ์รูปกุญแจปรากฏอยู่หรือไม่ ถ้ามีแสดงว่ามีการเข้ารหัสความปลอดภัยเชื่อถือได้ แต่ถ้าไม่มีให้สงสัยไว้ก่อนว่าเป็นเว็บปลอม หรือมีจุดประสงค์อื่นแอบแฝง

ถ้าเป็นเว็บธนาคารลิงค์การกรอกข้อมูลล็อกอินและพาสเวิร์ดจะต้องกดเข้าผ่านหน้าเว็บหลักของธนาคารเท่านั้น หรือสงสัยให้โทรสอบถามกับธนาคารโดยตรง และที่กำลังนิยมอยู่ในตอนนี้ก็คือแอพเฟซบุ๊กเล่นเกมควิซต่างๆ แอพเหล่านี้จะมีการระบุการเข้าถึงข้อมูลส่วนตัวของผู้ใช้ ข้อมูลรูปภาพ ข้อมูลเพื่อน หรือข้อมูลการใช้งานอื่นๆ จึงไม่ควรเข้าใช้งานอย่างเด็ดขาด

ต่อมาในขั้นตอนการใส่ล็อกอินพาสเวิร์ด แนะนำให้ใช้งานฟังก์ชั่นคีย์บอร์ดสกรีน (ในระบบปฏิบัติการวินโดว์ใช้คำสั่ง Windows+Q แล้วพิมพ์คำว่า osk)

โพสต์ทูเดย์
Post Today
Circulation: 320,000
Ad Rate: 1,100

Section: First Section/สกู๊ป
วันที่: อาทิตย์ 18 กันยายน 2559
ปีที่: 14 ฉบับที่: 4973 หน้า: A2(กลาง)
Col.Inch: 99.49 Ad Value: 109,439 PRValue (x3): 328,317 คลิป: สี่สี
หัวข้อข่าว: ดิจิทัลฟรีไม่มีในโลก 70%โดนฉกข้อมูล

แล้วใช้เมาส์คลิกใส่ข้อมูลต่างๆ แทนการพิมพ์ ซึ่งมัลแวร์จะไม่สามารถตรวจจับได้ว่าเราใส่ข้อมูลอะไร นอกจากนี้เราไม่ควรใส่ข้อมูลจริงลงในโซเชียลมีเดีย หรือเว็บไซต์ที่ไม่ใช่เว็บที่มีความสำคัญ อย่างเว็บของทางราชการ หรือเว็บไซต์ที่เกี่ยวข้องกับสถาบันการเงิน

ในเรื่องรูปถ่ายเราก็ควรให้ความสำคัญ เพราะปัจจุบันมีการแชร์โพสต์ภาพถ่ายอย่างแพร่หลายในโลกโซเชียลมีเดีย ไม่ควรแท็กสถานที่ หรือใช้สมาร์ทโฟนถ่ายภาพแบบใส่ข้อมูลพิกัดสถานที่ลงในรูปภาพเหล่านี้ เพราะจะมีข้อมูลที่ระบุถึงตำแหน่งที่อยู่ผู้ใช้งานอยู่ในภาพถ่ายเหล่านี้ด้วย

สุดท้าย ไม่ควรดาวน์โหลดแอพพลิเคชั่นที่ไม่ได้อยู่ในระบบของเพลย์สโตร์ หรือแอพสโตร์ เพราะแอพเหล่านี้ไม่ได้ผ่านระบบการรักษาความปลอดภัย ผู้ผลิตอาจจะมีวัตถุประสงค์ในการล้วงข้อมูลส่วนตัวเพื่อนำไปใช้ในทางไม่ดี ซึ่งจะพบปัญหานี้ได้มากในเครื่องที่ผ่านการแครก และลงแอพพลิเคชั่นที่ไม่ได้ผ่านระบบการตรวจสอบอย่างถูกต้อง