PUBLIC

อย่าตกเป็นเหยื่อของอาชญากรรมไซเบอร์!

มิจฉาชีพส่งอีเมลฟิชชิ่งมากกว่า 100 ล้านฉบับทุกวัน[1] คุณควรตื่นตัวและเรียนรู้วิธีป้องกันตัวเองและคนที่คุณรักจากอาชญากรรมไซเบอร์

ฟิชชิ่งคืออะไร?

ฟิชชิ่งเป็นอาชญากรรมทางไซเบอร์ที่มิจฉาชีพพยายามที่จะล่อลวงเพื่อให้ได้ข้อมูลส่วนบุคคลของคุณผ่านทางอีเมล, การรับส่งข้อความผ่านแอปพลิเคชัน, SMS (หรือที่เรียกว่า smishing) หรือทางโทรศัพท์ (ที่เรียกว่า vishing) มิจฉาชีพสามารถนำข้อมูลที่ได้จากการโจรกรรมนี้ ไปใช้เพื่อหลอกลวงการชำระเงิน และการฉ้อโกงบัตรเครดิตรวมถึงอาชญากรรมไซเบอร์ในรูปแบบอื่น ๆ ลิงก์หรือไฟล์แนบที่เป็นอันตรายมักรวมอยู่ในข้อความหลอกลวงฟิชชิ่งและวิชชิ่ง ซึ่งถูกออกแบบมาเพื่อล่อลวงโจรกรรมข้อมูลของคุณหรือทำให้ระบบของคุณติดมัลแวร์ (ซอฟต์แวร์ที่เป็นอันตราย)

PUBLIC

ใช้บริการธนาคารทีมีความปลอดภัยกับเรา

ข้อความฟิชชิ่งและวิชชิ่งอาจดูเหมือนว่าถูกส่งมาจากธนาคาร อาจมีตราสัญลักษณ์ของธนาคารหรือ แม้แต่ทำการลอกเลียนแบบจดหมายอิเล็กทรอนิกส์ของธนาคาร ท่านควรสังเกตที่อยู่อีเมลของผู้ส่งด้วยความระมัดระวัง เพื่อตรวจสอบให้ดีว่าเป็นโดนเมนที่ถูกต้องตรงกันหรือไม่ ตัวอย่างเช่น john@standardchartd.com

มิจฉาชีพอาจทำการส่งใบแจ้งยอดบัญชีธนาคารปลอม การแจ้งเบิกเงินเกินบัญชี หรือการยกเลิกเงินกู้ไปให้คุณ โปรดอย่าตอบอีเมลกลับ, ส่งข้อความหรือโทรศัพท์กลับไปยังผู้ที่ท่านไม่รู้จักหรือไม่ได้ร้องขอ ท่านสามารถเข้าเยี่ยมชมเว็บไซต์อย่างเป็นทางการของเรา เพื่อดูข้อมูลบริการธนาคารต่าง ๆ ได้ที่ https://www.sc.com/

สำหรับบริการธนาคารบนมือถือ ขอให้คุณปรับปรุง SC Mobile แอปพลิเคชั่น และระบบปฏิบัติการของโทรศัพท์ของคุณเป็นประจำ เพื่อให้แน่ใจว่าระบบรักษาความปลอดภัยที่คุณใช้งานอยู่ เป็นปัจจุบันอยู่เสมอ

หากคุณต้องการเปลี่ยนรหัสผ่าน โปรดใช้เว็บไซต์ [i-banking website] ของเรา โปรดอย่าคลิกที่ไฮเปอร์ลิงก์หรือดาวน์โหลดไฟล์แนบในอีเมล หรือข้อความที่คุณไม่ได้ร้องขอ

โดเมนอย่างเป็นทางการของธนาคารคือ sc.com

สแตนดาร์ดชาร์เตอร์ ไม่เคยทำการขอรหัส, รหัสผ่านครั้งเดียว (OTP) หรือหมายเลขบัตรเครดิตจากคุณ เพราะมันเป็นข้อมูลส่วนตัวและคุณไม่ควรเปิดเผยข้อมูลเหล่านี้กับใคร

โปรดระวัง หากคุณได้รับแจ้งจากผู้พยายามแอบอ้างหลอกลวง ว่าคุณได้รับรางวัลที่ไม่ได้คาดหวังจากการจับฉลาก จากธนาคารสแตนดาร์ดชาร์เตอร์ ซึ่งมิจฉาชีพอาจเรียกร้องผลประโยชน์จากคุณในรูปของเงิน หรือกระตุ้นล่อลวงให้คุณเปิดเผยข้อมูล

ส่วนบุคคลของคุณเพื่อให้คุณชนะในการจับฉลาก หากคุณมีข้อสงสัย สามารถโทรติดต่อ official hotline ของเราได้เสมอ เพื่อตรวจสอบความถูกต้อง

เรายินดีให้ความช่วยเหลือคุณ

หากคุณได้รับอีเมลที่น่าสงสัยจาก ธนาคารสแตนดาร์ดชาร์เตอร์ โปรดส่งอีเมลถึงเราและรายงานเหตุการณ์ดังกล่าวที่ be.secure@sc.com. โปรดติดต่อศูนย์บริการลูกค้าของเรา (Call Center hotline) ที่หมายเลขโทรศัพท์ 02-724-1553 ทันทีหากคุณสงสัยว่ามีผู้บุกรุกเข้าถึงบัญชีของคุณโดยไม่ได้รับอนุญาตหรือมีการทำธุรกรรมแปลกปลอมในบัญชีของคุณ เราจะดำเนินการเพื่อปกป้องบัญชีของคุณตามที่จะสามารถทำได้ ทั้งนี้ธนาคารอาจขอให้คุณช่วยจัดส่งเอกสารรายงานใบแจ้งความกับเจ้าหน้าที่ตำรวจหรือหน่วยงานที่บังคับใช้กฎหมายมาให้ด้วย

เราสามารถช่วยกันหยุดยั้งอาชญากรรมไซเบอร์ได้

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับฟิชชิ่งและวิชชิ่ง โปรดเข้าไปที่ https://www.sc.com/global/security-tips/

Here for good

โปรดอย่าตอบกลับอีเมลนี้

คุณไม่ควรส่งข้อมูลที่เป็นความลับและ / หรือข้อมูลสำคัญใด ๆ ไปยังธนาคารทางอีเมล เนื่องจากธนาคารไม่ได้รับรองหรือรับประกันเกี่ยวกับความปลอดภัยหรือความถูกต้องของข้อมูลที่คุณส่ง ธนาคารจะไม่รับผิดชอบต่อความสูญเสียหรือความเสียหายใด ๆ ที่เกิดขึ้นจากการที่คุณตัดสินใจใช้อีเมลเพื่อสื่อสารกับธนาคาร กรุณาให้ความสำคัญและพิจารณาให้ดีก่อนที่คุณจะตัดสินใจที่จะกระทำการใดๆ กับข้อมูลบนเว็บไซต์นี้หรือตอบกลับหรือส่งข้อมูลหรือเอกสารสำคัญใด ๆ ให้เราเพื่อตอบกลับจดหมายฉบับนี้ และคุณได้อ่านและทำความเข้าใจประกาศทางกฎหมายที่สำคัญนี้แล้ว Important Legal Notice