กลโกงบัตรต่าง ๆ

บัตรอิเล็กทรอนิกส์ เช่น บัตรเครดิต บัตรเดบิต บัตรกดเงินต่าง ๆ เป็นบัตรที่อำนวยความสะดวกในการทำธุรกรรมทางการเงินของเจ้าของบัตร เช่น ถอนเงิน โอนเงิน ชำระเงิน ซึ่งบัตรเหล่านี้จะบันทึกข้อมูลส่วนตัวและข้อมูลทางการเงินของเจ้าของบัตรไว้ หากมิจฉาชีพเข้าถึงข้อมูลเหล่านี้ได้จากการขโมยบัตรหรือขโมยข้อมูลในบัตร มิจฉาชีพก็จะสามารถนำข้อมูลเหล่านี้ไปปลอมเป็นเจ้าของบัตรทำธุรกรรมทางการเงินต่าง ๆ ไม่ว่าจะถอนเงินออกจากบัญชี หรือใช้วงเงินสินเชื่อของเหยื่อที่เป็นเจ้าของบัตร

ลักษณะกลโกง

1.คัดลอกข้อมูลจากแถบแม่เหล็กของบัตรโดยเครื่องสกิมเมอร์ (Skimmer) ที่ติดตั้งไว้ที่ตู้เอทีเอ็ม

มิจฉาชีพมักติดตั้งเครื่องสกิมเมอร์ที่ช่องเสียบบัตรของตู้เอทีเอ็ม เพื่อคัดลอกข้อมูลจากบัตร พร้อมติดตั้งแป้นครอบกดตัวเลขเพื่อบันทึกรหัสผ่านที่เหยื่อกด หรืออาจติดตั้งกล้องจิ๋วเพื่อแอบดูรหัสผ่าน

2. คัดลอกข้อมูลจากแถบแม่เหล็กของบัตรโดยเครื่องสกิมเมอร์ขนาดพกพาหรือเครื่องแฮนด์เฮลด์สกิมเมอร์ (Handheld Skimmer)

แฮนด์เฮลด์สกิมเมอร์เป็นเครื่องคัดลอกข้อมูลในแถบแม่เหล็กขนาดเล็กที่สามารถพกพาได้ ซึ่งมิจฉาชีพมักจะถือไว้ในฝ่ามือ และนำบัตรของเหยื่อมารูดพร้อมทั้งดูรหัสปลอดภัยจากด้านหลังบัตรโดยไม่ให้เหยื่อสังเกตเห็น ซึ่งอาจเกิดขึ้นที่ใดก็ได้ ไม่ว่าจะเป็นร้านค้า ร้านอาหาร สถานีบริการน้ำมัน หรือมิจฉาชีพอาจแอบอ้างเป็นเจ้าพนักงานธนาคารยื่นหน้าตู้เอทีเอ็ม ขอดูบัตรของเหยื่อ หรืออาจทำทีเสนอความช่วยเหลือแก่เหยื่อหากบัตรติดตู้เอทีเอ็ม แล้วคัดลอกข้อมูลผ่านเครื่องแฮนด์เฮลด์สกิมเมอร์เมื่อเหยื่อเผลอ

3. ปลอมแปลงเอกสารสมัครบัตรเครดิต

มิจฉาชีพอาจปลอมแปลงหรือใช้เอกสารส่วนตัวของเหยื่อ เช่น สำเนาบัตรประชาชนที่ได้ขโมยมา แล้วนำไปใช้สมัครบัตรเครดิต หรือแจ้งเปลี่ยนที่อยู่เปลี่ยนบัตร โดยแจ้งให้สถาบันการเงินส่งเอกสารและบัตรที่ออกใหม่ให้กับมิจฉาชีพโดยตรง เมื่อได้รับบัตรเครดิตก็นำไปใช้จ่ายในนามของเหยื่อ

4. ขโมยข้อมูลจากใบบันทึกรายการ (ATM Slip)

มิจฉาชีพจะเก็บใบบันทึกราย (ATM Slip) ตามตู้เอทีเอ็มที่มียอดคงเหลือค่อนข้างมากไปใช้ค้นหาข้อมูลสำคัญ ๆ ในการทำธุรกรรมทางการเงิน เช่น วันเดือนปีเกิด หมายเลขบัตรประชาชน โดยใช้วิธีที่แตกต่างกันออกไป เช่น แอบอ้างเป็นข้าราชการไปขอข้อมูลทะเบียนราษฎรจากเจ้าหน้าที่ฝ่ายปกครอง หรือค้นหาเลขที่บัญชีให้ครบ 10 หลักแล้วนำไปทดลองโอนผ่านธนาคารออนไลน์เพื่อให้ทราบชื่อเจ้าของบัญชี

เมื่อได้ข้อมูลของเหยื่อแล้ว มิจฉาชีพจะปลอมแปลงบัตรประจำตัวราชการปลอมโดยใช้ชื่อของเหยื่อเป็นเจ้าของบัตรแต่ติดรูปภาพของมิจฉาชีพ

แล้วนำบัตรดังกล่าวไปขอเปิดบัญชีเงินฝากและทำบัตรเอทีเอ็มใหม่ของธนาคารเดียวกันแต่คนละสาขา พร้อมทั้งขอเปิดใช้บริการธนาคารออนไลน์กับทุกบัญชีเงินฝากของเหยื่อ เพื่อโอนเงินทั้งหมดไปที่บัญชีเงินฝากที่เปิดใหม่ แล้วใช้บัตรเอทีเอ็มถอนเงินออกไป

ข้อควรสังเกต

01

เครื่องสกิมเมอร์

มิจฉาชีพจะติดตั้งเครื่องดังกล่าวไว้ที่ตู้เอทีเอ็ม ดังนั้น มิจฉาชีพมักจะเลือกตู้เอทีเอ็มในบริเวณที่มีคนไม่พลุกพล่าน ง่ายต่อการติดตั้ง

02

เครื่องแฮนด์เฮลด์สกิมเมอร์

มิจฉาชีพจะรูดบัตรของเหยื่อกับเครื่องแฮนด์เฮลด์สกิมเมอร์ ดังนั้น มิจฉาชีพจะต้องหลอกขอบัตรจากเหยื่อ

03

การปลอมแปลงเอกสาร

มิจฉาชีพจะต้องมีเอกสาร หรือข้อมูลส่วนตัวของเหยื่อ จึงจะสามารถสมัครบัตรในนามของเหยื่อได้

04

ขโมยข้อมูลจากใบบันทึกรายการตู้เอทีเอ็ม

มิจฉาชีพจะต้องมีใบบันทึกรายการ (Slip) ซึ่งมีข้อมูลบัญชีเงินฝากบางส่วนของเหยื่อไปหาข้อมูลเพิ่มเติม

วิธีป้องกัน

1. รหัสผ่านของบัตรควร

- เป็นรหัสผ่านที่ยากต่อการคาดเดา แต่เจ้าของบัตรต้องจำได้
- ไม่จดรหัสผ่านไว้คู่กับบัตร หรือในที่ที่ผู้อื่นสามารถเข้าถึงได้
- ไม่ใช้รหัสผ่านที่สถาบันการเงินส่งมาให้ และควรทำลายเอกสารแจ้งรหัสผ่าน
- เปลี่ยนรหัสอย่างน้อยทุก 3 เดือนหรือบ่อยกว่า
- เก็บรักษารหัสผ่านเป็นความลับ และไม่ควรให้ข้อมูลส่วนตัวหรือข้อมูลทางการเงินแก่ผู้อื่น

2. ก่อนใช้งานตู้เอทีเอ็มควร

- หลีกเลี่ยงการใช้ตู้เอทีเอ็มในสถานที่เปลี่ยว เพราะมีโอกาสที่มิจฉาชีพจะติดตั้งเครื่องคัดลอกข้อมูลไว้ได้โดยง่าย
- สังเกตช่องเสียบบัตร แป้นกดตัวเลข หรือบริเวณตู้เอทีเอ็ม ว่ามีสิ่งผิดปกติ เช่น แป้นครอบตัวเลข กล่องหรืออุปกรณ์ที่ติดไว้ในระยะมองเห็นการกดรหัสหรือไม่

3. หากใช้บัตรกับร้านค้าควร

- หลีกเลี่ยงร้านค้าที่มีความเสี่ยงที่จะเกิดการทุจริต เช่น สถานบริการน้ำมัน สถานบันเทิง
- ควรอยู่ในบริเวณที่มองเห็นการทำรายการ และให้บัตรอยู่ในสายตาตลอดเวลา เพื่อป้องกันพนักงานนำบัตรไปรูดกับเครื่องสกิมเมอร์

4. เมื่อใช้งานบัตรควร

- ใช้มือปิดบังไม่ให้ผู้อื่นมองเห็นแป้นกด ในขณะที่กำลังกดรหัสผ่าน
- เก็บใบบันทึกรายการทุกครั้ง เพื่อเป็นหลักฐานในการตรวจสอบยอดการใช้จ่าย
- ตรวจสอบรายการใช้จ่ายหรือยอดเงินอย่างสม่ำเสมอ หากมีรายการผิดปกติ ให้แจ้งธนาคารหรือบริษัทผู้ออกบัตรเพื่อตรวจสอบและดำเนินการแก้ไข

5. ไม่ควรให้เอกสารข้อมูลส่วนตัว และข้อมูลทางการเงินแก่บุคคลอื่น

6. หากบัตรสูญหายหรือถูกขโมย ควรแจ้งธนาคารหรือบริษัทผู้ออกบัตรเพื่ออายัดบัตรทันที

7. ติดตามข่าวสารกลโกง เพื่อรู้เท่าทันกลโกงใหม่ ๆ

สิ่งที่ควรทำเมื่อตกเป็นเหยื่อ

1. เมื่อพบรายการถอนเงินหรือโอนเงินผิดปกติ ควรแจ้งอายัดบัตรทันที พร้อมตรวจสอบยอดเงินใช้จ่ายหรือยอดเงินคงเหลือกับเจ้าหน้าที่ธนาคารหรือบริษัทผู้ออกบัตร
2. แจ้งความต่อเจ้าหน้าที่ตำรวจ
3. ทำใจ...เพราะเงินที่ถูกมิจฉาชีพขโมยไป โอกาสจะได้คืนนั้นน้อยมาก โดยเฉพาะในกรณีที่มิจฉาชีพได้ข้อมูลบัตรเพราะความประมาทของผู้ถือบัตร ทั้งนี้ กรณีที่เป็นการ skimming ที่ตู้เอทีเอ็มของธนาคารจริง ธนาคารจะชดใช้เงินให้แก่ลูกค้าที่ได้รับความเสียหาย

ข่าวกลโกงที่เกี่ยวข้อง

คลิ่ปมปริศนา CSI THAILAND: ไขคดี!แก๊งฉกเงินผ่านอินเทอร์เน็ต ล้วงข้อมูลแบงก์จากสลิปเอทีเอ็ม

คำถามถามบอย Q. A.

Q. หากพบตู้เอทีเอ็มที่สงสัยว่ามีเครื่องสกิมเมอร์ติดตั้งไว้ ควรทำอย่างไร

A. ไม่ใช้ตู้เอทีเอ็มนั้น และติดต่อสถาบันการเงินเจ้าของตู้เอทีเอ็ม เช่น สาขาใกล้เคียง หรือฝ่ายบริการลูกค้า (call center) เพื่อตรวจสอบ และขอปรึกษาวิธีใช้งานที่ปลอดภัย

Q. หากพบยอดถอนเงิน/โอนเงิน/ยอดการใช้จ่ายผ่านบัตรที่ผิดปกติ ควรทำอย่างไร

A. ติดต่อฝ่ายบริการลูกค้าของสถาบันการเงินนั้น เพื่อสอบถามข้อเท็จจริงเกี่ยวกับยอดเงินที่ผิดปกติ และหากพบว่าเป็นรายการที่เจ้าของบัตรไม่ได้เป็นผู้กระทำ ควรแจ้งอายัดบัตรทันที

ผู้จัดการบริการ ทีมกลยุทธ์ ศคง.