ข่าว สคบ.

สำนักงานคณะกรรมการคุ้มครองผู้บริโภค — สำนักนายกรัฐมนตรี

รู้ไว้ไม่โดน...โจรไซเบอร์หลอก

ทุกวันนี้การทำธุรกรรมการเงินผ่านช่องทางออนไลน์เป็นสิ่งที่เราคุ้นเคยกันดี เพราะมันสะดวกมากๆ ไม่ต้องเดินทางไปทำเรื่องที่ธนาคารเอง แต่ก็ยังเป็นอีกหนึ่งช่องทางที่มิจฉาชีพใช้หากินอีกด้วย โดยในช่วงนี้มีข่าว SMS ที่ส่งลิงค์ของธนาคารต่างๆ เพื่อหลอกให้เรากรอกข้อมูลต่างๆ รวมถึงรหัสผ่านบัญชีของเราแบบเนียนๆ จากนั้นจะทำการโอนเงินออกจากบัญชีของเราไป ซึ่งตอนนี้ก็มีข่าวออกมาว่าหลายๆ คนตกเป็นเหยื่อกันแล้ว

PHISHING คืออะไร?

Phishing (ฟิชชิ่ง) มาจากคำว่า Fishing ที่หมายถึงการตกปลา ซึ่งในที่นี้ก็คือการหลอกลวงประเภทหนึ่งที่จะใช้เว็บปลอมให้ผู้ใช้งานอย่างเราๆ ตกเป็นเหยื่อนั่นเอง โดยวิธีการที่เหล่ามิจฉาชีพใช้เพื่อหลอกพวกเราก็คือส่ง SMS หรืออีเมลปลอม สร้างสถานการณ์หลอกว่าตอนนี้บัญชีธนาคารของเรากำลังจะถูกปิด ถูกระงับ หรือมีปัญหาอื่นๆ จากนั้นจะให้กดเข้าลิ้งค์ของเว็บไซต์ธนาคาร (เว็บปลอม) ที่แนบมาด้วย เพื่อให้เรากรอกข้อมูลต่างๆ ลงไป ไม่ว่าจะเป็นเลขบัญชี, เลขบัตรประชาชน, วันเดือนปีเกิด ฯลฯ ถ้าหากว่าเราหลงกลกรอกข้อมูลลงไป ก็เป็นอันเสร็จโจร เพราะข้อมูลดังกล่าวจะถูกส่งกลับไปที่มิจฉาชีพเพื่อนำไปใช้เข้าบัญชีธนาคารของเราเพื่อทำการโอนเงินออกไปจนเกลี้ยง

ลักษณะของ SMS หรือ อีเมล ปลอม

สำหรับวิธีการสังเกตว่า SMS ที่ส่งมาเป็นข้อความจากธนาคารจริงๆ หรือเป็นข้อความจากมิจฉาชีพ ก็มีวิธีตรวจสอบเบื้องต้นตามนี้ 1) ไม่ระบุชื่อของผู้รับว่าส่งข้อความถึงใคร ๒) ข้อความที่เป็นภาษาไทยมีการใช้ภาษาแปลกๆ ในข้อความ 3) ข้อความที่ส่งมาจะเป็นลักษณะที่ทำให้เราตกใจ กังวล เช่น จะมีการปิดหรือล็อคบัญชีธนาคารของเรา 4) แนบลิงก์เว็บไซต์ให้กดเข้าไปเพื่ออ่าน และกรอกข้อมูล

เทคนิคง่ายๆ ในการตรวจสอบเว็บไซต์ปลอมเบื้องต้น

1) สังเกตจาก URL หรือที่อยู่ของเว็บไซต์นั้น ๆ เว็บไซต์ที่น่าเชื่อถือจะขึ้นต้นด้วย https:// เช่น เว็บไซต์ของธนาคารไทยพาณิชย์ คือ https://www.scb.co.th โดยเว็บไซต์ของสถาบันการเงินแทบทั้งหมดจะใช้ https:// เพื่อเพิ่มความปลอดภัยสำหรับข้อมูลบาง URL ก็สามารถบอกได้ว่าเว็บไซต์นั้นจดทะเบียนอยู่ในประเทศไหน เช่น https://www.scb.co.th ตัวอักษร th ด้านหลังสุดหมายถึง ประเทศไทย, sg = สิงคโปร์, uk = อังกฤษ

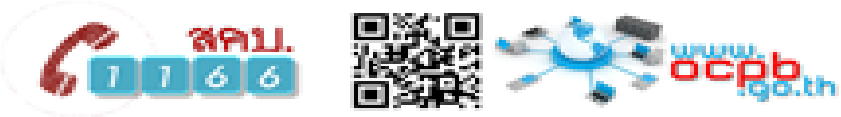
URL ที่เป็น .com .net หรืออื่น ๆ ถ้าหากไม่มั่นใจว่าเป็นของจริงหรือเปล่า เราสามารถเช็กข้อมูลเว็บไซต์นั้น ๆ ได้ที่ https://www.whois.com/whois/ ซึ่งสามารถบอกได้ว่าเว็บไซต์จดทะเบียนที่ไหน ใครเป็นเจ้าของ และถ้าหากเป็นเว็บไซต์จากต่างประเทศก็สงสัยไว้ก่อนเลยว่าเป็นของปลอม

2) มีการขอข้อมูลส่วนบุคคลที่มากเกินไปจนผิดปกติ อย่างเช่น เลขบัตรประชาชน, วันเดือนปีเกิด เพราะโดยทั่วไปจะขอแค่ ชื่อ-นามสกุล, อีเมล, หมายเลขโทรศัพท์เท่านั้น คลิกปุ่มเข้าใช้งานแล้วหน้าเว็บไม่ไปไหน ให้เรากรอกข้อมูลหลอกๆ แล้วลองกดส่งข้อมูลว่าเว็บไซต์นั้นจะไปที่หน้าไหนต่อ แต่ถ้าคลิกแล้วไม่ไปไหนยังวนอยู่หน้าเดิม ก็ตั้งข้อสงสัยไว้ได้เลย ว่าไม่น่าเชื่อถือและไม่ควรให้ข้อมูลใดๆ

3) ถ้าหากเราไม่มั่นใจในเว็บไซต์ที่ถูกส่งมา ให้ติดต่อเจ้าหน้าที่ของธนาคารก่อนเลย เพราะธนาคารต่าง ๆ ก็มีช่องทางการติดต่อที่สะดวกทั้ง Call Center หรือ Live Chat ทางเพจ Facebook สามารถสอบถามกันได้ทันที

4) ลบข้อความ SMS หรือ อีเมล น่าสงสัยทิ้งถ้าหากเราแน่ใจแล้วว่าเป็นของปลอม ถ้าหากเผลอให้ข้อมูลกับเว็บไซต์ปลอมไป ให้รีบติดต่อธนาคารทันที

ทั้งนี้ สคบ. ขอแนะนำทริคเพิ่มเติมในกรณีหากได้รับข้อความแปลกๆ แนบลิงก์มาด้วยให้ลองใส่รหัสผ่านปลอมไปก่อน ถ้าเข้าใช้งานได้แสดงว่าเป็นเว็บไซต์ปลอมถ้าหากใครที่เคยเจอข้อความ SMS หรือ อีเมลของมิจฉาชีพทำนองนี้ สามารถร้องเรียนได้ที่ ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย สายด่วน 1213 และหากผู้บริโภคที่ไม่ได้รับความเป็นธรรมจากการซื้อสินค้าและบริการ แจ้งที่สายด่วน สคบ. 1166 หรือเว็บไซต์ www.ocpb.go.th หรือ แอปพลิเคชันระบบร้องทุกข์ผู้บริโภค (OCPB Complain Mobile Application)



กองเผยแพร่และประชาสัมพันธ์ หมายเลขโทรศัพท์ ๐๒ ๑๔๑๓๔๗๐-๕ โทรสาร ๐๒ ๑๔๓ ๙๗๗๒-๓ E-mail : pr.ocpb@gmail.com