

อย่าตกเป็นเหยื่อของอาชญากรรมไซเบอร์!

ให้ความสำคัญกับการรักษาความปลอดภัยของโทรศัพท์มือถือ

ภัยคุกคามทางโทรศัพท์มือถือกำลังเพิ่มขึ้นอย่างรวดเร็ว และอาจทำให้ข้อมูลส่วนบุคคลและอุปกรณ์ต่าง ๆ ของคุณตกอยู่ในความเสี่ยง คุณควรเรียนรู้ว่าคุณจะป้องกันภัยคุกคามของคุณจากอาชญากรไซเบอร์ได้อย่างไร เมื่อคุณทำธุรกรรมทางการเงินระหว่างการเดินทาง

ทำไมคุณต้องรักษาความปลอดภัยอุปกรณ์เคลื่อนที่ของคุณ

อุปกรณ์เคลื่อนที่ ที่ไม่มีการรักษาความปลอดภัยจากภัยคุกคาม ตัวอย่างเช่นการติดตั้งแอปพลิเคชันที่เป็นอันตรายหรือการคลิกลิงก์ฟิชซิ่ง สามารถทำให้อาชญากรไซเบอร์บุกรุกเข้าไปยังอุปกรณ์เคลื่อนที่และข้อมูลสำคัญของคุณได้



ใช้บริการธนาคารที่มีความปลอดภัยกับเรา

คุณสามารถป้องกันข้อมูลธนาคารทางโทรศัพท์ของคุณได้ โดยทำตามคำแนะนำเหล่านี้



ดาวน์โหลด Standard Chartered Mobile App จาก Google Play หรือ App Store อย่าดาวน์โหลดแอปพลิเคชันจากบุคคลที่สามหรือไซต์ที่ไม่รู้จัก หากต้องการทราบข้อมูลเพิ่มเติมคลิกที่นี่ [here](#)



ออกจากระบบ Standard Chartered Mobile แอปพลิเคชัน ทุกครั้งหลังการใช้งานและอย่าปล่อยให้แอปพลิเคชันมีการทำงานอยู่เบื้องหลัง โดยเฉพาะหลังจากที่คุณได้เข้าใช้งานแล้ว



อย่าเก็บรหัสผ่าน, รหัสเข้าระบบ, หรือหมายเลขบัญชีของคุณไว้ในโทรศัพท์มือถือของคุณ อาชญากรไซเบอร์สามารถขโมยข้อมูลนี้ได้หากโทรศัพท์มือถือของคุณถูกแฮ็กหรือถูกขโมย



อย่าใช้อุปกรณ์ "เจลเบรก" (iOS) หรือ "รูท" (Android) ในการทำธุรกรรมธนาคารของคุณ เพราะจะทำให้แฮกเกอร์สามารถเข้าไปทำการเปลี่ยนแปลงระบบปฏิบัติการในโทรศัพท์ของคุณได้ง่ายขึ้น

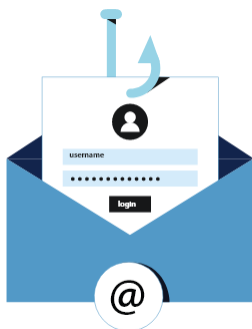


ลิงก์หรือไฟล์แนบที่เป็นอันตรายในข้อความพีชซึ่งได้ถูกออกแบบมาเพื่อให้แฮกเกอร์สามารถทำการโจรกรรมข้อมูลธนาคารของคุณได้ หรือทำให้อุปกรณ์เคลื่อนที่ของคุณติดไวรัส โปรดอย่าคลิกที่ไฮเปอร์ลิงก์หรือดาวน์โหลดไฟล์แนบในอีเมลหรือข้อความจากผู้ที่คุณไม่รู้จักหรือร้องขอ



ตรวจสอบว่าระบบปฏิบัติการของโทรศัพท์ของคุณได้รับการอัปเดตเป็นประจำเพื่อให้ได้รับการแก้ไขหากมีช่องโหว่ด้านความปลอดภัยเกิดขึ้น อาชญากรไซเบอร์สามารถใช้ช่องโหว่ของซอฟต์แวร์นี้เพื่อเข้าถึงโทรศัพท์ของคุณ โดยที่คุณไม่รู้ตัว

เรายินดีให้ความช่วยเหลือคุณ



โปรดติดต่อศูนย์บริการลูกค้าของเรา (Call Center hotline) ที่หมายเลขโทรศัพท์ 02-724-1553 ทั้งนี้หากคุณสงสัยว่ามีผู้บุกรุกเข้าถึงบัญชีของคุณโดยไม่ได้รับอนุญาตหรือมีการทำธุรกรรมแปลกปลอมในบัญชีของคุณ เราจะดำเนินการเพื่อปกป้องบัญชีของคุณตามที่จะสามารถทำได้ ทั้งนี้ธนาคารอาจขอให้คุณช่วยจัดส่งเอกสารรายงานใบแจ้งความกับเจ้าหน้าที่ตำรวจหรือหน่วยงานที่บังคับใช้กฎหมายมาให้ด้วย

เราสามารถช่วยกันหยุดยั้งอาชญากรรมไซเบอร์ได้



สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ Mobile Device
โปรดเข้าไปที่ <https://www.sc.com/global/security-tips/>

Here for good



โปรดอย่าตอบกลับอีเมลนี้

คุณไม่ควรส่งข้อมูลที่เป็นความลับและ / หรือข้อมูลสำคัญใด ๆ ไปยังธนาคารทางอีเมล เนื่องจากธนาคารไม่ได้รับรองหรือรับประกันเกี่ยวกับความปลอดภัยหรือความถูกต้องของข้อมูลที่คุณส่ง ธนาคารจะไม่รับผิดชอบต่อความสูญเสียหรือความเสียหายใด ๆ ที่เกิดขึ้นจากการที่คุณตัดสินใจใช้อีเมลเพื่อสื่อสารกับธนาคาร กรุณาให้ความสำคัญและพิจารณาให้ดีก่อนที่คุณจะตัดสินใจที่จะกระทำใดๆ กับข้อมูลบนเว็บไซต์นี้หรือตอบกลับหรือส่งข้อมูลหรือเอกสารสำคัญใด ๆ ให้เราเพื่อตอบกลับจดหมายฉบับนี้ และคุณได้อ่านและทำความเข้าใจประกาศทางกฎหมายที่สำคัญนี้แล้ว [Important Legal Notice](#).