SCB ไทยพาณิชย์

ประกาศแจ้งเตือนให้ระวัง

ม้าโทรจัน/สปายแวร์ บุกขโมยข้อมูลส่วนตัว

ตามที่ขณะนี้ได้มีการพยายามสร้างเว็บไซต์และอีเมล์ลวง เพื่อโจรกรรมข้อมูลลูกค้าของระบบออนไลน์ต่างๆ ดังนั้นเพื่อความปลอดภัย และป้องกันเหตุการณ์ทุจริตที่อาจเกิดขึ้น หากท่านสงสัยว่าได้ทำรายการผ่านหน้าเว็บไซต์ที่เหมือนกับของธนาคาร โดยใช้ Link ผ่านจากอีเมล์หลอกลวงดังกล่าว ธนาคารฯ ใคร่ขอเสนอแนะให้ท่านผู้ใช้บริการระบบ SCB Business Net รีบดำเนินการเปลี่ยนแปลงรหัสผ่านของท่านในทันที

ธนาคารขอแจ้งให้ลูกค้าทุกท่านทราบว่า ธนาคารไม่มีนโยบายสอบถามข้อมูลลูกค้าผู้ใช้บริการ ด้วยวิธีดังกล่าว

ม้าโทรจัน คือ

โปรแกรมที่ซ่อนตัวอยู่ในฮาร์ดดิสก์ด้วยฝีมือของแฮคเกอร์ ที่อาจ**ส่งโค้ดแฝงมากับไฟล์แนบท้ายอีเมล** การทำงานของโทรจันก็เหมือนกับเรื่องเล่าของกรีก ที่ว่าด้วยกลอุบายซ่อนทหารไว้ในม้าไม้ขนาดใหญ่ และนำไปมอบให้กับชาวเมืองทรอย (**Trojans**) พอตกกลางคืน ทหารกรีก ที่ซ่อนตัวอยู่ในม้าไม้ก็ลอบออกมาเปิดประตูเมือง ให้พวกของตนบุกเข้าตีเมืองทรอยได้อย่างง่ายดาย **เปรียบได้กับแฮคเกอร์ที่ส่งโปรแกรมลึกลับ (ม้าโทรจัน) มาคอยดักเก็บข้อมูลในพีซีของคุณแล้วส่งออกไปโดยที่คุณไม่รู้ตัวนั่นเอง**

ม้าโทรจันในคอมพิวเตอร์ทำงานอย่างไร?

ม้าโทรจันแตกต่างจากไวรัสที่การทำงาน ไวรัสจะทำงานโดยทำลายคอมพิวเตอร์ ทั้งฮาร์ดแวร์และซอฟท์แวร์ แต่โทรจันจะไม่ทำอะไรกับคอมพิวเตอร์ ไม่มีคำสั่งหรือ พฤติกรรมการทำลายคอมพิวเตอร์เหมือนไวรัส โทรจันเป็นโปรแกรมทั่วไปในคอมพิวเตอร์ ไวรัสนั้นมีคำสั่งอันตราย แต่โทรจันไม่มี ดังนั้นโปรแกรมตรวจสอบไวรัสไม่มีทางที่จะตรวจสอบหาโทรจันพบ โทรจันเป็นเครื่องมือของแฮกเกอร์ในการเจาะระบบ เพราะ**โทรจันคือโปรแกรมที่เขียนขึ้นเพื่อบันทึกว่าแป้นคีย์บอร์ดแป้นไหนถูกกดบ้าง ด้วยวิธีการนี้ก็จะได้ข้อมูลของ User ID, Password** หลังจากนั้น โปรแกรมม้าโทรจันจะบันทึกข้อมูลลงไปใน RAM, CMOS หรือ Hidden Directory ในฮาร์ดดิสก์ แล้วก็หาโอกาสที่จะอัพโหลดตัวเอง ไปยังแหล่งที่ผู้เขียน ม้าโทรจันกำหนดหรือบางทีแฮกเกอร์อาจจะใช้วิธี การเก็บไฟล์ดังกล่าวไปด้วยวิธีอื่น **โทรจันบางตัวอันตรายมาก เพราะสามารถใช้คำสั่งในการรันคำสั่งอื่นเพื่อทำลายระบบหรือเปลี่ยนไฟล์ได้**

การป้องกัน

1. ระวังอีเมลที่มีข้อความชักจูงแปลกๆ หรืออีเมลที่มีลิงค์พิเศษที่ขอให้ใส่ Username หรือ Password โปรดอย่าคลิกลิ้งค์ใดๆ ที่มากับอีเมลแปลกปลอม และควรลบอีเมลนั้นทิ้ง และโทรแจ้ง SCB Call Center ที่ **02-722-2222**
2. เพื่อความปลอดภัย ควรพิมพ์ชื่อเว็บไซต์ที่ต้องการทำรายการด้วยตนเอง และตรวจทานชื่อเว็บไซต์ก่อนใส่ Username และ Password ทุกครั้ง
3. อย่าเปิดเผยข้อมูล Username, Password กับผู้ใดโดยเด็ดขาด ธนาคารไม่มีนโยบายสอบถามข้อมูลส่วนตัวลูกค้า ไม่ว่าช่องทางใดๆ ก็ตาม
4. ติดตั้งโปรแกรม Anti-virus ที่ถูกลิขสิทธิ์และเชื่อถือได้ ทำการปรับปรุงเป็นตัวล่าสุดอยู่เสมอ และหมั่น Scan ตรวจจับ Virusในเครื่องคอมพิวเตอร์เป็นระยะๆ
5. ควรลบอีเมลที่น่าสงสัยว่ามี Virus แนบมา และไม่เปิดไฟล์ที่แนบมากับอีเมลที่มาจากบุคคลที่ไม่รู้จัก ตลอดจนไฟล์ที่ส่งด้วยโปรแกรม Chat ต่างๆ รวมทั้งหลีกเลี่ยงการดาวน์โหลดโปรแกรม หรือข้อมูลจากเว็บไซต์ที่ไม่น่าเชื่อถือ