<u>فراڈ کرنے والوں سے ہوشیار رہیں: کسٹمرز کے لیے سمارٹ ٹپس</u>

1. فِشنگ SMS اور ای میلز کے خلاف سمارٹ ٹپس

HKMA کی نگرانی سے متعلق تقاضوں کے مطابق بینک کسٹمرز کو SMS یا ای میل کے ذریعے ایسے پیغامات نہیں بھیجیں گے جن میں ویب سائٹس یا موبائل ایپلیکیشنز پر ٹرانزیکشنز کے لیے ایمبیڈڈ ہائپر لنکس شامل ہوں۔ اسی طرح وہ کسٹمرز سے ہائپر لنکس کے ذریعے حساس ذاتی معلومات فراہم کرنے کے لیے بھی نہیں کہیں گے جن میں لاگ اِن پاس ورڈز اور OTPs شامل ہیں۔

اگر آپ کو ایسے SMS یا ای میل پیغامات موصول ہوں جن میں ایمبیڈڈ ہائپر لنکس ہوں اور آپ سے انٹرنیٹ بینکنگ کے لاگ اِن اسناد درج کرنے کو کہا جائے تو یہ پیغامات بینکوں کی طرف سے نہیں ہوتے۔ بینک کی جانب سے بھیجے جانے کا دعوٰی کرنے والے کسی بھی ہائپر لنکس پر کلک کرنے سے پہلے دوبارہ سوچیں۔ اگر SMS یا ای میل میں موجود ہائپر لنکس (یا اٹیچمنٹس مشکوک لگیں تو ہائپر لنکس پر کلک نہ کریں (یا اٹیچمنٹس نہ کھولیں)۔ ہمیشہ انٹرنیٹ بینکنگ تک رسائی کے لیے براہ راست بینک کی ویب سائٹ کا پتہ خود درج کریں، یا بک مارک استعمال کریں یا انٹرنیٹ بینکنگ موبائل ایپلیکیشن (ایپ) استعمال کریں۔

کوئی بھی سوالات درپیش ہونے کی صورت میں، بینک کے کسٹمرز SMS یا ای میل کی اصل حیثیت کی تصدیق کے لیے دیگر ذرائع کے ذریعے متعلقہ بینک سے رابطہ کر سکتے ہیں (جیسے بینک کی کسٹمر سروس ہاٹ لائن)۔

انٹرنیٹ بینکنگ کے لاگ اِن اسناد، جن میں یوزر نیم لاگ اِن پاس ورڈز اور ون ٹائم پاس ورڈز (OTPs) شامل ہیں ڈیجیٹل دنیا میں اتنے ہی اہم ہیں جتنے حقیقی دنیا میں گھر کی چابیاں اور ان کی مناسب حفاظت کی جانی چاہیے۔

2. بینکوں کی جانب سے بھیجے جانے کا دعوٰی کرنے والی نمونہ فِشنگ ای میلز

<u>پانچ عام خصوصیات:</u>

1. وصول کنندہ کا نام درج نہیں ہوتا (یعنی غیر ظاہر شدہ وصول کنندہ)
2. بھیجنے والے کا نام اور ای میل ایڈریس بظاہر متعلقہ بینک کی اصل معلومات جیسا ہی ہو سکتا ہے
3. ای میل عموماً بینک کی جانب سے ایک اہم اطلاع کے طور پر ظاہر ہوتی ہے (مثلاً صارف کے اکاؤنٹ میں بڑی رقم کی منتقلی کی اطلاع یا کسٹمر سے نئی سیکیورٹی فیچر کو فعال کرنے کی درخواست کی جاتی ہے بصورت دیگر کسی مخصوص بینکاری سروس (جیسے فنڈ ٹرانسفر سروس) کو معطل کردی جائے گی)۔ کسٹمر سے ای میل میں موجود ہائپر لنک پر کلک کرنے یا اٹیچمنٹ کھولنے کو کہا جاتا ہے
4. ای میل میں عموماً ایک ایسا ہائپر لنک ہوتا ہے جو بینک کی اصل ویب سائٹ کے ایڈریس جیسا دکھائی دیتا ہے لیکن جب ہائپر لنک پر ماؤس لے جایا جائے تو، معلوم ہوتا ہے کہ اصل ایمبیڈڈ لنک کسی اور URL پر مشتمل ہے
5. ای میل میں گرامر کی غلطیاں یا ٹائپنگ کی خامیاں موجود ہو سکتی ہیں

<u>دوستانہ یاددہانی:</u>

اگر ای میل کے بارے میں شک ہو تو بینک کی کسٹمر سروس ہاٹ لائن کی تصدیق اس کے سرکاری ذرائع کے ذریعے کریں (جیسے ویب سائٹ خطوط یا تشہیری مواد) چاہے ای میل میں کوئی فون نمبر درج ہو۔

ہیکرز فِشنگ ای میل کو زیادہ اصلی ظاہر کرنے کے لیے اس کے آخر میں بعض اوقات سیکیورٹی سے متعلق تجاویز بھی شامل کر دیتے ہیں۔

3. کریڈٹ کارڈ فراڈ کے خلاف سمارٹ مشورے

وقتاً فوقتاً کریڈٹ کارڈ فراڈ کے واقعات پیش آتے رہتے ہیں جن میں فراڈ کرنے والے بدلتے ہوئے طریقۂ واردات اور مختلف دھوکہ دہی کی تکنیکیں استعمال کرتے ہیں۔ ہوشیار رہیں اور اپنے کارڈ کی معلومات کی حفاظت کریں تاکہ کریڈٹ کارڈ فراڈ کا شکار ہونے سے بچا جا سکے۔ ایک ذمہ دار کریڈٹ کارڈ کسٹمر کے طور پر آپ کو درج ذیل تجاویز پر توجہ دینی چاہیے:

- اپنے کریڈٹ کارڈز، کارڈ سے متعلق ڈیٹا اور متعلقہ تصدیقی عوامل (مثلاً ون ٹائم پاس ورڈ، موبائل ڈیوائس، وغیرہ) کی حفاظت میں مناسب احتیاط برتیں۔
- اپنے کریڈٹ کارڈ کی معلومات کسی تیسرے فریق کو فراہم نہ کریں، جن میں کارڈ نمبر میعاد ختم ہونے کی تاریخ سیکیورٹی کوڈ (جو عموماً کارڈ کے پچھلے حصے پر دستخط والے خانے کے قریب درج ہوتا ہے) اور ون ٹائم پاس ورڈ شامل ہیں۔
- ٹرانزیکشن کی منظوری کے لیے ذاتی اور کریڈٹ کارڈ کی معلومات فراہم کرنے سے پہلے تاجروں اور ویب سائٹس کی اصل حیثیت کی تصدیق کریں (مثلاً ہانگ کانگ پولیس فورس کے ''اسکیمیٹر'' کے ذریعے خطرے کی سطحیں یا الرٹس معلوم کریں) اور کسی بھی مشکوک کال SMS یا ای میل کے بارے میں ہوشیار رہیں (مثلاً فِشنگ پیغامات اکثر معتبر کمپنیوں تاجروں یا بینکوں کی جانب سے بھیجے جانے کا دعویٰ کرتے ہیں جن کا متن اور برانڈ لوگو بہت مشابہ ہوتا ہے اور ان میں جعلی ویب سائٹس کے ہائپر لنکس شامل ہوتے ہیں جو کارڈ ہولڈرز کو کریڈٹ کارڈ اور حساس ذاتی معلومات فراہم کرنے پر اکساتے ہیں۔)
- SMS میں موصول ہونے والے ون ٹائم پاس ورڈ کی تفصیلات غور سے چیک کریں، جس میں متعلقہ ٹرانزیکشن کی معلومات شامل ہیں (جس میں ٹرانزیکشن کی قسم، تاجر کا نام، رقم اور کرنسی وغیرہ شامل ہیں) اور اسمارٹ فون کے آٹو فل (AutoFill) فیچر کے استعمال میں محتاط رہیں۔ کبھی بھی ون ٹائم پاس ورڈ درج کرکے SMS میں ٹرانزیکشن کی تفصیلات کی تصدیق کیے بغیر ٹرانزیکشن جاری نہ کریں۔ ایک بار جب کارڈ کی معلومات (جس میں ون ٹائم پاس ورڈ شامل ہے) درج کر دی جاتی ہے تو ٹرانزیکشن منسوخ نہیں ہو سکتا اور کسٹمر اس ٹرانزیکشن کا ذمہ دار ہو سکتا ہے۔
- جب آپ نے کریڈٹ کارڈ کو کسی رابطے کے بغیر موبائل ادائیگی کی سروس کے ساتھ منسلک کیا ہو (جیسےGoogle Pay ،Apple Pay)، تو بینک اس موبائل نمبر پر ایک بائنڈنگ نوٹیفیکیشن بھیجے گا جو آپ نے بینک کے ساتھ رجسٹر کیا ہوا ہے، اور اس میں بتایا جائے گا کہ کریڈٹ کارڈ کو کس رابطے کے بغیر موبائل ادائیگی کی سروس کے ساتھ منسلک کیا گیا ہے۔ آپ کو نوٹیفیکیشن چیک کرنی چاہیے اور اگر آپ نے ایسی بائنڈنگ کی ہدایت نہیں دی ہے تو فوراً کارڈ جاری کرنے والے بینک کو اطلاع دیں۔ ایک بار بائنڈنگ کامیابی سے ہو جائے تو بعد میں ہونے والے ٹرانزیکشن کے لیے ون ٹائم پاس ورڈ کی ضرورت نہیں پڑ سکتی۔
- ہمیشہ بینکوں کی جانب سے بھیجے گئے مواصلاتی پیغامات (جیسے ای میلز، SMS وغیرہ) پر توجہ دیں۔ وقتاً فوقتاً اپنے کریڈٹ کارڈ کے ٹرانزیکشن کے ریکارڈ چیک کریں اور ماہانہ بیانات کی تصدیق کریں۔ اگر کوئی مشکوک یا غیر مجاز ٹرانزیکشن سامنے آئے تو فوری طور پر اپنے کارڈ جاری کرنے والے بینک کو اطلاع دیں، چاہے رقم کتنی بھی ہو۔
- اگر آپ کا کریڈٹ کارڈ کھو جائے، یا آپ کو شبہ ہو کہ آپ کے کارڈ یا کارڈ کی معلومات چوری ہو گئی ہیں، یا شبہ ہو کہ آپ کا کارڈ کسی مشکوک موبائل ڈیوائس کے ساتھ منسلک ہو گیا ہے، تو فوری طور پر اپنے کارڈ جاری کرنے والے بینک اور پولیس کو اطلاع دیں۔

اگر آپ اپنے کریڈٹ کارڈز اور کارڈ کی معلومات کا درست استعمال اور حفاظت نہیں کرتے، تو فراڈ کرنے والے اس موقع کا فائدہ اٹھا کر دھوکہ دہی کر سکتے ہیں (مثلاً آپ کے کارڈ چوری کر کے غیر مجاز کریڈٹ کارڈ ٹرانزیکشن کر سکتے ہیں)،

جس سے آپ کو مالی نقصان ہو سکتا ہے۔ مختصر یہ کہ اپنے کارڈ اور کارڈ کی معلومات کی حفاظت کریں تاکہ کریڈٹ کارڈ فراڈ کا شکار نہ ہوں۔

4. جعلی فون کالز اور SMS پیغامات کے خلاف سمارٹ مشورے

جب بھی آپ کو کالز، SMS، ای میلز، خطوط یا دیگر ذرائع سے ایسے پیغامات موصول ہوں جو بینک کی طرف سے ہونے کا دعویٰ کرتے ہوں، چاہے آپ کے اکاؤنٹ کو خطرہ بتایا جائے، آپ کے کریڈٹ کارڈ سے ٹرانزیکشن ہونے کا دعوی کیا جائے یا آپ کو پروموشنل مصنوعات میں کتنی بھی دلچسپی ہو، تو محتاط رہیں اور درج ذیل اقدامات کریں:

- کال کرنے والے یا بھیجنے والے کی شناخت کی تصدیق کریں؛
- صرف کال ڈسپلے پر بھروسہ نہ کریں تاکہ کال کرنے والے کی اصل شناخت معلوم ہو یا براہِ راست بینک ہاٹ لائن نمبر پر کال کرکے پیغامات میں دی گئی ہدایات پر عمل کریں؛
- اپنی حفاظت کے لیے حساس ذاتی معلومات آسانی سے فراہم نہ کریں۔

HKMA یا بینک کسی بھی فون کال، ای میل یا SMS کے ذریعے حساس ذاتی معلومات (جس میں لاگ اِن پاس ورڈز یا ون ٹائم پاس ورڈز شامل ہیں) طلب نہیں کرتے۔ نہ ہی وہ کسی اکاؤنٹ کی غیر معمولی صورتحال کی اطلاع پہلے سے ریکارڈ شدہ وائس میسجز کے ذریعے دیتے ہیں۔ آپ متعلقہ بینک کے ہاٹ لائن نمبرز ان کی سرکاری ویب سائٹس یا اپنے ATM/کریڈٹ کارڈز کے پچھلے حصے پر دیکھ سکتے ہیں۔ آپ ہانگ کانگ ایسوسی ایشن آف بینکس کی ویب سائٹ پر ان کالز کرنے والوں کی شناخت کی تصدیق کے لیے ریٹیل بینکس کے ہاٹ لائن نمبرز کی فہرست بھی دیکھ سکتے ہیں جن کے ذریعے اپنے آپ کو بینک کے نمائندے ظاہر کرنے والے کالرز کی شناخت کی تصدیق کی جا سکتی ہے۔ بینک کی ہاٹ لائن پر کال کر کے تصدیق کرنے کے بعد کسٹمر کے لیے سب سے محتاط طریقہ یہ ہے کہ وہ اس بینک کے نمائندے سے وہ فون نمبر استعمال کرتے ہوئے رابطہ کرے جو بینک سے حاصل کیا گیا ہو۔

5. کال کرنے والوں اور بینک ہاٹ لائن نمبرز کی تصدیق

آپ متعلقہ بینک کے ہاٹ لائن نمبرز ان کی سرکاری ویب سائٹس یا اپنے ATM/کریڈٹ کارڈز کے پچھلے حصے پر دیکھ سکتے ہیں۔ آپ ہانگ کانگ ایسوسی ایشن آف بینکس کی ویب سائٹ پر بھی وہ ریٹیل بینکس کے ہاٹ لائن نمبرز کی فہرست دیکھ سکتے ہیں جو بینک کے نمائندے ہونے کا دعویٰ کرنے والے کال کرنے والوں کی شناخت کی تصدیق کے لیے استعمال ہوتی ہے۔

6. فراڈ کے معاملات کے بارے میں عمومی سوالات (FAQs)

A. کیا مجھے ہانگ کانگ سے کسی اور جگہ رقم ٹرانسفر کرنے کے لیے مالی بیمہ یا ٹرانسفر فیس ادا کرنی ہوگی؟

بنیادی قانون کے آرٹیکل 112 کے مطابق، "ہانگ کانگ خصوصی انتظامی علاقے میں کسی بھی طرح کی غیر ملکی زرمبادلہ کنٹرول پالیسی لاگو نہیں ہوگی۔ ہانگ کانگ ڈالر آزادانہ طور پر قابل تبادلہ ہوگا۔ غیر ملکی زرمبادلہ، سونا، سیکیورٹیز، فیوچرز اور اسی طرح کے مارکیٹس جاری رہیں گے۔ ہانگ کانگ خصوصی انتظامی علاقے کی حکومت خطے کے اندر، اندر اور باہر کی سرمائے کی آزادانہ حرکت کی حفاظت کرے گی۔" اس کا مطلب ہے کہ ہانگ کانگ میں رقم ٹرانسفر کرنے پر کوئی پابندی نہیں ہے اور HKMA کسی بھی قسم کی ٹرانسفر فیس عائد نہیں کرتا۔

B. کیا آپ تصدیق کر سکتے ہیں کہ مجھے وہ لاٹری رقم حاصل کرنے سے پہلے کسی مخصوص بینک اکاؤنٹ میں پیشگی فیس جمع کرانی ہوگی جس کے جیتنے کا مجھے بتایا گیا ہے؟

ہمیں شبہ ہے کہ آپ کو کسی فراڈ کا سامنا کر ہو رہا ہے۔ HKMA ہانگ کانگ میں بینکنگ کا ضابطہ کار ہے اور ہمارا کسی بھی قسم کی لاٹری سرگرمی سے کوئی تعلق نہیں ہے۔

اس کے علاوہ، بنیادی قانون کے آرٹیکل 112 کے مطابق، "ہانگ کانگ خصوصی انتظامی علاقے میں کسی بھی طرح کی غیر ملکی زرمبادلہ کنٹرول پالیسی لاگو نہیں ہوگی۔ ہانگ کانگ ڈالر آزادانہ طور پر قابل تبادلہ ہوگا۔ غیر ملکی زرمبادلہ، سونا، سیکیورٹیز، فیوچرز اور اسی طرح کے مارکیٹس جاری رہیں گے۔ ہانگ کانگ خصوصی انتظامی علاقے کی حکومت خطے کے اندر، اندر اور باہر کی سرمائے کی آزادانہ حرکت کی حفاظت کرے گی۔" اس کا مطلب یہ ہے کہ ہانگ کانگ میں رقم کی منتقلی پر کوئی پابندی نہیں ہے اور حکومت کسی بھی قسم کی ٹرانسفر فیس کا مطالبہ نہیں کرتی۔

اگر آپ کو شبہ ہو کہ فراڈ سرگرمیاں شامل ہیں، تو آپ اس معاملے کی رپورٹ مقامی پولیس اسٹیشن یا ہانگ کانگ پولیس فورس کے کمرشل کرائم بیورو کو براہِ راست کر سکتے ہیں۔

C. اگر مجھے مشکوک فراڈ والے بینک ای میلز یا فون کالز موصول ہوں، یا مشکوک فراڈ والے بینک ویب سائٹس کا سامنا ہو تو مجھے کیا کرنا چاہیے؟

اگر آپ کو کوئی مشکوک پیغامات موصول ہوں یا کوئی مشکوک ویب سائٹس نظر آئیں جو بینک سے متعلق ہونے کا دعویٰ کرتی ہوں، تو براہِ کرم متعلقہ بینک اور پولیس (یا تو مقامی پولیس اسٹیشن یا کمرشل کرائم بیورو) سے رابطہ کریں اور اپنا کیس رپورٹ کریں۔

"لنکس پر کلک کریں، فراڈ کا شکار ہو جائیں!" (30 سیکنڈ ویڈیو) – ٹرانسکرپٹ

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

English		**Translation**	
Scammer:	Download the app to verify your information or you will face detention	اپنی معلومات کی تصدیق کرنے کے لیے ایپ ڈاؤن لوڈ کریں ورنہ آپ کو حراست کا سامنا کرنا پڑے گا	فراڈ کرنے والا:
Superimposed text:	...Download the app to verify your information, or you will face detention...	---اپنی معلومات کی تصدیق کرنے کے لیے ایپ ڈاؤن لوڈ کریں، ورنہ آپ کو حراست کا سامنا کرنا پڑے گا---	اوپر لکھا متن:
University student:	What?	کیا؟	یونیورسٹی طالب علم:
Voice-over:	Think there’s a misunderstanding?	لگتا ہے کچھ غلط فہمی ہو گئی ہے؟	وائس اوور:
Mother:	Why not find a part-time job?	کیوں نہ پارٹ ٹائم نوکری تلاش کریں؟	ماں:
Son:	Mom! Look at this job!	امی! اس نوکری کو دیکھیں!	بیٹا:
Voice-over:	Think you've found a dream job?	لگتا ہے آپ نے پسندیدہ نوکری تلاش کر لی ہے؟	وائس اوور:
Superimposed text:	...Great jobs available. Provide personal information to facilitate salary payment...	--- بہترین نوکریاں دستیاب ہیں۔ تنخواہ کی ادائیگی کے لیے ذاتی معلومات فراہم کریں---	اوپر لکھا متن:

Middle-aged woman:	Sure-win investment group with insider tips and recommendations?	یقیناً جیتنے والا سرمایہ کاری گروپ اندرونی معلومات اور سفارشات کے ساتھ؟	درمیانی عمر کی خاتون:
Superimposed text:	…Sure-win investment group, open your account now…	...یقیناً جیتنے والا سرمایہ کاری گروپ، ابھی اپنا اکاؤنٹ کھولیں...	اوپر لکھا متن:
Voice-over:	Think sure-win investment options are just lying around? One click on the wrong link can bring disaster	کیا آپ سمجھتے ہیں کہ یقیناً جیتنے والے سرمایہ کاری کے مواقع آسانی سے دستیاب ہیں؟ ایک غلط لنک پر کلک آپ کے لیے تباہی لا سکتا ہے۔	وائس اوور:
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/	براہِ کرم ایپ ڈاؤن لوڈ کرنے کے لیے لنک پر کلک کریں اور اپنی ذاتی معلومات، شناختی نمبر، بینک اکاؤنٹ لاگ اِن نام اور پاس ورڈ فراہم کریں http://xxbank.vip/	اوپر لکھا متن:
Voice-over:	Be cautious of fake links or you will regret it for life	جعلی لنکس سے محتاط رہیں ورنہ آپ عمر بھر پچھتائیں گے۔	وائس اوور:
Son:	My money and personal information!	میری رقم اور ذاتی معلومات!	بیٹا:
Voice-over:	Click the links fall for scams	لنکس پر کلک کریں فراڈ کا شکار ہو جائیں	وائس اوور:
Superimposed text:	Click the links Fall for scams	لنکس پر کلک کریں فراڈ کا شکار ہو جائیں	اوپر لکھا متن:

” تین فراڈ مخالف حربے“ – ونٹیج کانٹونیز اینٹی-فراڈ ویڈیو:(1)

پولیس یا قانون نافذ کرنے والے بن کر دھوکہ دینے والے سے بچاؤ

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

English		**Translation**	
Superimposed text:	Vintage Cantonese Anti-Scam Video (1)	ونٹیج کانٹونیز اینٹی-فراڈ ویڈیو (1)	اوپر لکھا متن:
Leading actress:	Who's calling?	کون کال کر رہا ہے؟	مرکزی اداکارہ:
Scammer:	I am a law enforcement officer. You have committed an offence!	میں قانون نافذ کرنے والا افسر ہوں۔ آپ نے جرم کیا ہے!	فراڈ کرنے والا:
Leading actress:	How could I have committed any offence? Don't wrong me	میں نے کیسے کوئی جرم کیا ہو سکتا ہے؟ میرے ساتھ ناانصافی نہ کریں	مرکزی اداکارہ:
Scammer:	You know it well whether you have committed an offence or not I have issued an arrest warrant against you	آپ خود اچھی طرح جانتے ہیں کہ آپ نے جرم کیا ہے یا نہیں میں نے آپ کے خلاف گرفتاری کا وارنٹ جاری کر دیا ہے۔	فراڈ کرنے والا:
Leading actress:	What?	کیا؟	مرکزی اداکارہ:
Scammer:	Cooperate and give me your bank account number and password Otherwise, you will be sent to prison	تعاون کریں اور مجھے اپنا بینک اکاؤنٹ نمبر اور پاس ورڈ دیں ورنہ آپ کو جیل بھیج دیا جائے گا	فراڈ کرنے والا:

Leading actress:	No way! My...my... My account number is...	بالکل نہیں! میرا--- میرا--- میرا اکاؤنٹ نمبر ہے---	مرکزی اداکارہ:
Male host of TV promotional video:	Scammers have many tricks; believe them and you'll be in a fix	فراڈ کرنے والوں کے پاس بہت سے حربے ہوتے ہیں؛ اگر آپ ان پر یقین کریں گے تو آپ مشکل میں پھنس جائیں گے۔	ٹی وی پروموشنل ویڈیو کے مرد میزبان:
Leading actress:	Humph! Needless to say This person must be a scammer	ہمف! کہنے کی ضرورت نہیں یہ شخص یقینی طور پر فراڈ کرنے والا ہے	مرکزی اداکارہ:
Leading actress:	Let me apply the "Three Anti-Scam Tactics"	آئیے "تین اینٹی-فراڈ حربے" آزمائیں۔	مرکزی اداکارہ:
Superimposed text:	Three Anti-Scam Tactics	تین اینٹی-فراڈ حربے	اوپر لکھا متن:
Leading actress:	Keep Calm	پرسکون رہیں	مرکزی اداکارہ:
Superimposed text:	Keep Calm Keep calm, don't panic	پرسکون رہیں پرسکون رہیں، گھبرائیں مت	اوپر لکھا متن:
Leading actress:	Give Nothing	کچھ نہ دیں	مرکزی اداکارہ:
Superimposed text:	Give Nothing Give no personal data or money	کچھ نہ دیں کوئی ذاتی معلومات یا رقم نہ دیں	اوپر لکھا متن:
Leading actress:	Verify and Seek Help	تصدیق کریں اور مدد حاصل کریں	مرکزی اداکارہ:

Superimposed text:	Verify and Seek Help Verify the caller's identity and seek help from others	تصدیق کریں اور مدد حاصل کریں کال کرنے والے کی شناخت کی تصدیق کریں اور دوسروں سے مدد حاصل کریں	اوپر لکھا متن:
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	تمہارے پاس اپنے حربے ہیں، لیکن میرے پاس گرفتاری کا وارنٹ ہے۔ میں تو صرف ہدایات پر عمل کر رہا ہوں۔ جلدی کرو اور اپنی رقم اور بینک اکاؤنٹ کا پاس ورڈ حوالے کر دو۔	فراڈ کرنے والا:
Leading actress:	Ha! Law enforcement officers will not request for account information Your arrest warrant is fake I have discerned your hoax	ہا! قانون نافذ کرنے والے افسران اکاؤنٹ کی معلومات طلب نہیں کرتے۔ تمہارا گرفتاری کا وارنٹ جعلی ہے۔ میں تمہاری اس دھوکہ دہی کو پہچان چکی ہوں۔	مرکزی اداکارہ:
Leading actress:	Watch this!	یہ دیکھیں!	مرکزی اداکارہ:
Scammer:	Argh...	آرغ---	فراڈی:
Superimposed text:	The End	اختتام	اوپر لکھا متن:
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	چاہے یہ حربہ کتنا ہی پرانا کیوں نہ ہو، ہمیشہ ایسے لوگ ہوتے ہیں جو اس کا شکار ہو جاتے ہیں۔ "تین اینٹی-فراڈ حربے" کو یاد رکھیں۔ فراڈ کرنے والے اب مزید بے لگام نہیں رہیں گے۔	مرکزی اداکارہ:

Superimposed text:	Remember the "Three Anti-Scam Tactics"! Scammers can no longer play tricks!	"تین اینٹی-فراڈ حربے" کو یاد رکھیں! فراڈ کرنے والوں کے اب مزید حربے نہیں چل سکتے!	اوپر لکھا متن:
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	اس کے علاوہ، HKMA نے "منی سیف" سروس متعارف کروائی ہے بالکل سیف کی طرح، یہ جمع شدہ رقم کے لیے اضافی حفاظتی تہہ فراہم کرتی ہے	مرکزی اداکارہ:
Superimposed text:	Money Safe	منی سیف	اوپر لکھا متن:
Leading actress:	Contact your bank for details now	مزید تفصیلات کے لیے ابھی اپنے بینک سے رابطہ کریں	مرکزی اداکارہ:
Superimposed text:	(Hong Kong Monetary Authority Logo)	(ہانگ کانگ مانیٹری اتھارٹی کا لوگو)	اوپر لکھا متن:

”تین فراڈ مخالف حربے“ – پرانی کانٹونیز اینٹی-فراڈ ویڈیو(2):

ڈیپ فیک ٹیکنالوجی کو بے نقاب کریں

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

English		**Translation**	
Superimposed text:	Vintage Cantonese Anti-Scam Video (2)	پرانی کانٹونیز اینٹی-فراڈ ویڈیو (2)	اوپر لکھا متن:
Superimposed text:	Three months ago	تین ماہ قبل	اوپر لکھا متن:
Son:	I am leaving for the capital for business Father, take good care of yourself!	میں کاروبار کے لیے دار الحکومت جا رہا ہوں ابا، اپنا خیال رکھنا!	بیٹا:
Father:	Be careful and stay safe	محتاط رہو اور محفوظ رہو	ابا:
Fake Son:	Father! Save me!	ابا! مجھے بچائیں!	جعلی بیٹا:
Father:	Why are you so scared?	تم اتنے ڈرے ہوئے کیوں ہو؟	ابا:
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! Transfer money to the account which I've just sent you immediately!	میں دارالحکومت جاتے ہوئے ڈاکوؤں کے ہاتھوں لوٹ لیا گیا میرا سارا سامان اور پیسہ چلا گیا، اور میں سامان بروقت پہنچا نہیں سکا مجھے اپنے گاہکوں کو ان کے نقصان کی تلافی کرنی ہوگی! فوراً رقم اس اکاؤنٹ میں منتقل کریں جو میں نے ابھی بھیجا ہے!	جعلی بیٹا:

Father:	For my son's sake, I had no choice but to…	اپنے بیٹے کے لیے، میرے پاس کوئی چارہ نہیں تھا مگر---	ابا:
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"!	رکیں جو جعلی ہے وہ اصلی لگتا ہے اور جو اصلی ہے وہ جعلی لگتا ہے جناب آئیے میں آپ کے ساتھ "تین اینٹی-فراڈ حربے" شیئر کروں!	ماسٹر:
Superimposed text:	Three Anti-Scam Tactics	تین اینٹی-فراڈ حربے	اوپر لکھا متن:
Master:	Tactic One Keep Calm	پہلا حربہ پرسکون رہیں	ماسٹر:
Superimposed text:	Keep Calm Keep calm, don't panic	پرسکون رہیں پرسکون رہیں، گھبرائیں مت	اوپر لکھا متن:
Master:	Tactic Two Give Nothing	دوسرا حربہ کچھ نہ دیں	ماسٹر:
Superimposed text:	Give Nothing Give no personal data or money	کچھ نہ دیں کوئی ذاتی معلومات یا رقم نہ دیں	اوپر لکھا متن:
Master:	Tactic Three Verify and Seek Help	تیسرا حربہ تصدیق کریں اور مدد حاصل کریں	ماسٹر:
Superimposed text:	Verify and Seek Help Verify the caller's identity and seek help from others	تصدیق کریں اور مدد حاصل کریں کال کرنے والے کی شناخت کی تصدیق کریں اور دوسروں سے مدد حاصل کریں	اوپر لکھا متن:
Master:	Sir, remember these words	جناب، ان باتوں کو یاد رکھیں	ماسٹر:

Father:	Your uncle is an official working in the capital Why not reach out to him for help?	تمہارا چچا دارالحکومت میں ایک اہلکار ہیں کیوں نہ ان سے مدد طلب کی جائے؟	ابا:
Fake Son:	Uncle is overwhelmed with responsibilities and not available!	چچا اپنی ذمہ داریوں میں بہت مصروف ہیں اور دستیاب نہیں ہیں!	جعلی بیٹا:
Father:	Humph! Uncle has already retired and returned home! You evil monster! How dare you impersonate my beloved son using “deepfake”!	ہمف! چچا پہلے ہی ریٹائر ہو کر گھر واپس آ چکے ہیں! تم شیطانی درندہ ہو! تمہاری جرات کیسے ہوئی کہ میرے پیارے بیٹے نقالی "ڈیپ فیک" کے ذریعے کرو!	ابا:
Superimposed text:	Goodbye	الوداع	اوپر لکھا متن:
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	چاہے یہ حربہ کتنا ہی پرانا کیوں نہ ہو، ہمیشہ ایسے لوگ ہوتے ہیں جو اس کا شکار ہو جاتے ہیں۔ "تین اینٹی-فراڈ حربے" کو یاد رکھیں۔ فراڈ کرنے والے اب مزید بے لگام نہیں رہیں گے۔	ماسٹر:
Superimposed text:	Remember the "Three Anti-Scam Tactics"! Scammers can no longer play tricks!	"تین اینٹی-فراڈ حربے" کو یاد رکھیں! فراڈ کرنے والوں کے اب مزید حربے نہیں چل سکتے!	اوپر لکھا متن:
Master:	In addition, the HKMA has launched the "Money Safe" service	اس کے علاوہ، HKMA نے "منی سیف" سروس متعارف کروائی ہے	ماسٹر:

Superimposed text:	Money Safe	منی سیف	اوپر لکھا متن:
Master:	Just like a treasure box, it adds an extra layer of protection for deposits Contact your bank for details now	بالکل خزانے کے ڈبے کی طرح، یہ جمع شدہ رقم کے لیے اضافی حفاظتی تہہ فراہم کرتی ہے مزید تفصیلات کے لیے ابھی اپنے بینک سے رابطہ کریں	ماسٹر:
Superimposed text:	(Hong Kong Monetary Authority Logo)	(ہانگ کانگ مانیٹری اتھارٹی کا لوگو)	اوپر لکھا متن: