

โพสต์ทูเดย์ Post Today Circulation: 320,000 Ad Rate: 1,100	Section: First Section/สฎป วันที่: อาทิตย์ 18 กันยายน 2559 ปีที่: 14 ฉบับที่: 4973 Col.Inch: 99.49 Ad Value: 109,439 หัวข้อข่าว: ดิจิทัลฟรีไม่มีในโลก 70%โดนฉกข้อมูล			หน้า: A2(กลาง) PRValue (x3): 328,317	คลิ๊ป: ลีลี

ดิจิทัลฟรีไม่มีในโลก 70%โดนฉกข้อมูล



ท 9 คนที่มีโทรศัพท์มือถือ หรือมือถือ ชาวเน็ตที่ออนไลน์เกือบตลอดเวลา เชื่อแน่ว่า คงต้องได้รับโทรศัพท์ หรือข้อมูล ขายสินค้าหรือบริการต่างๆ โดยเฉพาะบัตรเครดิต ประกัน พวกปล่อยเงินกู้รวมหนี้ล้างหนี้ พิเศษต่างๆ หลายคนสงสัยป็นราคาว่าพวกนี้ได้เบอร์อีเมล หรืออื่นๆ ติดต่อกันได้อย่างไร บางครั้งเป็นเบอร์ลับเฉพาะ แต่ก็มีการโทรเข้ามาเรียกชื่อได้ถูกต้อง และบางทีรู้ข้อมูลส่วนตัวหลายอย่างจนผวาถึงภัยหากฝ่ายที่ติดต่อเข้ามาต้องการจะโจรกรรม

ด้วยการที่ข้อมูลมันมีราคา มีการแลกกันว่าเบอร์โทรศัพท์ พร้อมชื่อผู้เป็นเจ้าของ ซื้อขายกันที่ชื่อละ 3 บาท หากข้อมูลนั้นพัฒนาให้สมบูรณ์ขึ้น รู้ว่ามีรายได้เท่าไร ชอบใช้จ่ายอย่างไร ชอบกินดื่มเที่ยวแบบไหน ว่ากันว่าราคาของข้อมูลจะสูงขึ้นเป็นชื่อละหลายสิบหลายร้อยบาท

ด้วยราคาค่างวดดังกล่าว จึงทำให้มีการขายข้อมูลกันอย่างคึกคัก รวมทั้งกรณีล่าสุด ซึ่งลูกค้าที่ชื่อว่า "พล" มณฑลนาคร วัย 41 ปี ที่ถูกพนักงานของเอไอเอสนำข้อมูลการโทรเข้าและออก ตำแหน่งและเส้นสัญญาณที่อยู่รอบตัว รวมทั้งระบบการเดินทาง ในไฟล์ข้อมูลที่ถูกส่งมาจากผู้หวังดีชี้ให้เห็นว่ามีข้อมูลย้อนหลังประมาณ 3-4 เดือน และมีหมายเลข

โทรศัพท์ย้อนหลังไปถึงปี 2556 ซึ่งหลังจากที่ลูกค้ารายนี้ได้แจ้งเรื่องร้องเรียนไปยังเอไอเอส เซเรเนด และพบผู้จัดการสาขาของเอไอเอสแห่งหนึ่ง แต่กลับไม่ได้ความชัดเจน ภรรยาของ "พล" จึงได้นำเรื่องดังกล่าวไปโพสต์ในกระทู้เว็บไซต์พันทิป จากนั้นจึงมีการติดต่อกลับจากทางผู้บริหารและเดินทางไปเจรจากันที่สำนักงานใหญ่ และเมื่อทราบเรื่องบริษัทได้จัดการลงโทษขั้นสูงสุดคือ ไล่นักงานคนดังกล่าวออกแล้ว

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

ปัญญา หอมเอนก ผู้เชี่ยวชาญด้านระบบคอมพิวเตอร์และความมั่นคงปลอดภัยสารสนเทศกล่าวว่า ความเป็นไปได้ที่ปัญหาเหล่านี้อาจกลายเป็นปัญหาใหญ่ระดับโลก เหตุการณ์ลักษณะดังกล่าวมักเกิดขึ้นในต่างประเทศเป็นส่วนมาก แม้ว่าหลายบริษัทหน่วยงานราชการจะมีมาตรการดูแลที่เข้มงวดแล้วก็ตาม เพราะการนำข้อมูลออกมาไม่ได้มีกลวิธีที่ซับซ้อนยุ่งยากแต่อย่างใด สามารถทำได้ง่ายๆ เช่น พนักงานคนนั้นกดคิวรี (Query) สืบค้นข้อมูลได้ เพราะคนเหล่านั้นได้รับหน้าที่ให้เข้าถึงข้อมูลได้ ซึ่งปัญหายังอยู่ที่เมื่อมีพนักงานจำนวนมาก การควบคุมจะอย่างไร บริษัทต้องตรวจสอบว่าพนักงานมีการเข้าไปถึงข้อมูลกี่ลำดับชั้น

อย่างไรก็ตาม สำหรับการเข้าถึงข้อมูลส่วนตัวของบุคคลไม่ใช่เฉพาะหน่วยงานของเอกชนเพียงอย่างเดียว แต่ยังรวมถึงหน่วยงานภาครัฐก็สามารถเข้าถึงข้อมูลได้ เช่น ข้อมูลทะเบียนราษฎร์ ข้อมูลตำรวจ ข้อมูลกรมการปกครอง ฯลฯ สามารถเข้าถึงได้เช่นกันเพียงมีเลขบัตรประจำตัวประชาชน ก็สืบค้นข้อมูลได้ ดังนั้นในอนาคตเวลาพนักงานหรือเจ้าหน้าที่จะเข้าไปดูข้อมูลสำคัญของลูกค้าหรือประชาชน ควรจะต้องใส่ไอดีส่วนตัว และหากพบว่านำข้อมูลลูกค้าไปหาประโยชน์ ควรลงโทษหนักใส่ ออกและดำเนินคดีอาญา

ด้าน **กมล เกียรติเรืองกมล** ผู้ช่วยอธิการบดีฝ่ายสารสนเทศและการเงิน สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง อธิบายถึงสถานการณ์ความไม่ปลอดภัยในโลกไซเบอร์ ไม่ว่าจะเป็นการใช้งานผ่านเว็บไซต์หรือแอปพลิเคชันต่างๆ ว่า จากสถิติและประสบการณ์ที่ลูกค้าในวงการไอทีบอกได้เลยว่า มากกว่า 70% ผู้บริโภคมีความเสี่ยงที่ข้อมูลส่วนตัวจะตกอยู่กับผู้ไม่หวังดี

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

จากนั้นขึ้นอยู่กับนโยบายในการรักษาข้อมูลลูกค้า และระบบรักษาความปลอดภัยของบริษัทว่าแข็งแกร่งพอจะป้องกันได้มากน้อยแค่ไหนในการ

โจรกรรมข้อมูลวิธีแรกคนร้ายมักจะใช้กลวิธีการใช้เว็บฟิชชิง เว็บเหล่านี้จะทำการก๊อปปี้หน้าเว็บจนแยกไม่ออก จนเหยื่อหลงเชื่อที่กำลังเข้าเว็บไซต์จริง หลอกเอาล็อกอินพาสเวิร์ดของผู้ใช้งานเข้าไป เอาข้อมูลหรือส่งคำสั่งโอนเงินไปเข้าอีกบัญชีหนึ่ง

ต่อมาคือวิธีการส่งมัลแวร์เข้าไปฝังไว้ในเครื่องชนิดที่โปรแกรมแอนตี้ไวรัสบางตัวก็ไม่สามารถตรวจจับได้ว่ามีการทำงานเบื้องหลังหรือหลบซ่อนตัวอยู่ที่ไหน มัลแวร์เหล่านี้ส่วนมากจะได้มาจากการที่เราเข้าใช้งานเว็บไซต์ผิดกฎหมาย มัลแวร์ที่ฝังตัวเข้ามากจะตรวจจับการทำงานของคีย์บอร์ดแล้วส่งข้อมูลกลับไปที่ดินทาง ซึ่งข้อมูลสำคัญเหล่านี้ก็คือล็อกอินและพาสเวิร์ด เลขที่บัตรประชาชน เบอร์โทรศัพท์ นั่นหมายความว่าแม้ว่าเราจะเข้าเว็บไซต์ที่มีระบบรักษาความปลอดภัยสูง ก็ไม่สามารถป้องกันการล้วงข้อมูลออกไปได้ เพราะเว็บไซต์กับการทำงานของคีย์บอร์ดในเครื่องเราเป็นคนละส่วนกัน

อีกวิธีหนึ่งก็คือการส่งไวรัสหรือมัลแวร์ในเครื่องสมาร์ทโฟน ซึ่งต่อไปเราจะได้ยินข่าวเกี่ยวกับการโจรกรรมข้อมูลในสมาร์ทโฟนมากขึ้น พวกนี้สามารถทำได้โดยการสร้างแอปพลิเคชันที่ผ่านการตรวจสอบความปลอดภัยให้เราดาวน์โหลด เช่น ฟรีเกม หรือแอปใช้งานฟรีต่างๆ โดยเบื้องหลังแอปเหล่านี้จะคอยดักจับข้อมูลในเครื่องส่งกลับไปที่ดินทาง

วิธีการป้องกันไม่ว่าจะเป็นการใช้งานเว็บไซต์โซเชียลมีเดีย หรือแอปพลิเคชัน สิ่งแรกที่ต้องทำก็คือให้สงสัยไว้ก่อนว่าเป็นเว็บหรือแอปที่มีจุดประสงค์ไม่ดี เวลาใช้งานเว็บไซต์ไม่ว่าจะเป็นเว็บอะไรก็ตาม ในขั้นตอนการกรอกล็อกอิน พาสเวิร์ด หรือกรอกข้อมูลส่วนตัว ให้ดูที่ช่องแอดเดรสของเว็บไซต์ว่ามี <https://> นำหน้าชื่อเว็บไซต์และมีสัญลักษณ์รูปกุญแจปรากฏอยู่หรือไม่ ถ้ามีแสดงว่ามีการเข้ารหัสความปลอดภัยเชื่อถือได้ แต่ถ้าไม่มีให้สงสัยไว้ก่อนว่าเป็นเว็บปลอม หรือมีจุดประสงค์อื่นแอบแฝง

ถ้าเป็นเว็บธนาคารลิงค์การกรอกข้อมูลล็อกอินและพาสเวิร์ดจะต้องกดเข้าผ่านหน้าเว็บหลักของธนาคารเท่านั้น หรือสงสัยให้โทรสอบถามกับธนาคารโดยตรง และที่กำลังนิยมอยู่ในตอนนี้ก็คือแอปเฟชบุ๊กเล่นเกมควิชต่างๆ แอปเหล่านี้จะมีการระบุการเข้าถึงข้อมูลส่วนตัวของผู้ใช้ ข้อมูลรูปภาพ ข้อมูลเพื่อน หรือข้อมูลการใช้งานอื่นๆ จึงไม่ควรเข้าใช้งานอย่างเด็ดขาด

ต่อมาในขั้นตอนการใส่ล็อกอินพาสเวิร์ด แนะนำให้ใช้งานฟังก์ชันคีย์บอร์ดสกรีน (ในระบบปฏิบัติการวินโดวส์ใช้คำสั่ง Windows+Q แล้วพิมพ์คำว่า osk)

แล้วใช้เมาส์คลิกใส่ข้อมูลต่างๆ แทนการพิมพ์ ซึ่ง
มันแล้วจะไม่สามารถตรวจสอบได้ว่าเราใส่ข้อมูลอะไร
นอกจากนี้เราไม่ควรใส่ข้อมูลจริงลงในโซเชียลมีเดีย
หรือเว็บไซต์ที่ไม่ใช่เว็บที่มีความสำคัญ อย่างเว็บ
ของทางราชการ หรือเว็บไซต์ที่เกี่ยวข้องกับสถาบัน
การเงิน

ในเรื่องรูปถ่ายเราก็ควรให้ความสำคัญ เพราะ
ปัจจุบันมีการแชร์โพสต์ภาพถ่ายอย่างแพร่หลายใน
โลกโซเชียลมีเดีย ไม่ควรแท็กสถานที่ หรือใช้สมาร์
ทโฟนถ่ายภาพแบบใส่ข้อมูลพิกัดสถานที่ลงใน
รูปภาพเหล่านี้ เพราะจะมีข้อมูลที่ระบุถึงตำแหน่ง
ที่อยู่ผู้ใช้งานอยู่ในภาพถ่ายเหล่านี้ด้วย

สุดท้าย ไม่ควรดาวน์โหลดแอปพลิเคชันที่ไม่
ได้อยู่ในระบบของเพลย์สโตร์ หรือแอปสโตร์ เพราะ
แอปเหล่านี้ไม่ได้ผ่านระบบการรักษาความปลอดภัย
ผู้ผลิตอาจจะมีวัตถุประสงค์ในการล้วงข้อมูลส่วนตัว
เพื่อนำไปใช้ในทางไม่ดี ซึ่งจะพบปัญหานี้ได้มากใน
เครื่องที่ผ่านการแครก และลงแอปพลิเคชันที่ไม่ได้
ผ่านระบบการตรวจสอบอย่างถูกต้อง