ธนาคารแห่งประเทศไทย

แถลงข่าวร่วม

ธนาคารแห่งประเทศไทยและสมาคมธนาคารไทย ชี้แจงกรณีผู้เสียหายร้องเรียน จากเหตุการใช้งานสายชาร์จปลอมแล้วถูกดูดข้อมูลและโอนเงินออกจากบัญชี

ตามที่ปรากฏข่าวพบผู้เสียหายจากการใช้งานสายชาร์จปลอมแล้วถูกดูดข้อมูลและโอนเงินออกจากบัญชีนั้น ธนาคารแห่งประเทศไทย (ธปท.) ได้หารือสมาคมธนาคารไทย เพื่อตรวจสอบกรณีดังกล่าวแล้ว พบว่ามิได้เกิดจากการใช้งานสายชาร์จปลอม แต่เกิดจากผู้เสียหายถูกมิจฉาชีพหลอกลวงให้ติดตั้งแอปพลิเคชันปลอมที่แฝงมัลแวร์ ทำให้มิจฉาชีพล่วงรู้ข้อมูลการทำธุรกรรมของลูกค้า และควบคุมเครื่องโทรศัพท์เพื่อสวมรอยทำธุรกรรมแทนจากระยะไกล เพื่อโอนเงินออกจากบัญชี โดยอาจเลือกทำธุรกรรมในช่วงเวลาที่ผู้เสียหายไม่ได้ใช้งานโทรศัพท์

ปัจจุบัน มิจฉาชีพมีวิธีหลอกลวงหลายรูปแบบ อาทิ SMS หลอกลวง แก๊งคอลเซ็นเตอร์ และแอปพลิเคชันให้สินเชื่อปลอม เป็นต้น และมีการปรับเปลี่ยนอย่างต่อเนื่อง โดยล่าสุดใช้การหลอกลวงให้ติดตั้งแอปพลิเคชันปลอมที่แฝงมัลแวร์ ซึ่ง ธปท. ได้ดำเนินการเพื่อป้องกันและแก้ไขปัญหา โดยการออกมาตรการต่างๆ ให้สถาบันการเงินต้องปฏิบัติ และร่วมกับกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงาน กสทช. สำนักงาน ปปง. และสำนักงานตำรวจแห่งชาติ เพื่อดำเนินการต่าง ๆ ได้แก่

- ปรับปรุงพัฒนาระบบรักษาความปลอดภัยบน Mobile Banking อย่างต่อเนื่อง
- ปิดกั้นเว็บไซต์หลอกลวง และตัดการเชื่อมต่อกับเครื่องคอมพิวเตอร์ที่มิจฉาชีพใช้ควบคุมเครื่องผู้เสียหายจากระยะไกล
- แก้ไขปัญหา SMS หลอกลวง ที่แอบอ้างชื่อเป็นสถาบันการเงิน
- จัดให้มีช่องทางการรับแจ้งความออนไลน์เพื่อให้ประชาชนแจ้งความได้สะดวกและอายัดบัญชีได้รวดเร็วขึ้น
- ประชาสัมพันธ์สร้างการตระหนักรู้ แจ้งเตือนภัย และให้คำแนะนำประชาชนอย่างต่อเนื่อง

อย่างไรก็ตาม สถาบันการเงินจำเป็นต้องพัฒนาเครื่องมือและการตอบสนองให้เท่าทันอย่างสม่ำเสมอ รวมทั้งการพัฒนากลไกความร่วมมือกับผู้ที่เกี่ยวข้องทั้งหน่วยงานภาครัฐและเอกชนให้มีประสิทธิภาพมากขึ้น

และขอความร่วมมือจากประชาชนเพิ่มความระมัดระวัง เพื่อมิให้ตกเป็นเหยื่อมิจฉาชีพ โดยสามารถป้องกันภัยในเบื้องต้นได้ ดังนี้

1. ไม่คลิกลิงก์จาก SMS LINE และ อีเมลที่มีแหล่งที่มาที่ไม่รู้จักหรือไม่น่าเชื่อถือ

2. ไม่ดาวน์โหลดโปรแกรม นอกเหนือจากแหล่งที่ได้รับการควบคุมและรับรองความปลอดภัยจากผู้พัฒนาระบบปฏิบัติการที่เป็น Official Store อาทิ Play Store หรือ App Store เท่านั้น

3. อัปเดต Mobile Banking ให้เป็นเวอร์ชันล่าสุดอยู่เสมอ หรือตั้งค่าให้มีการอัปเดตแบบอัตโนมัติ ซึ่งจะมีมาตรการป้องกันการควบคุมเครื่องทางไกลรวมถึงมีการปรับปรุงพัฒนาระบบรักษาความมั่นคงปลอดภัยอย่างสม่ำเสมอ

4. ไม่ใช้เครื่องโทรศัพท์มือถือที่ไม่ปลอดภัยมาทำธุรกรรมทางการเงิน อาทิ เครื่องที่ปลดล็อก (root/jailbreak) เพื่อให้สามารถติดตั้งแอปพลิเคชันใด ๆ ก็ได้ หรือใช้เครื่องที่มีระบบปฏิบัติการล้าสมัย เป็นต้น

5. ร่วมมือกับหน่วยงานที่เกี่ยวข้องในการให้ข้อมูลที่ถูกต้อง เพื่อให้การติดตามแก้ไขปัญหาเป็นไปอย่างรวดเร็ว และหากลูกค้าธนาคารพบธุรกรรมผิดปกติ สามารถติดต่อคอลเซ็นเตอร์หรือสาขาของธนาคารที่ลูกค้าใช้งาน เพื่อแจ้งตรวจสอบและยืนยันความถูกต้องของธุรกรรมในทันที โดยธนาคารจะดูแลแก้ไขปัญหาที่เกิดขึ้นโดยเร็วที่สุด

ทั้งนี้ ธปท. ได้เน้นย้ำให้สถาบันการเงินมีมาตรการดูแลลูกค้าทุกรายอย่างเต็มที่ตามขั้นตอนปฏิบัติที่กำหนด ซึ่งหากได้ตรวจสอบและพิสูจน์พบว่าลูกค้าไม่มีส่วนเกี่ยวข้องในการให้ข้อมูลส่วนตัว สถาบันการเงินต้องรีบพิจารณาช่วยเหลือและดูแลความเสียหายของลูกค้าโดยเร็วภายใน 5 วัน

ธนาคารแห่งประเทศไทย
สมาคมธนาคารไทย
วันที่ 18 มกราคม 2566