มุมไอที

มนวิกา ผดุงสิทธิ์*

โจรไฮเทค

ช่วงนี้มีข่าวที่เกี่ยวข้องกับกลโกงบัตรเครดิตและการฉ้อโกงทางเอทีเอ็มค่อนข้างบ่อย ถึงแม้เรื่องนี้จะดูเหมือนว่าไม่ได้เป็นเรื่อง IT แต่จริงๆ แล้ว ก็ถือว่าใกล้เคียง เพราะเป็นการที่กลุ่มมิจฉาชีพนำเทคโนโลยีมาใช้เป็นเครื่องมือในการฉ้อโกง ยิ่งเรามีเทคโนโลยีที่ “ไฮเทค” มากขึ้นเท่าใด วิธีการที่กลุ่มมิจฉาชีพนำมาใช้ก็ยิ่งสลับซับซ้อนมากขึ้นเท่านั้น และยิ่งเศรษฐกิจฝืดเคืองมากขึ้น กลุ่มคนร้ายก็มากขึ้น ผู้เขียนคิดว่าเรื่องนี้เป็นเรื่องที่ใกล้ตัวค่อนข้างมาก จึงขอถือโอกาสรวบรวมข่าวคราวเกี่ยวกับกลโกงบัตรเครดิตและเอทีเอ็ม เพื่อให้ทุกท่านได้เพิ่มความ (หวาดระแวง?) ระมัดระวังในการใช้บัตรเครดิตและเอทีเอ็มให้มากยิ่งขึ้น

พล.ต.ต.วิสุทธิ์ วาณิชบุตร ผู้บังคับการปราบปรามอาชญากรรมทางเศรษฐกิจและเทคโนโลยี (ปศท.) เปิดเผยว่า ในปัจจุบันมิจฉาชีพมีการใช้เทคโนโลยีเข้ามาเป็นเครื่องมือในการทำมาหากินยิ่งขึ้น โดยเฉพาะอย่างยิ่งการฉ้อโกงเกี่ยวกับบัตรเครดิตซึ่งมีวงเงินให้ฉ้อโกง

* Ph.D (Accounting) ผู้ช่วยศาสตราจารย์ประจำ ภาควิชาการบัญชี ผู้อำนวยการโครงการปริญญาโททางการบัญชี คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์
คณะกรรมการวิชาชีพด้านการศึกษาและเทคโนโลยีการบัญชี สภาวิชาชีพบัญชีฯ

ปีที่ 3 ฉบับที่ 8
ธันวาคม 2550
หน้า 20-23

มากกว่าเอทีเอ็ม ตัวอย่างเช่น กลุ่มมิจฉาชีพจะจ้างพนักงานร้านอาหาร ปั๊มน้ำมัน หรือร้านค้า เป็น “นกต่อ” ให้นำบัตรเครดิตของลูกค้าไปให้ โดยเมื่อได้บัตร จะมีการรูดบัตรเครดิต 2 ครั้ง ครั้งแรกเป็นการรูดจ่ายเงินเป็นค่าสินค้าตามปกติ ส่วนครั้งที่สองจะเป็นการดูดข้อมูลของลูกค้า (Skimming) โดยนำบัตรไปรูดกับเครื่อง Skimmer ซึ่งมีขนาดเล็ก ซึ่งเครื่องดังกล่าวจะ Copy แถบแม่เหล็กบนหลังบัตรและนำไปเขียนในแถบแม่เหล็กใหม่ ทำให้สามารถทำบัตรปลอมโดยมีข้อมูลเหมือนบัตรจริงทุกประการ จากนั้น ก็นำบัตรเครดิตปลอมไปใช้ซื้อสินค้าซึ่งจะเน้นที่สินค้าราคาแพง เช่น ทองคำ เครื่องเพชร ผู้ที่นำบัตรปลอมไปใช้ก็เป็นเพียง “มือปืนรับจ้าง” ซึ่งจะได้รับส่วนแบ่ง 20-25% และถ้าถูกจับได้ เรื่องก็จะจบอยู่ที่มือปืนรับจ้าง ไม่สามารถสืบสาวหาต้นตอได้

เมื่อไม่นานมานี้ ผู้เขียนได้ดูสารคดีรายการหนึ่ง ซึ่งสาธิตวิธีการใช้เครื่อง Skimmer ในการขโมยข้อมูลจากบัตรเครดิต โดยพนักงานจะผูกเครื่องดังกล่าวไว้ที่ข้อเท้าซึ่งคลุมด้วยกางเกงขายาว (เครื่องดังกล่าวมีขนาดเล็กเท่ากับเพจเจอร์) และเมื่อรับบัตรเครดิตจากลูกค้า พนักงานจะแกล้งทำบัตรหลุดมือ เมื่อก้มลงหยิบ จะหันข้างให้ลูกค้าและรูดบัตรผ่านเครื่อง Skimmer โดยที่ลูกค้าไม่ทันได้สังเกต หลังจากนั้น ก็จะคืนบัตรให้ลูกค้าและแจ้งว่าลูกค้าว่าจะเอาเครื่อง POS มาให้ลูกค้ารูดบัตรด้วยตนเอง เพื่อให้ลูกค้าเห็นว่าพนักงานมีความเป็นห่วงเรื่องความปลอดภัยของข้อมูลในบัตรเครดิต ซึ่งลูกค้าก็จะไม่สงสัยเลยว่าข้อมูลส่วนตัวของตนถูกขโมยจากพนักงานคนดังกล่าว หรืออีกกรณีหนึ่ง พนักงานจะซ่อนเครื่อง Skimmer ไว้ในกระเป๋าของผ้ากันเปื้อน และเมื่อรับบัตรเครดิตจากลูกค้า ก็จะทำเหมือนบัตรเปื้อน และใช้ผ้ากันเปื้อนเช็ดบัตร ซึ่งก็มีการรูดบัตรผ่านเครื่อง Skimmer ในขั้นตอนนี้เช่นกัน

ส่วนกลโกงบัตรเครดิตอีกรูปแบบหนึ่งนั้น จะเน้นที่ชาวต่างชาติที่เดินทางมาเมืองไทย โดยกลุ่มมิจฉาชีพจะติดต่อกับ “นกต่อ” ตามโรงแรมเพื่อดูดเอาข้อมูลในบัตรเครดิต พร้อมทั้งขอสำเนาหนังสือเดินทางและสลิปบัตรเครดิตเพื่อดูลายเซ็น จากนั้น จึงทำบัตรปลอมขึ้นมาโดยลายเซ็นที่เหมือนกับเจ้าของเดิมและให้ “มือปืนรับจ้าง” นำไปรูดซื้อสินค้า บัตรปลอมที่เหมือนบัตรจริงมากจะเรียกว่า บัตรปลอมโซนยุโรป ซึ่งจะมีราคาแพงกว่า 1 แสนบาท แต่ก็คุ้มเพราะมีวงเงินนำไปซื้อสินค้าได้เป็นหลักล้าน ส่วนบัตรราคาที่ถูกที่สุดที่ขายในประเทศไทยมีราคาประมาณใบละ 6,000 บาท ซึ่งก็ไม่แน่นอนว่าจะใช้รูดซื้อสินค้าได้มากน้อยเพียงใด

กลโกงบัตรเครดิตทั้งสองรูปแบบข้างต้นมีแนวโน้มเพิ่มขึ้น เนื่องจากคนร้ายเป็นแก๊งอาชญากรรมข้ามชาติ ไม่ใช่คนไทย และไม่ได้อาศัยอยู่ในประเทศไทย ทำให้ตำรวจมีข้อมูลน้อยเกี่ยวกับคนร้าย การจับกุมจึงเป็นไปได้ยาก และคนร้ายไม่ได้ฉ้อโกงในประเทศใดประเทศหนึ่งโดยเฉพาะ แต่จะทำการในหลายประเทศ เช่น ไทย มาเลเซีย สิงคโปร์ ยุโรป และสหรัฐอเมริกา เป็นต้น

พ.ต.ต.วิสุทธิ์ เปิดเผยเพิ่มเติมว่า วิธีการล่าสุดที่คนร้ายนำมาใช้คือ การแทปข้อมูล โดยใช้อุปกรณ์ที่สั่งทำขึ้นเป็นพิเศษเพื่อดูดข้อมูลรหัสบัตรเครดิตที่ผ่านเข้ามาในชุมสายโทรศัพท์ และใช้โปรแกรมที่เขียนขึ้นมาเองในการถอดและสกัดเอารหัสบัตรเครดิตพร้อมกับ Security Code ซึ่งเป็นรหัสลับของระบบรักษาความปลอดภัยของธนาคาร บางธนาคารมีการป้องกันวิธีการดังกล่าวโดยการเปลี่ยนจากระบบการส่งข้อมูลผ่านชุมสายโทรศัพท์มาเป็นการส่งข้อมูลทางเคเบิลใยแก้วนำแสงที่ฝังอยู่ใต้ดินแทน

นอกจากนี้ กลุ่มมิจฉาชีพอาจใช้อุปกรณ์พื้นฐานเป็นเครื่องมือ นั่นคือ การโทรศัพท์ไปหาลูกค้าและอ้างว่าโทรมาจากสถาบันการเงินที่ออกบัตรเครดิตเพื่อทวงหนี้บัตรเครดิต โดยขั้นแรกจะใช้รูปแบบของข้อความจากระบบโทรศัพท์อัตโนมัติ และแจ้งว่าลูกค้ามียอดค้างชำระบัตรเครดิต จะต้องไปชำระเงินภายในวันดังกล่าว และหากต้องการทราบข้อมูลเพิ่มเติม ให้กดเลข 9 เมื่อลูกค้าสงสัยและกดเลข 9 ก็จะมีผู้รับสายพร้อมกับซักถามข้อมูลเกี่ยวกับบัตรและข้อมูลส่วนตัว เช่น เลขที่บัตรประจำตัว

ประชาชน ชื่อและนามสกุลที่ถูกต้อง วันเดือนปีเกิด ที่อยู่ เบอร์โทรศัพท์ วงเงินที่ได้รับอนุมัติ ซึ่งข้อมูลดังกล่าว คนร้ายก็นำไปใช้กับบัตรเครดิตปลอม

สำหรับคดีที่เกี่ยวกับเอทีเอ็มนั้น ในเดือนมิถุนายน ของปีนี้ ศูนย์สืบสวนปราบปรามคนร้ายข้ามชาติและอาชญากรรมบัตรอิเล็กทรอนิกส์ กองบังคับการตำรวจท่องเที่ยว ได้จับกุมกลุ่มมิจฉาชีพที่ใช้เทคนิค Phishing โดยการจดทะเบียนเว็บไซต์ปลอมยังต่างประเทศ แล้วสร้างเว็บไซต์เลียนแบบเว็บไซต์ของธนาคารพาณิชย์และสถาบันการเงินของไทยที่เปิดให้บริการลูกค้าทางอินเทอร์เน็ต โดยเพิ่มช่องให้ลูกค้าใส่รหัสบัตรเอทีเอ็มบนหน้าเว็บไซต์ หลังจากนั้น คนร้ายก็สุ่มส่งหน้าเว็บไซต์ที่สร้างเลียนแบบไปตามอีเมล์ของลูกค้าธนาคาร ถ้าลูกค้ารายใดหลงเชื่อใส่รหัสผ่านลงไปในเว็บดังกล่าว คนร้ายก็จะนำรหัสผ่านที่ได้ไปใช้เข้าเว็บจริงเพื่อโอนเงินออกจากบัญชีลูกค้าไปเข้าบัญชีของคนร้ายหรือโอนเงินไปชำระค่าบริการโทรศัพท์มือถือในระบบเติมเงิน ซึ่งผลเสียหายที่เกิดขึ้นคิดเป็นมูลค่าหลายสิบล้านบาท โดยต้นตอของการสร้างเว็บไซต์นั้น ตำรวจสืบทราบว่ามาจากประเทศเบลเยียมและฝรั่งเศส และจากการตรวจสอบของสมาคมธนาคารไทย พบว่า คดีดังกล่าวเป็นคดีแรกที่เกิดขึ้นในประเทศไทย

ยังมีอีกหลายวิธีที่กลุ่มมิจฉาชีพใช้ในการขโมยข้อมูล เริ่มตั้งแต่การไม่ใช้เทคโนโลยีเป็นเครื่องมือเลย โดยใช้เทคนิคที่เรียกว่า Shoulder Surfing ซึ่งคนร้ายจะยืนอยู่ข้างหลังผู้ที่กำลังใช้เครื่องเอทีเอ็ม ทำเหมือนกับว่าเป็นนักท่องเที่ยว และคอยแอบดูรหัสของผู้ใช้ไม่ระมัดระวัง ซึ่งคนร้ายก็จะมีเทคนิคในการจำรหัสจากการกดปุ่มหน้าจอของผู้ใช้ โดยใช้วิธีการจำเสียงเนื่องจากเวลากดเอทีเอ็มจะมีเสียง และถ้าเหยื่อทิ้งสลิปเอทีเอ็มซึ่งมีเลขที่บัญชีธนาคารปรากฏอยู่ คนร้ายก็จะนำสลิปดังกล่าวมาใช้โดยโทรไปที่ธนาคารเพื่อโอนเงินผ่านทางโทรศัพท์ ซึ่งคนร้ายจะโอนออกจากบัญชีของเหยื่อที่ปรากฏอยู่ในสลิปและใช้รหัสประจำตัวแอบดูหรือจำได้ ซึ่งการโอนเงินทางโทรศัพท์สามารถโอนได้สูงสุดถึงครั้งละ 5 แสนบาท ดังนั้น เมื่อใช้เอทีเอ็ม ควรจะเก็บสลิปเอทีเอ็มเอาไว้กับตัว

คนร้ายอาจใช้เทคโนโลยีช่วยในการฉ้อโกง เช่น แอบติดตั้งกล้องถ่ายภาพขนาดเล็กมากไว้ในช่องเครื่องเอทีเอ็ม (เช่น กล่องใส่แผ่นพับโฆษณาข้างตู้เอทีเอ็ม) หรือใช้เครื่องมือซึ่งเป็นพลาสติกสวมครอบไปในช่องเสียบบัตรเพื่ออ่านรหัสบัตรเอทีเอ็ม หรือใช้กล้องสอดครอบแป้นกดรหัสเพื่อดูรหัสส่วนตัว และเมื่อเหยื่อกดรหัสส่วนตัวแล้วเงินไม่ออกมา ก็จะคิดว่าเครื่องมีปัญหา ไม่ได้คิดว่ามีการฉ้อโกงเกิดขึ้น หรือคนร้ายอาจจะใช้เทคนิคที่เรียกว่า Card Jamming นั่นคือ คนร้ายได้แก้เครื่องเสียบบัตรเอทีเอ็ม ทำให้เมื่อผู้ใช้เสียบบัตรเอทีเอ็มแล้ว ไม่สามารถนำบัตรเอทีเอ็มออกจากเครื่องได้ ซึ่งคนร้ายจะมาเก็บบัตรไปเมื่อลูกค้าไปแล้ว

อีกวิธีการหนึ่งที่คนร้ายนิยมใช้คือ การโทรศัพท์ไปแจ้งว่าเหยื่อเป็นผู้โชคดีได้รับรางวัล และขอให้เหยื่อตรวจสอบบัญชีได้เลยเพราะคนร้ายจะโอนเงินเข้าบัญชีให้ทันที และเมื่อเหยื่อกดเอทีเอ็มตรวจสอบแล้วพบว่ายังไม่มีเงินเพิ่มขึ้น คนร้ายก็แจ้งว่าอาจมีการผิดพลาดและขอให้เหยื่อทำตามขั้นตอนการตรวจสอบใหม่ตามที่คนร้ายบอก ซึ่งคนร้ายจะให้เหยื่อทำรายการโดยให้กดเมนูเลือกภาษาอังกฤษ และกดหมายเลขต่างๆ ตามขั้นตอนที่คนร้ายบอกเพื่อตรวจสอบว่าเงินเข้าบัญชีแล้วหรือยัง ซึ่งก็ไม่น่าแปลกใจที่ว่า เมื่อตรวจสอบครบตามขั้นตอนที่คนร้ายบอกแล้ว เงินของเหยื่อก็ถูกโอนไปยังบัญชีของคนร้ายเกือบหมดบัญชี

จากวิธีการฉ้อโกงที่หลากหลาย สถาบันการเงินต่างพยายามคิดหาวิธีสร้างความปลอดภัยให้กับการใช้บัตรเครดิตและเอทีเอ็ม เช่น บางธนาคารมีบริการแจ้งรายการใช้จ่ายบัตรเครดิตและบัตรเดบิตทุกชนิดของธนาคารผ่านระบบ SMS ไปยังโทรศัพท์มือถือของผู้ถือบัตรในทันทีที่มีการใช้จ่ายผ่านบัตร ซึ่งผู้ถือบัตรสามารถแจ้งขออายัดการใช้บัตรได้ทันทีที่ได้รับการแจ้งเตือนจากระบบ SMS ถึงรายการที่ตนไม่ได้ทำ บางธนาคารเริ่มติดชิปความจำสูงใน

บัตรเครดิตสามารถบรรจุข้อมูลได้มากกว่าแถบแม่เหล็กที่ใช้กันแต่เดิม และมีประสิทธิภาพในการรักษาความปลอดภัยข้อมูลแก่ผู้ถือบัตรที่สูงขึ้นด้วยการเข้ารหัสหลายชั้น ทำให้ยากต่อการปลอมแปลง นอกจากนี้ ข้อมูลจากจุลสารระบบการชำระเงินของธนาคารแห่งประเทศไทย ประจำเดือนกันยายน 2550 เปิดเผยว่า สถาบันการเงินใหญ่ๆ เช่น CITI Group ได้นำเทคโนโลยีไบโอเมตริก (Biometric) มาใช้ร่วมกับบัตรเครดิตในประเทศสิงคโปร์ ลูกค้าสามารถชำระเงินผ่านระบบไบโอเมตริกร่วมกับบัตรเครดิต โดยลูกค้าที่รับบริการจะต้องสแกนลายนิ้วมือด้วยเครื่องสแกนเนอร์ Pay by Touch ข้อมูลที่ได้จากการสแกนจะเชื่อมโยงกับข้อมูลในบัตรสมาชิกของลูกค้า และจะถูกนำไปเข้ารหัสเพื่อรักษาความปลอดภัยโดยมีโปรแกรมที่ควบคุมความปลอดภัยของข้อมูลที่ได้จากการสแกน ซึ่งไม่สามารถถอดรหัสไปทำเป็นลายนิ้วมือปลอมได้ เมื่อลูกค้าจะชำระเงินก็จะต้องกดนิ้วมือลงบนเครื่องอ่านซึ่งเชื่อมต่อกับระบบ POS (Point of Sales) และพิมพ์รหัสผ่านที่ลูกค้าได้กำหนดไว้เพื่อยืนยันว่าเป็นบุคคลนั้นจริง จากนั้น ขั้นตอนก็จะเป็นเช่นเดียวกับการชำระเงินทั่วไป

อย่างไรก็ตาม มาตรการป้องกันหลากหลายที่คิดขึ้นมาจะไม่ได้ผลเลย ถ้าผู้ใช้บัตรเครดิตและเอทีเอ็มไม่มีความระมัดระวัง ผู้ที่มีบัตรเครดิตไม่ควรคิดว่าเป็นเพียงบัตรพลาสติก แต่ควรจะระวังเหมือนกับการมีเงินสดในครอบครอง ก่อนกดเอทีเอ็ม ลองสังเกตรอบๆ ดูก่อนว่ามีสิ่งใดน่าสงสัยหรือไม่ เอกสารที่มีข้อมูลทางการเงินต่างๆ เช่น สลิปบัตรเครดิต สลิปจากตู้เอทีเอ็ม ควรจะทำลายก่อนที่จะทิ้ง ใช้อินเทอร์เน็ตด้วยความระมัดระวังก่อนที่จะกรอกข้อมูลใดๆ ถ้าได้รับอีเมล์ที่อ้างว่ามาจากธนาคารหรือสถาบันการเงินให้ระวังไว้ก่อน เพราะปกติแล้วธนาคารจะไม่มีนโยบายในการสอบถามข้อมูลส่วนตัว ข้อมูลบัญชี รหัสผ่านหรือ PIN ผ่านทางอีเมล์ หรืออย่ากดลิงค์ที่ปรากฏในอีเมล์ ใช้โปรแกรมป้องกันไวรัสและอัพเดทฐานข้อมูลไวรัส (DAT Files) อย่างสม่ำเสมอ เพราะไวรัสบางประเภทสามารถเปลี่ยนที่อยู่เว็บไซต์ที่เราคีย์ลงไปและนำเราไปสู่เว็บไซต์ปลอมที่มีลักษณะเหมือนกันได้ และที่สำคัญ อย่าหลงดีใจเมื่อมีผู้โทรมาบอกว่าเราถูกรางวัลใหญ่ พึงจำไว้ว่าในโลกนี้ไม่มีสิ่งใดที่ได้มาฟรีๆ