<u>ควรระวังมิจฉาชีพ: เคล็ดลับอัจฉริยะสำหรับผู้บริโภค</u>

1. เคล็ดลับอัจฉริยะในการป้องกัน SMS และอีเมลฟิชชิง

ตามข้อกำหนดการกำกับดูแลของ HKMA ธนาคารจะไม่ส่งข้อความ SMS
หรืออีเมลที่มีไฮเปอร์ลิงก์ฝังอยู่เพื่อนำลูกค้าไปยังเว็บไซต์หรือแอปพลิเคชันมือถือของธนาคารเพื่อทำธุรกรรม
และจะไม่ขอให้ลูกค้าให้ข้อมูลส่วนบุคคลที่มีความเสี่ยง รวมถึงรหัสผ่านสำหรับเข้าสู่ระบบและรหัส OTP
ผ่านไฮเปอร์ลิงก์

หากคุณได้รับ SMS หรืออีเมลที่มีไฮเปอร์ลิงก์ฝังอยู่และขอให้คุณป้อนข้อมูลเข้าสู่ระบบอินเทอร์เน็ตแบงก์กิ้ง
ซึ่งธนาคารจะไม่มีนโยบายการส่งข้อความเหล่านี้ คุณควรพิจารณาอย่างรอบคอบก่อนทำการคลิกลิงก์ใด ๆ
ที่อ้างว่าส่งมาจากธนาคาร หากคุณพบว่าลิงก์ (หรือไฟล์แนบ) ใน SMS หรืออีเมลมีความน่าสงสัย
อย่าคลิกลิงก์ดังกล่าว (หรือเปิดไฟล์แนบ)
คุณควรเข้าสู่อินเทอร์เน็ตแบงก์กิ้งโดยพิมพ์ที่อยู่เว็บไซต์ของธนาคารโดยตรง ใช้บุ๊กมาร์ก
หรือใช้แอปอินเทอร์เน็ตแบงก์กิ้งบนมือถือเสมอ

หากมีข้อสงสัย ลูกค้าธนาคารสามารถติดต่อธนาคารที่เกี่ยวข้องเพื่อตรวจสอบความถูกต้องของ SMS
หรืออีเมลผ่านช่องทางอื่น (เช่น สายด่วนบริการลูกค้าของธนาคาร)

ข้อมูลสำหรับเข้าสู่ระบบอินเทอร์เน็ตแบงก์กิ้ง รวมถึงชื่อผู้ใช้ รหัสผ่าน และรหัสผ่านแบบใช้ครั้งเดียว (OTP)
มีความสำคัญในโลกดิจิทัลไม่ต่างจากกุญแจบ้านในโลกจริง และควรได้รับการปกป้องอย่างเหมาะสม

2. ตัวอย่างอีเมลฟิชชิงที่แอบอ้างว่าเป็นอีเมลจากธนาคาร

<u>ลักษณะทั่วไป 5 ประการ:</u>

1. ไม่ระบุชื่อผู้รับ (กล่าวคือ เป็นผู้รับที่ไม่เปิดเผย)
2. ชื่อและที่อยู่อีเมลของผู้ส่งอาจเหมือนกับข้อมูลจริงของธนาคารที่เกี่ยวข้องทุกประการ

3. อีเมลมักปรากฏเป็นการแจ้งเตือนสำคัญจากธนาคาร (เช่น
   “การแจ้งเตือนการโอนเงินจำนวนมากในบัญชีลูกค้า” หรือ
   “ขอให้ลูกค้าเปิดใช้งานฟังก์ชันความปลอดภัยใหม่ มิฉะนั้นบริการธนาคารบางรายการจะถูกระงับ (เช่น บริการโอนเงิน)”) โดยจะขอให้ลูกค้าคลิกลิงก์หรือเปิดไฟล์แนบในอีเมล
4. อีเมลมักมีไฮเปอร์ลิงก์ที่ดูเหมือนที่อยู่เว็บไซต์จริงของธนาคาร อย่างไรก็ตาม
   เมื่อเลื่อนเมาส์ไปวางบนลิงก์ คุณจะสังเกตได้ว่าลิงก์จริงที่ฝังอยู่นั้นเป็น URL อื่น
5. อาจมีข้อผิดพลาดด้านไวยากรณ์หรือการสะกดคำในอีเมล

<u>คำเตือน:</u>

หากไม่แน่ใจเกี่ยวกับอีเมล ให้ตรวจสอบกับสายด่วนบริการลูกค้าของธนาคารผ่านช่องทางทางการ (เช่น เว็บไซต์ จดหมาย หรือสื่อส่งเสริมการขาย) แม้ว่าจะมีหมายเลขโทรศัพท์แสดงอยู่ในอีเมลก็ตาม แฮกเกอร์อาจเพิ่มเคล็ดลับด้านความปลอดภัยไว้ด้านล่างของอีเมลฟิชชิงเพื่อให้ดูน่าเชื่อถือมากขึ้น

3. เคล็ดลับอัจฉริยะในการป้องกันการหลอกลวงด้วยบัตรเครดิต

การหลอกลวงด้วยบัตรเครดิตมักเกิดขึ้นเป็นครั้งคราว
โดยมีการเปลี่ยนแปลงรูปแบบการก่อเหตุและกลวิธีหลอกลวงอยู่เสมอ
โปรดตะหนักและปกป้องข้อมูลบัตรของคุณเสมอเพื่อหลีกเลี่ยงการตกเป็นเหยื่อของการหลอกหลวงด้วยบัตรเครดิต ในฐานะผู้ใช้บัตรเครดิตอย่างชาญฉลาด คุณควรให้ความสำคัญกับคำแนะนำต่อไปนี้:

- ดูแลและป้องกันบัตรเครดิต ข้อมูลบัตร และปัจจัยยืนยันตัวตนที่เกี่ยวข้อง (เช่น รหัสผ่านแบบใช้ครั้งเดียว อุปกรณ์มือถือ เป็นต้น) อย่างเหมาะสม
- อย่าเปิดเผยข้อมูลบัตรเครดิตของคุณแก่บุคคลที่สาม รวมถึงหมายเลขบัตร วันหมดอายุ รหัสความปลอดภัย (โดยปกติพิมพ์อยู่ด้านหลังบัตรถัดจากช่องลายเซ็น) และรหัสผ่านแบบใช้ครั้งเดียว
- ตรวจสอบความน่าเชื่อถือของร้านค้าและเว็บไซต์ (เช่น ตรวจสอบระดับความเสี่ยง/การแจ้งเตือนผ่าน “Scameter” ของกองกำลังตำรวจฮ่องกง) ก่อนให้ข้อมูลส่วนบุคคลและข้อมูลบัตรเครดิตเพื่ออนุมัติธุรกรรม และระวังสายโทรศัพท์ SMS

หรืออีเมลที่น่าสงสัย (เช่น ข้อความฟิชชิงมักแอบอ้างว่าส่งมาจากบริษัท ร้านค้า หรือธนาคารที่เชื่อถือได้ โดยมีข้อความและโลโก้ที่คล้ายคลึงกัน และมักมีการฝังลิงก์เพื่อนำคุณไปยังเว็บไซต์ปลอม เพื่อล่อลวงให้ผู้ถือบัตรให้ข้อมูลบัตรเครดิตและข้อมูลส่วนบุคคลที่มีความเสี่ยง)

- ตรวจสอบรายละเอียดของรหัสผ่านแบบใช้ครั้งเดียวที่ได้รับทาง SMS อย่างรอบคอบ รวมถึงข้อมูลธุรกรรมที่เกี่ยวข้อง (เช่น ประเภทธุรกรรม ชื่อร้านค้า จำนวนเงิน และสกุลเงิน เป็นต้น) และควรระมัดระวังในการใช้ฟีเจอร์ AutoFill ของสมาร์ทโฟน อย่าป้อนรหัสผ่านแบบใช้ครั้งเดียวและดำเนินธุรกรรมโดยไม่ตรวจสอบรายละเอียดธุรกรรมใน SMS เมื่อป้อนข้อมูลบัตร (รวมถึงรหัสผ่านแบบใช้ครั้งเดียว) ในบางกรณี ธุรกรรมอาจไม่สามารถยกเลิกได้และลูกค้าอาจต้องรับผิดชอบต่อธุรกรรมนั้น
- หลังจากที่คุณผูกบัตรเครดิตกับบริการชำระเงินผ่านมือถือแบบไร้สัมผัส (เช่น Apple Pay, Google Pay) ธนาคารจะส่งการแจ้งเตือนการผูกบัตรไปยังหมายเลขมือถือที่คุณลงทะเบียนไว้ โดยระบุบริการชำระเงินที่บัตรถูกผูกไว้ คุณควรตรวจสอบการแจ้งเตือนและแจ้งธนาคารผู้ออกบัตรทันทีหากคุณไม่ได้ดำเนินการคำสั่งผูกบัตรดังกล่าว เมื่อผูกบัตรสำเร็จแล้ว อาจไม่จำเป็นต้องใช้รหัสผ่านแบบใช้ครั้งเดียวสำหรับธุรกรรมในภายหลัง
- ให้ความสำคัญกับข้อความการสื่อสาร (เช่น อีเมล SMS เป็นต้น) ที่ส่งมาจากธนาคารอยู่เสมอ ตรวจสอบบันทึกรายการธุรกรรมบัตรเครดิตเป็นประจำและตรวจสอบใบแจ้งยอดรายเดือน แจ้งธนาคารผู้ออกบัตรทันทีหากพบธุรกรรมที่น่าสงสัยหรือไม่ได้รับอนุญาต ไม่ว่าจะเป็นจำนวนเงินเท่าใดก็ตาม
- แจ้งธนาคารผู้ออกบัตรและตำรวจทันทีหากคุณทำบัตรเครดิตสูญหาย หรือสงสัยว่าบัตรหรือข้อมูลบัตรถูกขโมย หรือสงสัยว่าบัตรถูกผูกกับอุปกรณ์มือถือที่น่าสงสัย

หากคุณไม่ได้ใช้หรือปกป้องบัตรเครดิตและข้อมูลบัตรอย่างเหมาะสม มิจฉาชีพอาจใช้โอกาสนี้ในการก่อการฉ้อโกง (เช่น ขโมยบัตรเพื่อทำธุรกรรมโดยไม่ได้รับอนุญาต) ส่งผลให้คุณสูญเสียทางการเงิน กล่าวโดยสรุป โปรดปกป้องบัตรและข้อมูลบัตรของคุณเพื่อหลีกเลี่ยงการตกเป็นเหยื่อของการหลอกลวงด้วยบัตรเครดิต

4. เคล็ดลับอัจฉริยะในการป้องกันสายโทรศัพท์และข้อความ SMS ปลอม

เมื่อได้รับสายโทรศัพท์ ข้อความ SMS อีเมล จดหมาย
หรือการติดต่อผ่านช่องทางอื่นใดที่อ้างว่ามาจากธนาคาร แม้จะมีการแจ้งว่าบัญชีของคุณกำลังมีความเสี่ยง มีการทำธุรกรรมผ่านบัตรเครดิตของคุณ หรือไม่ว่าคุณจะสนใจในผลิตภัณฑ์ที่กำลังถูกนำเสนอเพียงใด คุณควรระมัดระวังและ:

- ตรวจสอบยืนยันตัวตนของผู้โทรหรือผู้ส่ง
- หลีกเลี่ยงการเชื่อถือข้อมูลหมายเลขสายเรียกเข้าที่แสดงเพียงอย่างเดียวเพื่อยืนยันตัวตนที่แท้จริงของผู้โทร
  หรือโทรกลับไปยังหมายเลขสายด่วนของธนาคารที่ให้มาในข้อความโดยตรงและปฏิบัติตามคำแนะนำ
- อย่าให้ข้อมูลส่วนบุคคลที่มีความเสี่ยงโดยง่าย เพื่อปกป้องผลประโยชน์ของคุณเอง

HKMA หรือธนาคารจะไม่ขอข้อมูลส่วนบุคคลที่มีความเสี่ยงใด ๆ
(รวมถึงรหัสผ่านสำหรับเข้าสู่ระบบหรือรหัสผ่านแบบใช้ครั้งเดียว) ผ่านทางโทรศัพท์ อีเมล หรือข้อความ SMS และจะไม่แจ้งความผิดปกติของบัญชีผ่านข้อความเสียงที่บันทึกไว้ล่วงหน้า
คุณสามารถตรวจสอบหมายเลขสายด่วนของธนาคารที่เกี่ยวข้องได้จากเว็บไซต์ทางการของแต่ละธนาคาร หรือด้านหลังบัตร ATM/บัตรเครดิตของคุณ นอกจากนี้
คุณยังสามารถดู**รายการหมายเลขสายด่วนของธนาคารเพื่อรายย่อย**สำหรับใช้ยืนยันตัวตนของผู้ที่อ้างว่าเป็นตัวแทนธนาคารได้บนเว็บไซต์ของ Hong Kong Association of Banks
หลังจากโทรติดต่อสายด่วนของธนาคารเพื่อตรวจสอบยืนยันแล้ว
วิธีที่รอบคอบที่สุดในการดำเนินการต่อคือการติดต่อเจ้าหน้าที่ของธนาคารผ่านหมายเลขโทรศัพท์ที่ได้รับจากธนาคาร

5. การตรวจสอบยืนยันตัวตนของผู้โทรและหมายเลขสายด่วนของธนาคาร

คุณสามารถตรวจสอบหมายเลขสายด่วนของธนาคารที่เกี่ยวข้องได้จากเว็บไซต์ทางการของแต่ละธนาคาร หรือด้านหลังบัตร ATM/บัตรเครดิตของคุณ นอกจากนี้ คุณยังสามารถดูรายการหมายเลขสายด่วนของธนาคาร**เพื่อรายย่อย**สำหรับใช้ยืนยันตัวตนของผู้ที่อ้างว่าเป็นตัวแทนธนาคารได้บนเว็บไซต์ของ Hong Kong Association of Banks

6. **คำถามที่พบบ่อยเกี่ยวกับคดีฉ้อโกง**

A. ฉันต้องจ่ายค่าประกันทางการเงินหรือค่าธรรมเนียมการโอนสำหรับการโอนเงินจากฮ่องกงไปยังที่อื่นหรือไม่

ตามมาตรา 112 ของกฎหมายพื้นฐานระบุว่า
"จะไม่มีการใช้นโยบายควบคุมอัตราแลกเปลี่ยนเงินตราต่างประเทศในเขตบริหารพิเศษฮ่องกง เงินดอลลาร์ฮ่องกงสามารถแลกเปลี่ยนได้อย่างเสรี ตลาดสำหรับอัตราแลกเปลี่ยน ทองคำ หลักทรัพย์ สัญญาซื้อขายล่วงหน้า และอื่น ๆ จะยังคงดำเนินต่อไป
รัฐบาลของเขตบริหารพิเศษฮ่องกงจะปกป้องการไหลเวียนของเงินทุนอย่างเสรีภายใน เข้าสู่ และออกจากเขต"
ซึ่งหมายความว่าไม่มีข้อจำกัดในการโอนเงินในฮ่องกง และ HKMA ไม่ได้เรียกเก็บค่าธรรมเนียมใด ๆ สำหรับการโอนเงิน

B. คุณช่วยยืนยันได้หรือไม่ว่าฉันต้องวางเงินค่าธรรมเนียมล่วงหน้าเข้าบัญชีธนาคารที่กำหนดก่อน จึงจะสามารถรับเงินรางวัลลอตเตอรี่ที่ฉันถูกแจ้งว่าได้รับได้

เราสงสัยว่าคุณอาจเผชิญกับคดีฉ้อโกง HKMA เป็นหน่วยงานกำกับดูแลด้านการธนาคารในฮ่องกง และเราไม่มีความเกี่ยวข้องกับกิจกรรมลอตเตอรี่ใด ๆ

นอกจากนี้ ตามมาตรา 112 กฎหมายพื้นฐานระบุว่า
"จะไม่มีการใช้นโยบายควบคุมอัตราแลกเปลี่ยนเงินตราต่างประเทศในเขตบริหารพิเศษฮ่องกง เงินดอลลาร์ฮ่องกงสามารถแลกเปลี่ยนได้อย่างเสรี ตลาดสำหรับอัตราแลกเปลี่ยน ทองคำ หลักทรัพย์ สัญญาซื้อขายล่วงหน้า และอื่น ๆ จะยังคงดำเนินต่อไป
รัฐบาลของเขตบริหารพิเศษฮ่องกงจะปกป้องการไหลเวียนของเงินทุนอย่างเสรีภายใน เข้าสู่ และออกจากเขต"
ซึ่งหมายความว่าไม่มีข้อจำกัดในการโอนเงินในฮ่องกง และรัฐบาลไม่ได้เรียกเก็บค่าธรรมเนียมใด ๆ สำหรับการโอนเงิน

หากคุณสงสัยว่ามีกิจกรรมฉ้อโกงเกิดขึ้น
คุณอาจพิจารณาแจ้งเรื่องไปยังสถานีตำรวจท้องที่หรือกองปราบปรามอาชญากรรมทางการค้า (Commercial Crime Bureau) ของกองกำลังตำรวจฮ่องกง (Hong Kong Police Force) โดยตรง

C. ฉันควรทำอย่างไรหากได้รับอีเมลหรือสายโทรศัพท์จากธนาคารที่น่าสงสัย หรือพบเว็บไซต์ธนาคารที่น่าสงสัยว่าเป็นการฉ้อโกง

หากคุณได้รับข้อความที่น่าสงสัยหรือพบเว็บไซต์ที่น่าสงสัยซึ่งอ้างว่าเกี่ยวข้องกับธนาคาร
โปรดติดต่อธนาคารที่เกี่ยวข้องและตำรวจ
(ไม่ว่าจะเป็นสถานีตำรวจท้องที่หรือ**กองปราบปรามอาชญากรรมทางการค้า (Commercial Crime Bureau)** เพื่อรายงานกรณีดังกล่าว

“คลิกลิงก์ แล้วตกเป็นเหยื่อมิจฉาชีพ!” (วิดีโอ 30 วินาที) – บทถอดเสียง

ลิงก์วิดีโอ: https://www.youtube.com/watch?v=T1vEFnbiWh4

English		**Translation** *(This column is to be filled in by translators)*	
Scammer:	Download the app to verify your information or you will face detention	มิจฉาชีพ:	ดาวน์โหลดแอปเพื่อตรวจสอบยืนยันข้อมูลของคุณ มิฉะนั้นคุณจะถูกควบคุมตัว
Superimposed text:	...Download the app to verify your information, or you will face detention...	ข้อความที่แสดงบนหน้าจอ:	...ดาวน์โหลดแอปเพื่อตรวจสอบยืนยันข้อมูลของคุณ มิฉะนั้นคุณจะถูกควบคุมตัว...
University student:	What?	นักศึกษามหาวิทยาลัย:	อะไรนะ
Voice-over:	Think there’s a misunderstanding?	เสียงบรรยาย:	คิดว่าอาจเข้าใจผิด
Mother:	Why not find a part-time job?	แม่:	ทำไมไม่หางานพาร์ทไทม์ล่ะ
Son:	Mom! Look at this job!	ลูกชาย:	แม่! ดูงานนี้สิ!
Voice-over:	Think you've found a dream job?	เสียงบรรยาย:	คิดว่าคุณเจองานในฝันแล้วใช่ไหม
Superimposed text:	...Great jobs available. Provide personal information to facilitate salary payment...	ข้อความที่แสดงบนหน้าจอ:	...มีงานดี ๆ มากมาย โปรดให้ข้อมูลส่วนบุคคลเพื่ออำนวยความสะดวกในการจ่ายเงินเดือน..

Middle-aged woman:	Sure-win investment group with insider tips and recommendations?	ผู้หญิงวัยกลางคน:	กลุ่มการลงทุนการันตีกำไร พร้อมข้อมูลวงในและคำแนะนำ หรือ
Superimposed text:	…Sure-win investment group, open your account now…	ข้อความที่แสดงบนหน้าจอ:	…กลุ่มการลงทุนการันตีกำไร เปิดบัญชีของคุณตอนนี้…
Voice-over:	Think sure-win investment options are just lying around? One click on the wrong link can bring disaster	เสียงบรรยาย:	คิดว่าทางเลือกการลงทุนที่การันตีกำไรมีอยู่ทั่วไปนั้นหรือ
Superimposed text:	Please click the link to download the app and provide your personal information, ID number, bank account login name and password http://xxbank.vip/	ข้อความที่แสดงบนหน้าจอ:	การคลิกลิงก์ผิดเพียงครั้งเดียว ก็อาจนำไปสู่หายนะ โปรดคลิกลิงก์เพื่อดาวน์โหลดแอป และให้ข้อมูลส่วนบุคคล หมายเลขบัตรประจำตัวประชาชน ชื่อผู้ใช้และรหัสผ่านสำหรับเข้าสู่ระบบบัญชีธนาคาร http://xxbank.vip/
Voice-over:	Be cautious of fake links or you will regret it for life	เสียงบรรยาย:	ระวังลิงก์ปลอม มิฉะนั้นคุณจะเสียใจไปตลอดชีวิต
Son:	My money and personal information!	ลูกชาย:	เงินและข้อมูลส่วนบุคคลของผม !
Voice-over:	Click the links fall for scams	เสียงบรรยาย:	คลิกลิงก์ แล้วตกเป็นเหยื่อมิจฉาชีพ

Superimposed text:	Click the links Fall for scams	ข้อความที่แสดงบนหน้าจอ:	คลิกลิงก์ แล้วตกเป็นเหยื่อมิจฉาชีพ

“สามกลยุทธ์ต้านมิจฉาชีพ” - วิดีโอต้านมิจฉาชีพภาษากวางตุ้งสไตล์วินเทจ (1): รับมือการแอบอ้างเป็นเจ้าหน้าที่บังคับใช้กฎหมาย

ลิงก์วิดีโอ: https://www.youtube.com/watch?v=4dLS5soS0fI&t=2s

English		**Translation** *(This column is to be filled in by translators)*	
Superimposed text:	Vintage Cantonese Anti-Scam Video (1)	ข้อความที่แสดงบนหน้าจอ:	วิดีโอต้านมิจฉาชีพภาษากวางตุ้งย้อนยุค (1)
Leading actress:	Who’s calling?	นักแสดงนำหญิง:	ใครโทรมาค่ะ
Scammer:	I am a law enforcement officer. You have committed an offence!	มิจฉาชีพ:	ผมเป็นเจ้าหน้าที่บังคับใช้กฎหมาย คุณได้กระทำความผิด
Leading actress:	How could I have committed any offence? Don't wrong me	นักแสดงนำหญิง:	ฉันจะไปทำความผิดได้ยังไง อย่ามาใส่ร้ายฉันนะ
Scammer:	You know it well whether you have committed an offence or not I have issued an arrest warrant against you	มิจฉาชีพ:	คุณย่อมรู้ดีว่าคุณได้กระทำความผิดอะไรไว้หรือไม่ ผมได้ออกหมายจับคุณแล้ว
Leading actress:	What?	นักแสดงนำหญิง:	อะไรนะ
Scammer:	Cooperate and give me your bank account number and password	มิจฉาชีพ:	ให้ความร่วมมือและบอกหมายเลขบัญชีธนาคารกับรหัสผ่านขอ

	Otherwise, you will be sent to prison		งคุณมาซะ ไม่เช่นนั้นคุณจะถูกส่งเข้าคุก
Leading actress:	No way! My...my... My account number is...	นักแสดงนำหญิง:	ไม่มีทาง บัญชีของฉัน...ของฉัน... หมายเลขบัญชีของฉันคือ...
Male host of TV promotional video:	Scammers have many tricks; believe them and you'll be in a fix	พิธีกรชายของวิดีโอโปรโมททางทีวี:	มิจฉาชีพมีกลโกงมากมาย ถ้าหลงไปเชื่อพวกเขาแล้วคุณจะตกที่นั่งลำบาก
Leading actress:	Humph! Needless to say This person must be a scammer	นักแสดงนำหญิง:	หึ ไม่ต้องบอกก็รู้ คนนี้ต้องเป็นมิจฉาชีพแน่
Leading actress:	Let me apply the "Three Anti-Scam Tactics"	นักแสดงนำหญิง:	ฉันจะใช้ "สามกลยุทธ์ต้านมิจฉาชีพ"
Superimposed text:	Three Anti-Scam Tactics	ข้อความที่แสดงบนหน้าจอ:	สามกลยุทธ์ต้านมิจฉาชีพ
Leading actress:	Keep Calm	นักแสดงนำหญิง:	ตั้งสติ
Superimposed text:	Keep Calm Keep calm, don't panic	ข้อความที่แสดงบนหน้าจอ:	ตั้งสติ ตั้งสติ อย่าตื่นตระหนก
Leading actress:	Give Nothing	นักแสดงนำหญิง:	ไม่ให้ข้อมูล

Superimposed text:	Give Nothing Give no personal data or money	ข้อความที่แสดงบนหน้าจอ:	ไม่ให้ข้อมูล อย่าให้ข้อมูลส่วนบุคคลหรือเงินใด ๆ
Leading actress:	Verify and Seek Help	นักแสดงนำหญิง:	ตรวจสอบและขอความช่วยเหลือ
Superimposed text:	Verify and Seek Help Verify the caller's identity and seek help from others	ข้อความที่แสดงบนหน้าจอ:	ตรวจสอบและขอความช่วยเหลือ ตรวจสอบตัวตนของผู้โทรและขอความช่วยเหลือจากผู้อื่น
Scammer:	You have your tactics, but I have an arrest warrant I am only following instructions on this Hurry up and hand over your money and bank account password	มิจฉาชีพ:	คุณมีกลยุทธ์ของคุณ แต่ผมมีหมายจับ ผมแค่ทำเรื่องนี้ตามคำสั่ง รีบส่งเงินและรหัสผ่านบัญชีธนาคารของคุณมา
Leading actress:	Ha! Law enforcement officers will not request for account information Your arrest warrant is fake I have discerned your hoax	นักแสดงนำหญิง:	ฮ่า เจ้าหน้าที่บังคับใช้กฎหมายจะไม่ขอข้อมูลบัญชี หมายจับของคุณเป็นของปลอม ฉันจับได้แล้วว่าเป็นกลลวงของคุณ
Leading actress:	Watch this!	นักแสดงนำหญิง:	ดูนี่สิ
Scammer:	Argh...	มิจฉาชีพ:	อ๊าก...

Superimposed text:	The End	ข้อความที่แสดงบนหน้าจอ:	จบ
Leading actress:	No matter how old the trick is, there are always people who fall for it Remember the "Three Anti-Scam Tactics" Scammers will no longer be rampant	นักแสดงนำหญิง:	ไม่ว่ากลโกงจะเก่าแค่ไหน ก็ยังมีคนตกเป็นเหยื่อเสมอ จำ "สามกลยุทธ์ต้านมิจฉาชีพ" ไว้ มิจฉาชีพจะได้ไม่ระบาดอีกต่อไป
Superimposed text:	Remember the "Three Anti-Scam Tactics"! Scammers can no longer play tricks!	ข้อความที่แสดงบนหน้าจอ:	จำ "สามกลยุทธ์ต้านมิจฉาชีพ"! มิจฉาชีพจะไม่สามารถใช้กลโกงได้อีก
Leading actress:	In addition, the HKMA has launched the "Money Safe" service Just like a safe, it adds an extra layer of protection for deposits	นักแสดงนำหญิง:	นอกจากนี้ HKMA ได้เปิดตัวบริการ "Money Safe" โดยจะเปรียบเสมือนตู้เซฟที่เพิ่มชั้นการปกป้องเงินฝากอีกระดับ
Superimposed text:	Money Safe	ข้อความที่แสดงบนหน้าจอ:	Money Safe
Leading actress:	Contact your bank for details now	นักแสดงนำหญิง:	ติดต่อธนาคารของคุณเพื่อดูรายละเอียดได้แล้ววันนี้
Superimposed text:	(Hong Kong Monetary Authority Logo)	ข้อความที่แสดงบนหน้าจอ:	(โลโก้ Hong Kong Monetary Authority)

“สามกลยุทธ์ต้านมิจฉาชีพ” - วิดีโอต้านมิจฉาชีพภาษากวางตุ้งสไตล์วินเทจ (2): ทำลายกลลวงเทคโนโลยีดีปเฟก

ลิงก์วิดีโอ: https://www.youtube.com/watch?v=VJvrWYZBvBw&t=5s

English		**Translation** *(This column is to be filled in by translators)*	
Superimposed text:	Vintage Cantonese Anti-Scam Video (2)	ข้อความที่แสดงบนหน้าจอ:	วิดีโอต้านมิจฉาชีพภาษากวางตุ้งย้อนยุค (2)
Superimposed text:	Three months ago	ข้อความที่แสดงบนหน้าจอ:	สามเดือนก่อน
Son:	I am leaving for the capital for business Father, take good care of yourself!	ลูกชาย:	ข้ากำลังจะเดินทางไปเมืองหลวงเพื่อติดต่อธุรกิจ พ่อ ดูแลตัวเองดี ๆ นะ
Father:	Be careful and stay safe	พ่อ:	ปลอดภัยไว้ก่อนและระวังตัวด้วย
Fake Son:	Father! Save me!	ลูกชายปลอม:	พ่อ! ช่วยข้าด้วย!
Father:	Why are you so scared?	พ่อ:	ทำไมเจ้าถึงดูหวาดกลัวเช่นนั้น
Fake Son:	I was robbed by bandits on the way to the capital I lost all my goods and money, and I could not deliver the goods on time I need to compensate the clients for their losses!	ลูกชายปลอม:	ข้าถูกโจรปล้นระหว่างทางไปเมืองหลวง ข้าสูญเสียสินค้าและเงินไปทั้งหมด และไม่สามารถส่งสินค้าได้ทันเวลา ข้าต้องชดเชยค่าเสียหายให้ลู

	Transfer money to the account which I've just sent you immediately!		กค้า! โอนเงินไปยังบัญชีที่ข้าเพิ่งส่งให้ท่านทันทีด้วย!
Father:	For my son's sake, I had no choice but to…	พ่อ:	เพื่อลูกชายแล้ว ข้าจึงไม่มีทางเลือกนอกจากต้อง…
Master:	Hold on What is fake looks real while what is real looks fake Sir Let me share with you the "Three Anti-Scam Tactics"!	อาจารย์:	ช้าก่อน ของปลอมอาจดูเหมือนจริง ในขณะที่ของจริงกลับดูเหมือนปลอม ท่านขอรับ ข้าขอแบ่งปัน "สามกลยุทธ์ต้านมิจฉาชีพ"!
Superimposed text:	Three Anti-Scam Tactics	ข้อความที่แสดงบนหน้าจอ:	สามกลยุทธ์ต้านมิจฉาชีพ
Master:	Tactic One Keep Calm	อาจารย์:	กลยุทธ์ที่หนึ่ง ตั้งสติ
Superimposed text:	Keep Calm Keep calm, don't panic	ข้อความที่แสดงบนหน้าจอ:	ตั้งสติ ตั้งสติ อย่าตื่นตระหนก
Master:	Tactic Two Give Nothing	อาจารย์:	กลยุทธ์ที่สอง ไม่ให้ข้อมูล
Superimposed text:	Give Nothing Give no personal data or money	ข้อความที่แสดงบนหน้าจอ:	ไม่ให้ข้อมูล อย่าให้ข้อมูลส่วนบุคคลหรือเงินใด ๆ

Master:	Tactic Three Verify and Seek Help	อาจารย์:	กลยุทธ์ที่สาม ตรวจสอบและขอความช่วยเหลือ
Superimposed text:	Verify and Seek Help Verify the caller's identity and seek help from others	ข้อความที่แสดงบนหน้าจอ:	ตรวจสอบและขอความช่วยเหลือ ตรวจสอบตัวตนของผู้โทรและขอความช่วยเหลือจากผู้อื่น
Master:	Sir, remember these words	อาจารย์:	ท่านขอรับ จงจำคำเหล่านี้ไว้
Father:	Your uncle is an official working in the capital Why not reach out to him for help?	พ่อ:	ลุงของเจ้าทำงานเป็นขุนนางอยู่ในเมืองหลวง เหตุใดไม่ติดต่อเพื่อขอความช่วยเหลือจากเขาล่ะ
Fake Son:	Uncle is overwhelmed with responsibilities and not available!	ลูกชายปลอม:	ท่านลุงมีภาระหน้าที่ล้นมือและไม่ว่างขอรับ!
Father:	Humph! Uncle has already retired and returned home! You evil monster! How dare you impersonate my beloved son using “deepfake”!	พ่อ:	หึ! ลุงเจ้าเกษียณและกลับบ้านไปแล้ว! เจ้าปีศาจร้าย! บังอาจแอบอ้างเป็นลูกชายที่รักของข้าโดยใช้ “ดีปเฟก”!
Superimposed text:	Goodbye	ข้อความที่แสดงบนหน้าจอ:	ลาก่อน

Master:	No matter how old the trick is, there are always people who fall for it Remember the "Three Anti-Scam Tactics" Scammers will no longer be rampant	อาจารย์:	ไม่ว่ากลโกงจะเก่าแค่ไหน ก็ยังมีคนตกเป็นเหยื่อเสมอ จำ "สามกลยุทธ์ต้านมิจฉาชีพ" ไว้ มิจฉาชีพจะไม่ระบาดอีกต่อไป
Superimposed text:	Remember the "Three Anti-Scam Tactics"! Scammers can no longer play tricks!	ข้อความที่แสดงบนหน้าจอ:	จำ "สามกลยุทธ์ต้านมิจฉาชีพ"! มิจฉาชีพจะไม่สามารถใช้กลโกงได้อีก
Master:	In addition, the HKMA has launched the "Money Safe" service	อาจารย์:	นอกจากนี้ HKMA ได้เปิดตัวบริการ "Money Safe"
Superimposed text:	Money Safe	ข้อความที่แสดงบนหน้าจอ:	Money Safe
Master:	Just like a treasure box, it adds an extra layer of protection for deposits Contact your bank for details now	อาจารย์:	เปรียบเสมือนหีบสมบัติที่เพิ่มชั้นการปกป้องเงินฝากอีกระดับ ติดต่อธนาคารของคุณเพื่อดูรายละเอียดได้แล้ววันนี้
Superimposed text:	(Hong Kong Monetary Authority Logo)	ข้อความที่แสดงบนหน้าจอ:	(โลโก้ Hong Kong Monetary Authority)