

อยู่อย่างปลอดภัยจากการหลอกลวง

สำหรับเราที่ คอมมแบงก์ (CommBank) แล้ว ความไว้วางใจและความปลอดภัยเป็นสิ่งที่สำคัญที่สุด เราเห็นลูกค้าที่ถูกกดดันหรือถูกหลอกลวงให้ส่งเงินให้มิจฉาชีพมีจำนวนมากขึ้นเรื่อย ๆ การหลอกลวงเหล่านี้มักจะมีความซับซ้อนและเข้ามาในหลากหลายรูปแบบ สิ่งสำคัญคือคุณต้องคอยระวังและแจ้งให้เราทราบ หากคุณรู้สึกว่ามีบางอย่างผิดปกติ หากคุณต้องการเรียนรู้เพิ่มเติมเกี่ยวกับวิธีการป้องกันตนเอง รวมถึงการรายงานการหลอกลวง โปรดดูที่ commbank.com.au/safe

การรับรองความถูกต้องและการพิสูจน์ตัวตน

- คุณสามารถทำการตรวจสอบเรื่องความปลอดภัยได้ที่แอป CommBank
- แอปได้มีการ เปิดใช้งานการรับรองความถูกต้องแบบหลายปัจจัย ซึ่งจะให้การตรวจสอบความถูกต้อง(ข้อมูล)เพิ่มเติมในการยืนยันตัวตนของคุณ
- ใช้ **CallerCheck** เพื่อพิสูจน์การยืนยันตัวตนของผู้โทรเข้ามาโดยอ้างว่าโทรมาจากธนาคาร
- ใช้ **CustomerCheck** ที่สาขาเพื่อพิสูจน์ตัวตนของคุณกับเจ้าหน้าที่ของเรา
- NameCheck** จะแจ้งให้คุณทราบหากรายละเอียดบัญชีในการชำระเงินครั้งแรกนั้นดูเหมือนจะไม่ถูกต้อง

รหัสผ่านและข้อมูลส่วนบุคคล

- อย่าเปิดเผยรหัสผ่านหรือเลขรหัสประจำตัว (PIN) และระมัดระวังในการแบ่งปันข้อมูลส่วนบุคคล
- อย่าให้รหัสการยืนยันตัวตนของคุณ หรือ เน็ตโค้ด (NetCode) ของคุณให้กับใคร ซึ่งรวมถึงพนักงานของ CommBank
- คุณสามารถเปลี่ยนรหัสผ่านใน เน็ตแบงก์ (NetBank) และแอป CommBank ได้ตลอดเวลา
- สร้างรหัสผ่านที่แข็งแกร่งและเปลี่ยนรหัสผ่านเป็นประจำ สำหรับเคล็ดลับในการสร้างรหัสผ่าน โปรดไปที่ commbank.com.au/password-security

ความปลอดภัยของอุปกรณ์และการชำระเงิน

- อัปเดตซอฟต์แวร์ป้องกันไวรัสให้ทันสมัยอยู่เสมอ รวมถึงป้องกันคอมพิวเตอร์ของคุณจากภัยคุกคามที่พบได้บ่อย
- ใช้วิธีการชำระเงินที่ปลอดภัย เช่น ใช้วิธีการแตะบัตรหรืออุปกรณ์ใช้ชำระเงิน (tapping) หรือใช้วิธีการสอด้บัตรของคุณเข้าเครื่อง
- อย่าแชร์อุปกรณ์ที่สามารถเข้าถึงกระเป๋าสตางค์ดิจิทัลของคุณได้

อีเมล ข้อความ เอสเอ็มเอส (SMS) และออนไลน์

- อย่าคลิกลิงก์ที่อยู่ในอีเมลหรืออยู่ในข้อความ SMS ที่น่าสงสัย
- หากคุณมีสิ่งใดที่ไม่แน่ใจเกี่ยวกับข้อความ โปรดพูดคุยกับบุคคลที่คุณไว้วางใจหรือติดต่อองค์กรโดยตรง ผ่านทางรายละเอียดการติดต่ออย่างเป็นทางการ
- วางสายโทรศัพท์ที่มาจากสายอัตโนมัติ โทรศัพท์ที่น่าสงสัย หรือโทรศัพท์จากบุคคลที่สามผู้ซึ่งทำการข่มขู่คุณ
- ระมัดระวังเกี่ยวกับการติดต่อจากบุคคลที่คุณที่ไม่รู้จักบนโซเชียลมีเดียและแพลตฟอร์มออนไลน์

หยุด ตรวจสอบ ปฏิเสธ

หยุด มีบางอย่างดูผิดปกติหรือไม่ หากคุณมีข้อสงสัย วิธีที่ดีที่สุดคือให้หยุด รวบรวมสติ **ตรวจสอบ** ทำการสอบถามบุคคลที่คุณไว้วางใจ หรือใช้รายละเอียดอย่างเป็นทางการขององค์กรเพื่อทำการติดต่อองค์กรโดยตรง **ปฏิเสธ** วางสายโทรศัพท์เข้ามา ลบอีเมลถึง บล็อกเบอร์โทรศัพท์นั้น เปลี่ยนรหัสผ่านของคุณ

หากคุณเชื่อว่าคุณได้ตกเป็นเหยื่อของการหลอกลวง โปรดติดต่อ CommBank กันที่หมายเลข **13 22 21** หรือ **+61 2 9999 3283** หากโทรจากต่างประเทศ

คุณสามารถใช้บริการแปลและล่ามฟรีของรัฐบาลซึ่งจะสามารถช่วยให้คุณสื่อสารกับเราได้ หากภาษาอังกฤษไม่ใช่ภาษาแรกของคุณ ซึ่งมีให้บริการมากกว่า 150 ภาษา เราสามารถจัดการบริการนี้ให้กับคุณได้เมื่อคุณโทรศัพท์มาหาเรา หรือมาหาเราที่สาขาของธนาคาร

สิ่งที่ควรทราบมีดังต่อไปนี้ เราจะไม่ส่งอีเมล หรือ SMS ถึงคุณเพื่อขอข้อมูลธนาคารของคุณ เช่น รหัสลูกค้าเน็ตแบงก์ของคุณ (NetBank Client ID) รหัสผ่าน หรือ NetCode ของคุณ รวมถึงจะไม่ส่งลิงก์เพื่อเข้าสู่ระบบโดยตรงจากอีเมล หรือ SMS โปรดพิมพ์ข้อความว่า commbank.com.au ลงในโปรแกรมท่องเว็บ หรือ เบราว์เซอร์ (browser) เสมอ หรือใช้แอป CommBank เพื่อที่คุณจะสามารถทำธุรกรรมทางธนาคารของคุณอย่างปลอดภัย หากคุณได้รับสิ่งที่น่าสงสัยจาก CommBank โปรดส่งสิ่งนี้ไปที่ CommBank@cba.com.au และทำการลงบันทึกกับ Commonwealth Bank of Australia ABN 48 123 123 124 AFSL และใบอนุญาตเครดิตของออสเตรเลีย 234945

ข้อมูลที่สำคัญเกี่ยวกับการหลอกลวงที่พบได้บ่อย



การลงทุน (รวมถึงสกุลเงินดิจิทัล หรือ คริปโต - Crypto)

มิจฉาชีพ หรือ แสกมเมอร์ (scammer) มักทำการหลอกลวงบุคคลโดยให้คำสัญญาเกี่ยวกับการได้รับผลตอบแทนที่สูง ซึ่งมักเกี่ยวข้องกับคริปโตหรือโอกาสในการลงทุนอื่น ๆ มิจฉาชีพอาจพยายามติดต่อคุณทางโทรศัพท์ อีเมล หรือแพลตฟอร์มทางโซเชียลมีเดีย

เคล็ดลับในการป้องกันตัวเอง

- หากสิ่งที่ฟังนั้นดูดีเกินไปที่จะเป็นความจริง ความจริงก็อาจจะเป็นเช่นนั้น
- ใช้ความระมัดระวังในเรื่องที่เกี่ยวกับข้อเสนอที่คุณไม่ได้เป็นผู้ร้องขอไว้ และเรื่องที่คุณถูกกดดันให้ลงทุนหรือให้กระทำการอย่างรวดเร็ว
- ตรวจสอบความถูกต้องตามกฎหมายของบริษัทหรือนายหน้าบนเว็บไซต์ของสำนักงานคณะกรรมการกำกับหลักทรัพย์และการลงทุนของออสเตรเลีย (ASIC - Australian Securities & Investments Commission)

การโจมตีผ่านอีเมลเพื่อหลอกให้สูญเสียรายได้ผ่านทางอีเมล หรือ Business Email Compromise



มิจฉาชีพสามารถมุ่งเป้าไปหลอกลวงธุรกิจต่าง ๆ ด้วยการใช้อีเมลที่อยู่หรืออีเมลที่ได้มาอย่างมีขอบซึ่งทำให้ดูเหมือนว่าเป็นอีเมลที่ส่งมาจากผู้ติดต่อที่เชื่อถือได้ เช่น ผู้ช่วยของคุณ ลูกค้ายกยความ ผู้จัดการ หรือผู้ขายของคุณ

เคล็ดลับในการป้องกันตัวเองมีดังต่อไปนี้

- โทรหาองค์กรตามหมายเลขติดต่ออย่างเป็นทางการเพื่อยืนยันรายละเอียด ก่อนที่คุณจะชำระเงินในครั้งแรก หรือทำการเปลี่ยนแปลงรายละเอียดการชำระเงินของคุณ
- ใช้คุณสมบัติ NameCheck เมื่อจะทำการชำระเงิน เพื่อตรวจสอบว่าชื่อบัญชีนั้นตรงกับเลขสาขาของธนาคาร (BSB) และตรงกับหมายเลขบัญชีที่ให้ไว้หรือไม่
- ฝึกอบรมพนักงานเพื่อให้สามารถจำแนกและรายงานความพยายามในการหลอกลวงเพื่อให้ได้มาของข้อมูลหรือ ฟิชซิง (phishing)



การเข้าถึงจากระยะไกล

เมื่อมิจฉาชีพโทรศัพท์หาคุณและพยายามเข้าถึงบัญชีหรืออุปกรณ์ของคุณ โดยหลอกล่ามาจากบริษัทหรือองค์กรที่เชื่อถือได้

เคล็ดลับในการป้องกันตัวเองมีดังต่อไปนี้

- อย่าดาวน์โหลดซอฟต์แวร์เพื่อเข้าถึงจากระยะไกลได้ตามคำขอ หรือกระทำภายใต้แรงกดดันจากการโทรศัพท์โดยบุคคลที่สาม
- คุณสามารถโทรศัพท์กลับไปที่องค์กรได้ตลอดเวลา โดยใช้รายละเอียดการติดต่อที่ถูกต้องตามกฎหมาย ซึ่งอยู่บนเว็บไซต์อย่างเป็นทางการขององค์กร
- คุณสามารถขอให้ทางเรายืนยันการโทรศัพท์ได้ตลอดเวลาผ่านฟีเจอร์ CallerCheck ในแอป หากคุณได้รับสายที่อ้างว่าเป็นพนักงานจาก CommBank

ฟิชซิง และ สมิซซิง (smishing) หรือ การหลอกลวงทางข้อความ



มิจฉาชีพใช้อีเมลหรือข้อความหลอกลวงที่อาจมีลิงก์ที่จะนำคุณไปยังเว็บไซต์ที่ใช้ในการหลอกลวงหรือขอข้อมูลส่วนบุคคลที่มีความอ่อนไหว ซึ่งเป็นข้อมูลส่วนบุคคลที่เป็นเรื่องส่วนตัว

เคล็ดลับในการป้องกันตัวเอง มีดังต่อไปนี้

- โปรดอย่าคลิกลิงก์ในอีเมล หรือ ข้อความ SMS ที่น่าสงสัย
- คุณสามารถยืนยันความถูกต้องของข้อความได้โดยติดต่อกับองค์กรโดยตรง โดยใช้วิธีติดต่ออย่างเป็นทางการที่มีอยู่
- รายงานข้อความที่น่าสงสัยจาก CommBank ไปที่ hoax@cba.com.au



ข้อมูลที่สำคัญเกี่ยวกับการหลอกลวงที่พบได้บ่อย



ความสัมพันธ์

มิจาซีพจะสร้างโปรไฟล์ปลอมเพื่อสร้างความสัมพันธ์และหลอกล่อเพื่อให้ส่งเงินหรือข้อมูลส่วนตัวให้มิจาซีพ

เคล็ดลับในการป้องกันตัวเองมีดังต่อไปนี้

- อย่าส่งเงินหรือเปิดเผยรหัสผ่าน รายละเอียดบัตรเครดิต หรือเลขบัญชีกับใครก็ตามที่คุณไม่ไว้วางใจ
- หาข้อมูลผู้ที่เป็นคู่ครองของคุณทางออนไลน์โดยผ่านทางกูเกิ้ล (Google) หรือแอปโซเชียลมีเดีย ลองค้นหารูปภาพแบบย้อนกลับเพื่อดูว่ามีคนอื่นเป็นเจ้าของรูปภาพที่ส่งมาให้คุณหรือไม่
- พูดคุยกับครอบครัวและเพื่อนของคุณ เกี่ยวกับความสัมพันธ์ทางออนไลน์ของคุณ พวกเขาอาจสามารถเสนอมุมมองรวมถึงระบุสัญญาณเตือนที่คุณอาจจะไม่ได้สังเกตเห็น



การซื้อขายออนไลน์

มิจาซีพจะสร้างร้านค้าออนไลน์หรือโฆษณาเพื่อที่จะล่อลวงผู้ซื้อให้ซื้อผลิตภัณฑ์ที่ไม่มีอยู่จริง หรือเป็นของปลอม

เคล็ดลับในการป้องกันตัวเองมีดังต่อไปนี้

- ซื้อสินค้าจากเว็บไซต์ที่มีชื่อเสียงและปลอดภัยเท่านั้น และโปรดระวังข้อเสนอใด ๆ ที่ดูดีเกินกว่าที่จะเป็นจริง
- ใช้วิธีการชำระเงินที่ปลอดภัยและหลีกเลี่ยงการโอนเงินโดยตรงไปยังผู้ขาย
- อย่ารับซื้อสินค้าหรือถูกกดดันโดย 'ข้อเสนอที่จำกัด' หรือการสิ้นสุดการขายแบบมีการ 'นับถอยหลัง'

โอกาสในการจ้างงาน



ในกรณีที่ข้อเสนอการจ้างงานดูเหมือนจะต้องใช้ความพยายามเพียงเล็กน้อย หรือไม่ต้องใช้ความพยายามสำหรับผลตอบแทนทางการเงินที่สูง หรือมีกรณีที่ให้สัญญาว่างานนี้จะสามารถทำเงินได้อย่างรวดเร็ว

เคล็ดลับในการป้องกันตัวคุณเองมีดังต่อไปนี้

- ตรวจสอบบริษัทรวมถึงข้อเสนอผ่านช่องทางอย่างเป็นทางการ และหาข้อมูลเกี่ยวกับบริษัทเพื่อให้แน่ใจว่าบริษัทนี้เป็นบริษัทที่ถูกต้องตามกฎหมายและมีการทำการค้าในปัจจุบัน
- ระวังการเสนองานผ่านโซเชียลมีเดีย แชทที่ต้องเข้ารหัส (encrypted chat) อีเมล ไทป์สคริปต์ หรือจดหมายจากคนที่คุณไม่เคยพบหรือบริษัทที่คุณไม่รู้จัก
- บริษัทที่ถูกต้องตามกฎหมายจะไม่ขอให้คุณชำระเงินล่วงหน้า หรือใช้ข้อมูลธนาคารส่วนบุคคลของคุณเพื่ออำนวยความสะดวกด้านเงินทุนหรือการชำระเงินของบริษัท.

การคุกคามและการลงโทษ



มิจาซีพแอบอ้างว่าเป็นเจ้าหน้าที่หรือองค์กรที่เชื่อถือได้ เพื่อเรียกเงินด้วยการขู่กรงใจว่าจะปรับ หรือจะดำเนินการทางกฎหมาย

เคล็ดลับในการป้องกันตัวเองมีดังต่อไปนี้

- วางสายเมื่อผู้โทรติดต่อเข้ามาข่มขู่ และทำการติดต่อกับองค์กรโดยตรง
- องค์กรที่ถูกต้องตามกฎหมายจะไม่ขอให้คุณชำระเงินโดยวิธีการที่ผิดปกติ เช่น โดยการใช้นิตของขวัญ หรือบัตรเครดิต คำ บัตรกำนัล iTunes การโอนเงิน หรือ บิตคอยส์ (Bitcoins)
- หากคุณกังวลเรื่องความปลอดภัย โปรดติดต่อสายช่วยเหลือของตำรวจ

