Cảnh giác với kẻ lừa đảo: Mẹo thông minh dành cho người tiêu dùng

1. Mẹo phòng tránh tin nhắn SMS và email lừa đảo (phishing)

Theo yêu cầu giám sát của Cơ quan Tiền tệ Hồng Kông (HKMA), các ngân hàng sẽ không gửi tin nhắn SMS hoặc email có chứa liên kết nhúng dẫn khách hàng đến website hoặc ứng dụng di động của họ để thực hiện giao dịch. Ngân hàng cũng không yêu cầu khách hàng cung cấp thông tin cá nhân nhạy cảm, bao gồm mật khẩu đăng nhập và mã OTP, thông qua các liên kết.

Nếu bạn nhận được SMS hoặc email có chứa liên kết yêu cầu nhập thông tin đăng nhập ngân hàng trực tuyến, thì những tin nhắn này không phải do ngân hàng gửi. Bạn nên suy nghĩ kỹ trước khi nhấp vào bất kỳ liên kết nào được cho là từ ngân hàng. Nếu bạn thấy các liên kết (hoặc tệp đính kèm) trong SMS hoặc email có dấu hiệu đáng ngờ, không nhấp vào liên kết (hoặc mở tệp đính kèm). Bạn nên luôn truy cập dịch vụ ngân hàng trực tuyến bằng cách nhập trực tiếp địa chỉ website của ngân hàng, hoặc sử dụng dấu trang đã lưu, hoặc ứng dụng ngân hàng trực tuyến trên điện thoại.

Nếu có bất kỳ thắc mắc nào, khách hàng có thể liên hệ trực tiếp với ngân hàng liên quan qua các kênh khác (ví dụ: đường dây nóng chăm sóc khách hàng của ngân hàng) để xác minh tính xác thực của SMS hoặc email.

Thông tin đăng nhập ngân hàng trực tuyến, bao gồm tên người dùng, mật khẩu và mã xác thực một lần (OTP), quan trọng trong thế giới số cũng giống như chìa khóa nhà trong đời thực, vì vậy cần được bảo vệ cẩn thận.

2. Ví dụ email lừa đảo giả mạo ngân hàng

Năm đặc điểm thường gặp:

1. Không ghi rõ tên người nhận (tức là gửi cho người nhận không xác định).
2. Tên và địa chỉ email của người gửi có thể trông giống hệt thông tin thật của ngân hàng liên quan.
3. Email thường có nội dung như một thông báo quan trọng từ ngân hàng (ví dụ: “Thông báo có giao dịch chuyển tiền giá trị lớn trong tài khoản của khách hàng” hoặc “Yêu cầu khách hàng kích hoạt chức năng bảo mật mới, nếu không một số dịch vụ ngân hàng (như dịch vụ chuyển tiền) sẽ bị tạm ngưng”). Khách hàng sẽ được yêu cầu nhấp vào liên kết hoặc mở tệp đính kèm trong email.
4. Email thường chứa một liên kết trông giống địa chỉ website chính thức của ngân hàng. Tuy nhiên, khi di chuột lên liên kết, bạn sẽ thấy đường dẫn thực tế được nhúng là một URL khác.
5. Trong email có thể xuất hiện lỗi ngữ pháp hoặc lỗi chính tả.

Lời nhắc thân thiện:

Nếu bạn nghi ngờ về tính xác thực của email, hãy kiểm tra số điện thoại chăm sóc khách hàng của ngân hàng thông qua các kênh chính thức (ví dụ: website, thư từ hoặc tài liệu quảng bá), ngay cả khi email có hiển thị số điện thoại.

Tin tặc có thể thêm một số mẹo bảo mật ở cuối email lừa đảo để làm cho email trông giống thật hơn.

3. Mẹo thông minh phòng tránh lừa đảo thẻ tín dụng

Các vụ lừa đảo thẻ tín dụng vẫn xảy ra theo từng thời điểm, với thủ đoạn ngày càng tinh vi và nhiều chiêu trò khác nhau do kẻ gian sử dụng. Hãy luôn cảnh giác và bảo vệ thông tin thẻ của bạn để tránh trở thành nạn nhân của lừa đảo thẻ tín dụng. Là một người dùng thẻ tín dụng thông minh, bạn nên lưu ý các điều sau:

- Cẩn trọng và áp dụng các biện pháp bảo vệ thẻ tín dụng, dữ liệu thẻ và các yếu tố xác thực liên quan (ví dụ: mã OTP, thiết bị di động, v.v.).
- Không tiết lộ cho bên thứ ba thông tin thẻ tín dụng của bạn, bao gồm số thẻ, ngày hết hạn, mã bảo mật (thường in ở mặt sau thẻ, cạnh ô chữ ký) và mã OTP.
- Xác minh tính xác thực của người bán và website (ví dụ: tra cứu mức độ rủi ro/cảnh báo qua công cụ "Scameter" của Lực lượng Cảnh sát Hồng Kông) trước khi cung cấp thông tin cá nhân và thông tin thẻ tín dụng để thực hiện giao dịch. Đồng thời, luôn cảnh giác với các cuộc gọi, SMS hoặc email đáng ngờ (ví dụ: tin nhắn lừa đảo thường giả mạo là do các công ty, cửa hàng hoặc ngân hàng uy tín gửi, với nội dung và logo rất giống thật, và thường chứa liên kết dẫn đến website giả để dụ chủ thẻ cung cấp thông tin thẻ và dữ liệu cá nhân nhạy cảm).
- Kiểm tra kỹ nội dung SMS chứa mã OTP, bao gồm thông tin giao dịch liên quan (như loại giao dịch, tên đơn vị chấp nhận thẻ, số tiền và loại tiền tệ, v.v.), và cẩn trọng khi sử dụng tính năng tự động điền (AutoFill) trên điện thoại thông minh. Tuyệt đối không nhập mã OTP và tiếp tục giao dịch nếu chưa xác minh rõ chi tiết giao dịch trong SMS. Sau khi thông tin thẻ (bao gồm mã OTP) đã được nhập, giao dịch có thể không hủy được và khách hàng có thể phải chịu trách nhiệm cho giao dịch đó.
- Sau khi bạn liên kết thẻ tín dụng với dịch vụ thanh toán di động không tiếp xúc (ví dụ: Apple Pay, Google Pay), ngân hàng sẽ gửi thông báo liên kết đến số điện thoại bạn đã đăng ký với ngân hàng, nêu rõ dịch vụ thanh toán di động mà thẻ đã được liên kết. Bạn nên kiểm tra thông báo này và liên hệ ngay với ngân hàng phát hành thẻ nếu bạn không thực hiện yêu cầu liên kết đó. Sau khi liên kết thành công, các giao dịch sau này có thể không cần mã OTP.
- Luôn chú ý đến các thông báo liên lạc (như email, SMS, v.v.) từ ngân hàng. Thường xuyên kiểm tra lịch sử giao dịch thẻ tín dụng và đối chiếu sao kê hàng tháng. Báo ngay cho ngân hàng phát hành thẻ nếu phát hiện bất kỳ giao dịch đáng ngờ hoặc trái phép nào, bất kể số tiền lớn hay nhỏ.
- Báo ngay cho ngân hàng phát hành thẻ và cơ quan Cảnh sát nếu bạn làm mất thẻ tín dụng, nghi ngờ thẻ hoặc thông tin thẻ bị đánh cắp, hoặc nghi ngờ thẻ của bạn đã bị liên kết với một thiết bị di động đáng ngờ.

Nếu bạn không sử dụng hoặc bảo vệ thẻ tín dụng và thông tin thẻ đúng cách, kẻ gian có thể lợi dụng sơ hở đó để thực hiện hành vi gian lận (ví dụ: đánh cắp thẻ để thực hiện giao dịch trái phép), gây tổn thất tài chính cho bạn. Tóm lại, hãy luôn bảo vệ thẻ và thông tin thẻ của mình để tránh trở thành nạn nhân của lừa đảo thẻ tín dụng.

4. Mẹo thông minh phòng tránh cuộc gọi và tin nhắn SMS giả mạo

Khi nhận được các cuộc gọi, SMS, email, thư từ hoặc bất kỳ hình thức liên lạc nào khác tự nhận là từ ngân hàng, dù họ nói tài khoản của bạn đang gặp rủi ro, có giao dịch được thực hiện bằng thẻ tín dụng của bạn, hay bạn quan tâm đến các sản phẩm đang được quảng bá, bạn vẫn cần phải thận trọng và:

- Xác minh danh tính của người gọi hoặc người gửi;
- Tránh chỉ dựa vào số điện thoại hiển thị cuộc gọi đến để xác định danh tính thật của người gọi, hoặc gọi trực tiếp vào số hotline ngân hàng được cung cấp trong tin nhắn rồi làm theo hướng dẫn; và
- Không dễ dàng cung cấp thông tin cá nhân nhạy cảm để bảo vệ quyền lợi của chính mình.

HKMA và các ngân hàng không yêu cầu cung cấp bất kỳ thông tin cá nhân nhạy cảm nào, bao gồm mật khẩu đăng nhập hoặc mã OTP, qua điện thoại, email hoặc SMS. Họ cũng không thông báo về các bất thường trong tài khoản thông qua tin nhắn thoại ghi âm sẵn. Bạn có thể tra cứu số hotline của các ngân hàng liên quan trên website chính thức của họ hoặc ở mặt sau thẻ ATM hoặc thẻ tín dụng. Bạn cũng có thể tìm danh sách hotline của các ngân hàng bán lẻ để xác minh danh tính người gọi tự xưng là đại diện ngân hàng trên website của Hiệp hội Ngân hàng Hồng Kông. Sau khi gọi đến hotline ngân hàng để xác thực, cách an toàn nhất để tiếp tục là liên hệ lại với đại diện ngân hàng qua số điện thoại do chính ngân hàng cung cấp.

5. Xác minh người gọi và số hotline của ngân hàng

Bạn có thể tra cứu số hotline của các ngân hàng liên quan trên website chính thức của từng ngân hàng hoặc ở mặt sau thẻ ATM hoặc thẻ tín dụng của bạn. Bạn cũng có thể tìm danh sách hotline của các ngân hàng bán lẻ dùng để xác minh danh tính người gọi tự xưng là đại diện ngân hàng trên website của Hiệp hội Ngân hàng Hồng Kông.

6. Câu hỏi thường gặp về các vụ lừa đảo

A. Tôi có cần phải trả phí bảo hiểm tài chính hoặc phí chuyển tiền khi chuyển tiền từ Hồng Kông ra nước ngoài không?

Theo Điều 112 của Luật Cơ bản, "Không áp dụng chính sách kiểm soát ngoại hối tại Đặc khu Hành chính Hồng Kông. Đồng đô la Hồng Kông được tự do chuyển đổi. Các thị trường ngoại hối, vàng, chứng khoán, hợp đồng tương lai và các thị trường tương tự tiếp tục hoạt động. Chính quyền Đặc khu Hành chính Hồng Kông bảo đảm sự lưu chuyển tự do của vốn trong, vào và ra khỏi khu vực." Điều này có nghĩa là không có hạn chế nào đối với việc chuyển tiền tại Hồng Kông và HKMA không thu bất kỳ loại phí nào đối với việc chuyển tiền.

B. Bạn có thể xác minh giúp tôi có cần phải nộp một khoản phí ứng trước vào tài khoản ngân hàng được chỉ định trước khi nhận số tiền trúng xổ số mà tôi được thông báo là đã trúng không?

Chúng tôi nghi ngờ bạn đã gặp phải một vụ lừa đảo. HKMA là cơ quan quản lý ngân hàng tại Hồng Kông và không có bất kỳ mối liên hệ nào với các hoạt động xổ số.

Ngoài ra, theo Điều 112 của Luật Cơ bản, "Không áp dụng chính sách kiểm soát ngoại hối tại Đặc khu Hành chính Hồng Kông. Đồng đô la Hồng Kông được tự do chuyển đổi. Các thị trường ngoại hối, vàng, chứng khoán, hợp đồng tương lai và các thị trường tương tự tiếp tục hoạt động. Chính quyền Đặc khu Hành chính Hồng Kông bảo đảm sự lưu chuyển tự do của vốn trong, vào và ra khỏi khu vực." Điều này có nghĩa là không có hạn chế nào đối với việc chuyển tiền tại Hồng Kông và chính phủ không yêu cầu bất kỳ loại phí nào cho việc chuyển tiền.

Nếu bạn nghi ngờ có hành vi lừa đảo, bạn nên báo cáo vụ việc trực tiếp cho đồn cảnh sát địa phương hoặc Cục Điều tra Tội phạm Thương mại của Lực lượng Cảnh sát Hồng Kông.

C. Tôi nên làm gì nếu nhận được email hoặc cuộc gọi ngân hàng nghi ngờ là lừa đảo, hoặc phát hiện website ngân hàng nghi ngờ là giả mạo?

Nếu bạn nhận được bất kỳ tin nhắn đáng ngờ nào hoặc phát hiện các website đáng ngờ tự xưng có liên quan đến ngân hàng, vui lòng liên hệ với ngân hàng liên quan và báo cáo vụ việc cho cảnh sát (tại đồn cảnh sát địa phương hoặc Cục Điều tra Tội phạm Thương mại).

“Nhấp vào liên kết, sập bẫy lừa đảo!” (video 30 giây) – Lời thoại

Liên kết Video: https://www.youtube.com/watch?v=T1vEFnbiWh4

English		**Translation**	
Scammer:	Download the app to verify your information or you will face detention	Kẻ lừa đảo:	Tải ứng dụng để xác minh thông tin của bạn, nếu không bạn sẽ bị tạm giam
Superimposed text:	...Download the app to verify your information, or you will face detention...	Chữ hiển thị trên màn hình:	…Tải ứng dụng để xác minh thông tin của bạn, nếu không bạn sẽ bị tạm giam…
University student:	What?	Sinh viên đại học:	Cái gì?
Voice-over:	Think there’s a misunderstanding?	Lời dẫn:	Bạn nghĩ có sự nhầm lẫn sao?
Mother:	Why not find a part-time job?	Mẹ:	Sao con không tìm một công việc bán thời gian?
Son:	Mom! Look at this job!	Con trai:	Mẹ ơi! Nhìn công việc này nè!
Voice-over:	Think you've found a dream job?	Lời dẫn:	Bạn nghĩ mình đã tìm được công việc mơ ước?
Superimposed text:	...Great jobs available. Provide personal information to facilitate salary payment...	Chữ hiển thị trên màn hình:	…Có nhiều việc làm hấp dẫn. Hãy cung cấp thông tin cá nhân để thuận tiện cho việc trả lương…
Middle-aged woman:	Sure-win investment group with insider tips and recommendations?	Phụ nữ trung niên:	Nhóm đầu tư chắc thắng với thông tin nội bộ và khuyến nghị sao?
Superimposed text:	…Sure-win investment group,	Chữ hiển thị	…Nhóm đầu tư chắc thắng,

	open your account now…	trên màn hình:	mở tài khoản ngay…
Voice-over:	Think sure-win investment options are just lying around? One click on the wrong link can bring disaster	Lời dẫn:	Bạn nghĩ cơ hội đầu tư chắc thắng có sẵn khắp nơi sao? Chỉ một cú nhấp nhầm liên kết cũng có thể dẫn đến thảm họa
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/	Chữ hiển thị trên màn hình:	Vui lòng nhấp vào liên kết để tải ứng dụng và cung cấp thông tin cá nhân, số CMND, tên đăng nhập và mật khẩu tài khoản ngân hàng http://xxbank.vip/
Voice-over:	Be cautious of fake links or you will regret it for life	Lời dẫn:	Hãy cảnh giác với các liên kết giả mạo, nếu không bạn sẽ hối hận cả đời
Son:	My money and personal information!	Con trai:	Tiền của con và thông tin cá nhân của con!
Voice-over:	Click the links fall for scams	Lời dẫn:	Nhấp vào liên kết, sập bẫy lừa đảo
Superimposed text:	Click the links Fall for scams	Chữ hiển thị trên màn hình:	Nhấp vào liên kết Sập bẫy lừa đảo

“Ba Chiêu Chống Lừa Đảo” - Video chống lừa đảo phong cách Quảng Đông cổ điển (1): Đối phó với hành vi giả mạo cơ quan thực thi pháp luật

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

English		**Translation**	
Superimposed text:	Vintage Cantonese Anti-Scam Video (1)	Chữ trên màn hình:	Video chống lừa đảo phong cách Quảng Đông cổ điển (1)
Leading actress:	Who’s calling?	Nữ chính:	Ai gọi đấy?
Scammer:	I am a law enforcement officer. You have committed an offence!	Kẻ lừa đảo:	Tôi là nhân viên thực thi pháp luật. Cô đã phạm tội!
Leading actress:	How could I have committed any offence? Don't wrong me	Nữ chính:	Sao tôi có thể phạm tội được chứ? Đừng vu oan cho tôi
Scammer:	You know it well whether you have committed an offence or not I have issued an arrest warrant against you	Kẻ lừa đảo:	Cô biết rõ mình có phạm tội hay không. Tôi đã phát lệnh bắt giữ cô
Leading actress:	What?	Nữ chính:	Cái gì?
Scammer:	Cooperate and give me your bank account number and password Otherwise, you will be sent to prison	Kẻ lừa đảo:	Hợp tác và đưa tôi số tài khoản ngân hàng cùng mật khẩu. Nếu không, cô sẽ bị tống vào tù
Leading actress:	No way! My...my...	Nữ chính:	Không đời nào! Số… số…

	My account number is...		Số tài khoản của tôi là…
Male host of TV promotional video:	Scammers have many tricks; believe them and you'll be in a fix	Nam MC quảng bá:	Kẻ lừa đảo có rất nhiều chiêu trò, tin chúng là gặp rắc rối ngay
Leading actress:	Humph! Needless to say This person must be a scammer	Nữ chính:	Hừ! Khỏi phải nói, người này chắc chắn là kẻ lừa đảo
Leading actress:	Let me apply the "Three Anti-Scam Tactics"	Nữ chính:	Để tôi áp dụng “Ba Chiêu Chống Lừa Đảo”
Superimposed text:	Three Anti-Scam Tactics	Chữ trên màn hình:	Ba Chiêu Chống Lừa Đảo
Leading actress:	Keep Calm	Nữ chính:	Bình tĩnh
Superimposed text:	Keep Calm Keep calm, don't panic	Chữ trên màn hình:	Bình tĩnh. Giữ bình tĩnh, đừng hoảng loạn
Leading actress:	Give Nothing	Nữ chính:	Không cung cấp gì
Superimposed text:	Give Nothing Give no personal data or money	Chữ trên màn hình:	Không cung cấp gì. Không cung cấp dữ liệu cá nhân hoặc tiền
Leading actress:	Verify and Seek Help	Nữ chính:	Xác minh và tìm sự trợ giúp
Superimposed text:	Verify and Seek Help Verify the caller's identity and seek help from others	Chữ trên màn hình:	Xác minh và tìm sự trợ giúp Xác minh danh tính người gọi và nhờ người khác hỗ trợ

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	Kẻ lừa đảo:	Cô có chiêu của cô, nhưng tôi có lệnh bắt giữ. Tôi chỉ làm theo chỉ thị. Mau đưa tiền và mật khẩu tài khoản ngân hàng đây
Leading actress:	Ha! Law enforcement officers will not request for account information Your arrest warrant is fake I have discerned your hoax	Nữ chính:	Ha! Cơ quan thực thi pháp luật sẽ không yêu cầu thông tin tài khoản. Lệnh bắt giữ của anh là giả. Tôi đã nhìn thấu trò lừa của anh
Leading actress:	Watch this!	Nữ chính:	Xem đây!
Scammer:	Argh...	Kẻ lừa đảo:	Á…
Superimposed text:	The End	Chữ trên màn hình:	Hết
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	Nữ chính:	Dù chiêu trò cũ đến đâu, vẫn luôn có người mắc bẫy. Hãy nhớ “Ba Chiêu Chống Lừa Đảo”. Kẻ lừa đảo sẽ không còn hoành hành nữa
Superimposed text:	Remember the "Three Anti-Scam Tactics"! Scammers can no longer play tricks!	Chữ trên màn hình:	Hãy nhớ “Ba Chiêu Chống Lừa Đảo”! Kẻ lừa đảo không còn đất diễn!
Leading actress:	In addition, the HKMA has launched the "Money Safe" service	Nữ chính:	Ngoài ra, HKMA đã triển khai dịch vụ “Money Safe”. Giống như một chiếc két

	Just like a safe, it adds an extra layer of protection for deposits		sắt, nó bổ sung thêm một lớp bảo vệ cho tiền gửi
Superimposed text:	Money Safe	Chữ trên màn hình:	Money Safe
Leading actress:	Contact your bank for details now	Nữ chính:	Hãy liên hệ ngân hàng của bạn ngay để biết thêm chi tiết
Superimposed text:	(Hong Kong Monetary Authority Logo)	Chữ trên màn hình:	(Logo Cơ quan Tiền tệ Hồng Kông)

“Ba Chiêu Chống Lừa Đảo” – Video chống lừa đảo phong cách Quảng Đông cổ điển (2): Vạch trần công nghệ Deepfake

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

English		**Translation**	
Superimposed text:	Vintage Cantonese Anti-Scam Video (2)	Chữ trên màn hình	Video chống lừa đảo phong cách Quảng Đông cổ điển (2)
Superimposed text:	Three months ago	Chữ trên màn hình	Ba tháng trước
Son:	I am leaving for the capital for business Father, take good care of yourself!	Con trai	Con lên thủ đô làm ăn đây. Cha nhớ giữ gìn sức khỏe nhé!
Father:	Be careful and stay safe	Cha	Đi đường cẩn thận và giữ an toàn
Fake Son:	Father! Save me!	Con trai giả	Cha ơi! Cứu con với!
Father:	Why are you so scared?	Cha	Sao con lại sợ hãi thế?
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!	Con trai giả	Con bị cướp trên đường lên thủ đô. Con mất hết hàng hóa và tiền bạc, không giao hàng kịp cho khách được. Con phải bồi thường thiệt hại cho khách hàng! Cha chuyển tiền ngay vào tài khoản con vừa gửi cho cha!
Father:	For my son’s sake, I had no choice but to…	Cha	Vì con trai, ta không còn cách nào khác…

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"!	Chuyên gia	Khoan đã. Cái giả nhìn như thật, cái thật lại giống giả. Thưa ông, để tôi chia sẻ “Ba Chiêu Chống Lừa Đảo”!
Superimposed text:	Three Anti-Scam Tactics	Chữ trên màn hình	Ba Chiêu Chống Lừa Đảo
Master:	Tactic One Keep Calm	Chuyên gia	Chiêu thứ nhất
Superimposed text:	Keep Calm Keep calm, don't panic	Chữ trên màn hình	Bình tĩnh Giữ bình tĩnh, đừng hoảng loạn
Master:	Tactic Two Give Nothing	Chuyên gia	Chiêu thứ hai Không cung cấp gì
Superimposed text:	Give Nothing Give no personal data or money	Chữ trên màn hình	Không cung cấp gì Không cung cấp dữ liệu cá nhân hoặc tiền
Master:	Tactic Three Verify and Seek Help	Chuyên gia	Chiêu thứ ba Xác minh và tìm sự trợ giúp
Superimposed text:	Verify and Seek Help Verify the caller's identity and seek help from others	Chữ trên màn hình	Xác minh và tìm sự trợ giúp Xác minh danh tính người gọi và nhờ người khác hỗ trợ
Master:	Sir, remember these words	Chuyên gia	Thưa ông, hãy nhớ những điều này

Father:	Your uncle is an official working in the capital Why not reach out to him for help?	Cha	Chú của con là quan chức làm việc ở thủ đô. Sao con không tìm chú ấy giúp?
Fake Son:	Uncle is overwhelmed with responsibilities and not available!	Con trai giả	Chú bận trăm công nghìn việc, không rảnh!
Father:	Humph! Uncle has already retired and returned home! You evil monster! How dare you impersonate my beloved son using “deepfake”!	Cha	Hừ! Chú đã nghỉ hưu và về quê rồi! Đồ yêu quái! Dám dùng “deepfake” giả mạo con trai ta!
Superimposed text:	Goodbye	Chữ trên màn hình	Tạm biệt
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	Chuyên gia	Dù chiêu trò cũ đến đâu, vẫn luôn có người mắc bẫy. Hãy nhớ “Ba Chiêu Chống Lừa Đảo” Kẻ lừa đảo sẽ không còn hoành hành nữa
Superimposed text:	Remember the "Three Anti-Scam Tactics"! Scammers can no longer play tricks!	Chữ trên màn hình	Hãy nhớ “Ba Chiêu Chống Lừa Đảo”! Kẻ lừa đảo không còn đất diễn!
Master:	In addition, the HKMA has launched the "Money Safe" service	Chuyên gia	Ngoài ra, HKMA đã triển khai dịch vụ “Money Safe”
Superimposed text:	Money Safe	Chữ trên màn hình	Money Safe

Master:	Just like a treasure box, it adds an extra layer of protection for deposits Contact your bank for details now	Chuyên gia	Giống như một chiếc rương báu, nó bổ sung thêm một lớp bảo vệ cho tiền gửi. Hãy liên hệ ngân hàng của bạn ngay để biết thêm chi tiết
Superimposed text:	(Hong Kong Monetary Authority Logo)	Chữ trên màn hình	(Logo Cơ quan Tiền tệ Hồng Kông)