

## เจาะข้อมูล 'บัตรเครดิต'

### ภัยร้ายที่ทวีความรุนแรง!!

ธนาคารและสถาบันการเงินพัฒนาเทคโนโลยีป้องกันให้ทันเหล่ามิจฉาชีพ ที่พยายามพัฒนากลวิธีขโมยข้อมูลบัตรเครดิตของผู้เคราะห์ร้ายอย่างต่อเนื่อง เช่นเดียวกับผู้ใช้บัตรเครดิตในประเทศเพิ่มขึ้นอย่างต่อเนื่อง สวนทางกับความรู้ของผู้ใช้ที่วันนี้หลายคนยังไม่รู้ถึงวิธีป้องกันจากเหล่า "แฮกเกอร์ทั่วโลก" ซึ่งพร้อมเจาะข้อมูลเมื่อมีโอกาส



นอกจากนี้ยังมีข้อสังเกต ของผู้เชี่ยวชาญเกี่ยวกับร้านค้าที่กระตุ้นยอดขายด้วยการเก็บ ข้อมูลบัตรเครดิตของลูกค้า เพื่อทำการตลาด โดยหากไม่มีการป้องกันลูกค้าอาจตกเป็นเหยื่ออย่าง "หวานหมู" ไม่ต่างจากนักช้อปปิ้งบนโลกไซเบอร์ ที่กรอกข้อมูลบัตรเครดิตเพื่อซื้อของในอินเทอร์เน็ต เสี่ยงตกเป็นเหยื่อของ "แฮกเกอร์ทั่วโลก" ไม่แน่ว่าครั้งต่อไปอาจหนีท่วมไม่รู้ตัว

เพื่อความไม่ประมาท ดร.โกเมน พิบูลย์โรจน์ ผู้อำนวยการโปรแกรมเทคโนโลยี เพื่อความมั่นคง ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ เล่าถึงสถานการณ์ของบรรดานักเจาะข้อมูลบัตรเครดิตว่า ตอนนี้มีจลาจลทั่วโลกมีการแข่งขันเพื่อเจาะข้อมูลบัตรเครดิตอย่างแพร่หลาย เพราะเป็นแหล่งข้อมูลที่ขโมยง่าย เปรียบเสมือนกุญแจบ้านที่ไม่ว่าใครได้ไปก็สามารถเข้าไปข้างในได้ทันที



วิธีการเจาะข้อมูลของมิจฉาชีพมี 2 วิธีคือ 1.เจาะข้อมูลผ่านระบบอินเทอร์เน็ต ด้วยการเจาะไปที่ฐานข้อมูลเว็บไซต์ที่ขายของบนอินเทอร์เน็ต ซึ่งเก็บรวบรวมรหัสบัตรเครดิตของลูกค้าไว้ เมื่อได้ข้อมูล "แฮกเกอร์" สามารถนำรหัสไปขายต่อหรือใช้ซื้อของ ในเว็บไซต์ต่าง ๆ วิธีการนี้ ส่วนใหญ่คนร้ายมักเป็นคนต่างประเทศที่ต้องการรหัสบัตรที่ละมาก ๆ และตามจับได้ยากเพราะอยู่คนละประเทศ

บางกรณีคนร้ายโทรฯ หาเหยื่ออ้างว่า รหัสบัตรเครดิตมีปัญหาและให้เข้าเว็บไซต์ที่ คนร้ายปลอมแปลงขึ้น ซึ่งมีความคล้ายคลึงกับหน้าเว็บของสถาบันการเงิน และหลังจากกรอกข้อมูลคนร้ายจะนำรหัสไปซื้อของบนอินเทอร์เน็ต

"ผู้ที่ชอบซื้อของผ่าน อินเทอร์เน็ต หากคอมพิวเตอร์หาย ตกไปอยู่ในมือมิจฉาชีพสามารถเข้าไปในหน้าเว็บที่กรอกข้อมูลบัตรเครดิต โดยนำข้อมูลเหล่านั้นไปซื้อของผ่าน เครือข่ายอินเทอร์เน็ต หรือการส่งเอสเอ็มเอสรหัสบัตรผ่าน มือถือไปยังผู้ประกอบการเพื่อร่วมโปรโมชั่น ข้อมูลบัตรจะ อยู่ในกล่องส่งข้อความ เมื่อโทรศัพท์หายคนร้ายสามารถนำไปใช้ผ่านอินเทอร์เน็ตได้ทันที บางกรณีอาจใช้กล้องมือถือถ่ายภาพหน้าบัตรและหลังบัตรเพื่อนำข้อมูลไปปลอมแปลงได้"

วิธีที่ 2 คือ ก๊อบปี้แถบแม่เหล็กบัตรโดยตรง ที่แพร่ระบาดอย่างมากในประเทศ โดยผู้ใช้บัตรใช้ซื้อสินค้า และต้องรูดบัตรผ่านเครื่องบันทึกข้อมูลหรือ "สแกนเนอร์" มิจฉาชีพจะร่วมมือกับพนักงานในการก๊อบปี้ข้อมูลแถบแม่เหล็ก และเมื่อได้มาสามารถก๊อบปี้ใส่บัตรเครดิตเปล่า ได้ทันที คนร้ายจะก๊อบข้อมูลครั้งละหลาย ๆ ใบ และปลอมแปลงเซ็นผู้ใช้ก่อนเหยื่อรู้ตัว

ต่อด้านหลัง

นอกจากนี้บางร้านค้าเก็บข้อมูลการใช้ของผู้ใช้บัตรเครดิต โดยให้ลูกจ้างรูดบัตรเครดิต 2 ครั้ง ครั้งที่ 1 รูดเพื่อจ่ายสินค้า รูดครั้งที่ 2 เก็บข้อมูลลูกค้า โดยไม่สามารถรู้ได้เลยว่า ผู้ประกอบการได้นำข้อมูลอะไรไปบ้าง แต่หากมีการทุจริตเกิดขึ้นด้วยการเจาะฐานข้อมูลลูกค้า อาจก่อให้เกิดความเสียหายต่อลูกค้าได้



“สิ่งที่น่าเป็นห่วง คือ ผู้ใช้บัตรเครดิตมักทิ้งสลิปการใช้งานทันที เสี่ยงต่อการลักขโมยได้ เพราะหากมีจาชิปมีความใกล้เคียงกับผู้ใช้สามารถเดารหัสบัตรที่ไม่เปิดเผยในสลิปได้ โดยนำเอาข้อมูลไปซื้อสินค้าผ่านระบบอินเทอร์เน็ต”

ดร.โกเมน แนะนำวิธีการป้องกันว่า ผู้ใช้บัตรเครดิตต้องใช้โดยให้อยู่ในสายตาเสมอ อย่าให้ร้านค้านำบัตรไปรูดในที่ไกลตา และควรเก็บสลิปหลังใช้งานทุกครั้ง เพื่อตรวจสอบกับสถาบันการเงินเมื่อถึงสิ้นเดือน หากไม่ใช้แล้วควรฉีกให้ละเอียดก่อนทิ้ง

สำหรับผู้ที่ใช้บัตรเครดิตในการซื้อสินค้าผ่านอินเทอร์เน็ตควรใช้บัตร ใบใดใบหนึ่งเพื่อป้องกันการถูก “แฮกเกอร์” และต้องหาระบบป้องกันกับสถาบันการเงินเพื่อไม่ให้ตกเป็นเหยื่อ ขณะเดียวกันไม่ควรใช้บัตรเครดิตในร้านค้าที่เจียมเหงา หรือร้านที่ไม่ น่าไว้วางใจ ตลอดจนสังเกตทางร้านไม่ให้รูดบัตรเครดิตเกิน 1 ครั้ง

“อนาคตเป็นเรื่องที่น่าเป็นห่วงเพราะผู้ใช้บัตรเครดิตในประเทศหลายคน ยังไม่มีความรู้ แต่มีจาชิปทั่วโลกพร้อมที่จะเจาะข้อมูลทุกเมื่อ”

ด้าน พ.ต.ท.พันชนะ นุชนารถ รอง ผกก.1 บก.ทท. และเลขาฯ ศูนย์สืบสวนปราบปรามคนร้ายข้ามชาติและอาชญากรรมบัตรอิเล็กทรอนิกส์ เล่าถึงสถานการณ์ว่า ตอนนีการปลอมแปลงบัตรเครดิตน้อยลงหลังเจ้าหน้าที่บุกทำลายแก๊งต่างชาติรายใหญ่ที่ลักลอบปลอมแปลง ล่าสุดการปลอมบัตรเครดิตจากจีนเข้ามามากขึ้น ตอนนี้อยู่ในขั้นตรวจสอบกับทางการจีนว่า เกี่ยวข้องกับมีจาชิปที่หลอกหลวงคืนภาษีหรือไม่

“การควบคุมแก๊งเหล่านี้ค่อนข้างยาก เนื่องจากสก็มเมอร์มีชายอยู่ทั่วไปตามร้านไอทีต่าง ๆ โดยคนร้ายสามารถนำมาดัดแปลงเพื่อกอบขโมยข้อมูลได้ ขณะเดียวกันการขโมยข้อมูล บัตรเอทีเอ็มก็ไม่ต่างกันมากนัก”

นอกจากนี้ร้านค้าที่เก็บข้อมูลบัตรเครดิตของลูกค้าสามารถทำได้หากไม่ทำให้ลูกค้าเดือดร้อน และควรมีโปรแกรมป้องกัน เพราะข้อมูลของลูกค้าถือว่าเป็นความลับสูงสุด หากมีการรั่วไหลผู้ประกอบการอาจมีความผิดได้

สำหรับการป้องกันไม่ให้ตกเป็นเหยื่อของแก๊งปลอมบัตรเอทีเอ็ม ผู้ใช้ไม่ควรฝากผู้อื่นกดเงิน สั่งเกตบริเวณช่องใส่บัตร หากมีความผิดปกติ ไม่ควรกด ขณะกรรหัสบัตรต้องเอามือป้องเพื่อไม่ให้คนด้านหลังหรือกล้องที่คนร้ายแอบซ่อนไว้

ช่วงนี้เศรษฐกิจไม่ดี ประชาชนเองต้องมีความรู้ในการใช้บัตรต่าง ๆ เพราะจะมีบรรดาสถาบันการเงินมาช่วยเหลืออย่างเดียวไม่ได้ แต่หากผู้ใช้มีความรู้เบื้องต้นก็สามารถยับยั้งได้เช่นกัน

แม้ไม่ใช่เรื่องใหม่สำหรับ สังคมไทย แต่เหล่ามีจาชิป ก็มีการพัฒนาอยู่ตลอดเวลา ดังนั้นผู้ใช้บัตรเครดิตก็ไม่ควรประมาท.

## ศราวุธ ดีหมื่นไวย์

ที่มา :

<http://www.dailynews.co.th/newstartpage/index.cfm?page=content&categoryId=486&contentId=8332&highlight=เจาะข้อมูลบัตรเครดิต>