คำแนะนำด้านความปลอดภัย

ตามที่ได้มีข่าวเกี่ยวกับลูกค้าที่ใช้บริการ Internet Banking ของธนาคารพาณิชย์ตกเป็นเหยื่อของมิจฉาชีพโดยผู้ไม่หวังดีจะปลอมอีเมล (E-Mail) และส่งไปยังลูกค้า ทำให้ลูกค้าหลงเชื่อว่าธนาคารส่งอีเมล (E-Mail) ไปให้ลูกค้าเพื่อดำเนินการอย่างใดอย่างหนึ่ง โดยให้คลิกลิงค์ (Click Link) เพื่อเข้าสู่เว็บไซต์ (Website) ซึ่งมีหน้าเว็บเพจ (Webpage) ที่คล้ายคลึงกับของธนาคาร เมื่อลูกค้าป้อนรหัสผู้ใช้งานและรหัสผ่านข้อมูลความลับนี้จะถูกดักจับโดยโปรแกรมที่ผู้ไม่หวังดีซ่อนไว้ แล้วจะนำข้อมูลที่ได้ไปทำธุรกรรมผ่านบัญชีลูกค้าที่ตกเป็นเหยื่อได้อย่างง่ายดายโดยที่ลูกค้าจะไม่รู้ตัว ซึ่งการหลอกลวงแบบนี้จะเข้าลักษณะที่เรียกว่า Phishing ซึ่งการหลอกลวงลักษณะนี้ขึ้นอยู่กับวิธีการใช้งานของลูกค้าเป็นสำคัญ

ดังนั้นเพื่อเป็นการป้องกันมิให้ลูกค้าของธนาคารตกเป็นเหยื่อของการหลอกลวงดังกล่าว จึงได้แนะนำวิธีการใช้งาน Internet Banking อย่างปลอดภัย ดังนี้

1. ไม่ควรทำรายการผ่านเครื่องคอมพิวเตอร์สาธารณะ เนื่องจากลูกค้าไม่สามารถทราบได้ว่าจะมีโปรแกรมอื่นใดแอบแฝงอยู่ภายในเครื่องคอมพิวเตอร์หรือไม่ ซึ่งหากลูกค้าไม่มีความระมัดระวังเพียงพอก็อาจทิ้งร่องรอยข้อมูลของลูกค้าไว้ในเครื่องคอมพิวเตอร์ได้ซึ่งทำให้มิจฉาชีพสามารถเข้ามาสืบค้นข้อมูลสำคัญได้

2. การเข้าสู่เว็บไซต์ (Website) ใด ๆ ควรใส่ข้อมูลที่อยู่ของเว็บไซต์ (Website) บนอินเทอร์เน็ต (URL) ด้วยตนเอง ไม่ควรคลิกลิงค์ (Click Link) ที่มากับอีเมล (E-Mail)

3. ควรตรวจทานชื่อเว็บไซต์ (Website) ก่อนทำรายการใด ๆ ว่าเป็นเว็บไซต์ (Website) ที่ต้องการเข้าถึงหรือไม่

4. ทุกครั้งที่ทำรายการที่มีการระบุข้อมูลสำคัญต่าง ๆ ผ่านเว็บไซต์ (Website) ต้องแน่ใจว่ากำลังทำรายการอยู่บนเว็บไซต์ (Website) ที่ปลอดภัย โดยสามารถตรวจสอบได้ว่าเว็บไซต์ (Website) ดังกล่าว ปลอดภัยหรือไม่ โดยให้พิจารณาจากช่องเบราว์เซอร์ (Browser) ซึ่งเว็บไซต์ (Website) ที่ปลอดภัยควรขึ้นต้นด้วย https:// ซึ่งแตกต่างจากเว็บไซต์ (Website) ทั่วไปที่ขึ้นต้นด้วย http:// นอกจากนี้ควรสังเกตสัญลักษณ์รูปกุญแจบริเวณด้านล่างของหน้าเว็บไซต์ (Website) ด้วย หากไม่พบสัญลักษณ์ดังกล่าวแสดงว่าการทำธุรกรรมผ่านเว็บไซต์ (Website) ดังกล่าวอาจไม่ความปลอดภัยเพียงพอ

5. ควรเก็บรักษารหัสผู้ใช้งาน (User ID) และรหัสผ่าน (Password) ไว้เป็นความลับ

6. หมั่นเปลี่ยนรหัสผ่าน (Password) อยู่เสมอและไม่ควรใช้รหัสผ่านที่บุคคลอื่นคาดเดาได้ง่าย

7. หลีกเลี่ยงการคลิกลิงค์ (Click Link) ที่แนบมากับอีเมล (E-Mail) แปลกปลอม อีเมล (E-Mail) ที่ไม่ทราบผู้ส่งหรืออีเมล (E-Mail) ที่ขอข้อมูลส่วนบุคคล เพราะอาจมีโปรแกรมสอดแนม (Spyware) แนบมากับลิงค์เหล่านั้นเพื่อโจรกรรมข้อมูล

8. ติดตั้งโปรแกรมป้องกันไวรัส (Anti-Virus) ที่ถูกลิขสิทธิ์และเชื่อถือได้โดยต้องทำการปรับปรุงให้เป็นปัจจุบัน (Update) อยู่เสมอและหมั่นตรวจจับไวรัส (Scan Virus) ในเครื่องคอมพิวเตอร์เป็นระยะ ๆ

9. ควรลบอีเมล (E-Mail) ที่น่าสงสัยว่ามีไวรัส (Virus) แนบมาและไม่เปิดแฟ้มข้อมูล (File) ที่แนบมากับอีเมล (E-Mail) ที่มาจากบุคคลไม่รู้จัก ตลอดจนแฟ้มข้อมูล (File) ที่ส่งด้วยโปรแกรม Chat ต่าง ๆ รวมทั้งหลีกเลี่ยงการดาวน์โหลดโปรแกรมหรือข้อมูลจากเว็บไซต์ (Website) ที่ไม่น่าเชื่อถือ

อย่างไรก็ตาม ธนาคารออมสินได้มีระบบป้องกันและรักษาความปลอดภัยระบบเครือข่ายในการให้บริการธนาคารทางอินเทอร์เน็ตอย่างปลอดภัยให้กับลูกค้าของธนาคารแล้ว และสุดท้ายนี้ธนาคารขอยืนยันอีกครั้งหนึ่งว่าธนาคารไม่มีนโยบายติดต่อลูกค้าเพื่อส่งลิงค์ให้กรอกข้อมูลสำคัญและรหัสส่วนตัวแต่อย่างใด

หากมีข้อสงสัยหรือต้องการข้อมูลเพิ่มเติมกรุณาติดต่อ Contact Center โทรศัพท์หมายเลข 0-2299-8668 E-Mail: ib.office@gsb.or.th