

Giữ An toàn trước những Vụ lừa đảo

Sự tin cậy và an toàn là ưu tiên hàng đầu đối với chúng tôi tại CommBank. Chúng tôi nhận thấy ngày càng có nhiều trường hợp khách hàng bị những kẻ lừa đảo gây áp lực hoặc lừa gạt để gửi tiền cho chúng. Những vụ lừa đảo này có thể tinh vi và có nhiều hình thức khác nhau. Điều quan trọng là quý vị phải cảnh giác và cho chúng tôi biết nếu có điều gì đó không ổn. Để tìm hiểu thêm về cách tự bảo vệ mình và trình báo hành vi lừa đảo, hãy xem commbank.com.au/safe.

Xác thực và Xác minh

- Hãy kiểm tra sự an toàn trong ứng dụng CommBank.
- Bật xác thực đa yếu tố, nhằm bổ sung thêm bước kiểm tra để chứng minh danh tính của quý vị.
- Sử dụng **CallerCheck (Kiểm tra Người gọi)** để xác minh danh tính của người gọi tự xưng là nhân viên của ngân hàng.
- Sử dụng **CustomerCheck (Kiểm tra Khách hàng)** tại chi nhánh để xác minh chính quý vị với nhân viên của chúng tôi.
- NameCheck (Kiểm tra Tên)** sẽ nhắc quý vị nếu chi tiết tài khoản trong khoản thanh toán lần đầu có vẻ không chính xác.

An toàn Thiết bị và Thanh toán

- Luôn cập nhật phần mềm chống vi-rút và bảo vệ máy tính của quý vị khỏi các mối đe dọa phổ biến.
- Sử dụng các phương thức thanh toán an toàn như chạm hoặc cho thẻ của quý vị vào máy.
- Không chia sẻ các thiết bị có quyền truy cập vào ví kỹ thuật số của quý vị.

Mật khẩu và Thông tin Cá nhân

- Không bao giờ chia sẻ mật khẩu hoặc mã PIN và thận trọng khi chia sẻ thông tin cá nhân.
- Không bao giờ cung cấp NetCode của quý vị cho bất kỳ ai, kể cả nhân viên CommBank.
- Quý vị có thể thay đổi mật khẩu của mình trong NetBank và ứng dụng CommBank bất kỳ lúc nào.
- Tạo mật khẩu mạnh và thay đổi chúng thường xuyên. Để biết hướng dẫn của chúng tôi về cách tạo mật khẩu, hãy truy cập commbank.com.au/password-security.

Email, SMS và Trực tuyến

- Đừng nhấp vào liên kết trong email hoặc SMS khả nghi.
- Nếu quý vị không chắc chắn về tin nhắn, hãy thảo luận về tin nhắn đó với người mà quý vị tin tưởng hoặc liên lạc trực tiếp với tổ chức thông qua chi tiết liên lạc chính thức.
- Cúp máy đối với các cuộc gọi điện thoại tự động, đáng ngờ hoặc đe dọa từ bên thứ ba.
- Hãy thận trọng với những người liên lạc không quen trên diễn đàn truyền thông xã hội và trực tuyến.

Dừng lại. Kiểm tra. Từ chối.

Dừng lại. Có điều gì đó có vẻ không ổn? Nếu nghi ngờ, tốt nhất nên dừng lại. Hãy hít thở.

Kiểm tra. Hãy hỏi người mà quý vị tin tưởng hoặc liên lạc trực tiếp với tổ chức bằng cách sử dụng thông tin chi tiết chính thức của họ.

Từ chối. Cúp máy với người gọi, xóa email, chặn số điện thoại. Thay đổi mật khẩu của quý vị.

Nếu quý vị cho rằng mình là nạn nhân của một vụ lừa đảo, hãy liên lạc ngay với CommBank theo số **13 22 21**, hoặc **+61 2 9999 3283** từ nước ngoài.

Nếu tiếng Anh không phải là ngôn ngữ đầu tiên của quý vị, Dịch vụ Phiên dịch và Thông dịch miễn phí của chính phủ có thể giúp quý vị liên lạc với chúng tôi. Dịch vụ này hiện có bằng hơn 150 ngôn ngữ. Chúng tôi có thể sắp xếp dịch vụ này khi quý vị gọi cho chúng tôi hoặc ghé thăm chúng tôi tại chi nhánh.

Những điều quý vị nên biết: Chúng tôi sẽ không bao giờ gửi cho quý vị email hoặc SMS yêu cầu cung cấp thông tin ngân hàng như Số Khách hàng NetBank, mật khẩu hoặc NetCode của quý vị; hoặc bao gồm đường liên kết để đăng nhập trực tiếp từ email hoặc SMS. Luôn đánh máy commbank.com.au vào trình duyệt hoặc sử dụng ứng dụng CommBank để tiếp cận tài khoản ngân hàng của quý vị một cách an toàn. Nếu có gì đó đáng ngờ từ CommBank, hãy chuyển thông tin này đến hoax@cba.com.au rồi xóa nó. Commonwealth Bank of Australia ABN 48 123 123 124 AFSL và giấy phép tín dụng Úc 234945.



Thông tin quan trọng về các vụ lừa đảo thường gặp



Đầu tư (Bao gồm cả Tiền điện tử - Crypto)

Những kẻ lừa đảo lôi kéo mọi người với lời hứa hẹn mang lại lợi nhuận cao, thường liên quan đến tiền điện tử hoặc các cơ hội đầu tư khác. Những kẻ lừa đảo có thể tìm cách liên lạc với quý vị qua điện thoại, email hoặc diễn đàn truyền thông xã hội.

Hướng dẫn cách bảo vệ bản thân:

- Nếu nghe có vẻ tốt đến mức không thể là sự thật, thì có lẽ đúng như vậy.
- Hãy thận trọng với những lời chào mời không được yêu cầu và áp lực phải đầu tư hoặc hành động nhanh chóng.
- Trước tiên, hãy xác minh tính hợp pháp của công ty hoặc nhà môi giới trên trang mạng của ASIC.



Tiếp cận Từ xa

Trong trường hợp kẻ lừa đảo gọi cho quý vị và tìm cách tiếp cận tài khoản hoặc thiết bị của quý vị, giả vờ đến từ một công ty hoặc tổ chức đáng tin cậy.

Hướng dẫn cách bảo vệ bản thân:

- Không bao giờ tải xuống phần mềm tiếp cận từ xa theo yêu cầu hoặc chịu áp lực từ người gọi bên thứ ba.
- Quý vị luôn có thể gọi lại cho một tổ chức bằng thông tin liên lạc hợp pháp của họ, được tìm thấy trên trang mạng chính thức của họ.
- Nếu nhận được cuộc gọi trong đó người gọi tự xưng là nhân viên CommBank, quý vị luôn có thể yêu cầu chúng tôi xác minh cuộc gọi thông qua tính năng CallerCheck trong ứng dụng.

Email của Doanh nghiệp bị Xâm nhập



Những kẻ lừa đảo có thể nhắm mục tiêu vào các doanh nghiệp bằng email từ một địa chỉ bị xâm nhập, hoặc các email được tạo trông giống như đến từ một người liên lạc đáng tin cậy như: trợ lý, khách hàng, luật sư, người quản lý hoặc nhà cung cấp của quý vị.

Hướng dẫn cách bảo vệ bản thân:

- Trước khi thanh toán lần đầu hoặc thay đổi chi tiết thanh toán, trước tiên hãy gọi cho tổ chức đó theo số liên lạc chính thức của họ để xác nhận chi tiết.
- Sử dụng tính năng NameCheck khi thanh toán, để xem tên tài khoản có khớp với BSB và số tài khoản đã cung cấp hay không.
- Đào tạo nhân viên cách nhận biết và trình báo các nỗ lực lừa đảo trên mạng.

Lừa đảo trên mạng và Ăn trộm Thông tin



Những kẻ lừa đảo sử dụng email hoặc tin nhắn văn bản lừa đảo có thể bao gồm liên kết dẫn quý vị đến một trang mạng gian trá hoặc yêu cầu thông tin cá nhân nhạy cảm.

Hướng dẫn cách bảo vệ bản thân:

- Đừng nhấp vào liên kết trong email hoặc SMS khả nghi.
- Quý vị có thể xác nhận tính xác thực của tin nhắn bằng cách liên lạc trực tiếp với tổ chức đó, sử dụng các phương thức liên lạc chính thức hiện có của họ.
- Trình báo mọi tin nhắn đáng ngờ từ CommBank tới hoax@cba.com.au

Thông tin quan trọng về các vụ lừa đảo thường gặp



Quan hệ

Những kẻ lừa đảo tạo hồ sơ giả để hình thành mối quan hệ và lôi kéo nạn nhân gửi tiền hoặc thông tin cá nhân.

Hướng dẫn cách bảo vệ bản thân:

- Không bao giờ gửi tiền hoặc chia sẻ mật khẩu, thông tin thẻ tín dụng hoặc tài khoản với bất kỳ ai mà quý vị không tin tưởng.
- Hãy tìm hiểu về bạn đời tiềm năng của quý vị trên mạng thông qua Google hoặc các ứng dụng truyền thông xã hội. Hãy thử tìm kiếm hình ảnh ngược để xác định xem có ai khác sở hữu những bức hình quý vị được gửi hay không.
- Nói chuyện với gia đình và bạn bè về mối quan hệ trực tuyến của quý vị. Họ có thể đưa ra quan điểm và xác định các dấu hiệu cảnh báo mà quý vị có thể không nhận thấy.

Cơ hội Việc làm

Trường hợp lời mời làm việc dường như đòi hỏi ít hoặc không cần nỗ lực để đạt được lợi nhuận tài chính cao, hoặc hứa hẹn kiếm tiền nhanh chóng.

Hướng dẫn cách bảo vệ bản thân:

- Xác minh công ty và lời mời chào thông qua các kênh chính thức, đồng thời tìm hiểu về công ty để đảm bảo chúng hợp pháp và hiện đang kinh doanh.
- Hãy cảnh giác với những lời mời làm việc qua mạng xã hội, trò chuyện được mã hóa, email, điện thoại hoặc thư từ những người quý vị chưa gặp hoặc công ty quý vị không biết.
- Một công ty hợp pháp sẽ không bao giờ yêu cầu quý vị thanh toán trước hoặc sử dụng thông tin ngân hàng cá nhân của quý vị để tạo điều kiện thuận lợi cho việc kinh doanh hoặc quỹ của công ty.



Mua sắm Trực tuyến

Những kẻ lừa đảo tạo các cửa hàng hoặc quảng cáo trực tuyến để thu hút người mua hàng mua sản phẩm không tồn tại hoặc giả mạo.

Hướng dẫn cách bảo vệ bản thân:

- Chỉ mua sắm trên các trang mạng có uy tín và an toàn và hãy cảnh giác với bất kỳ lời mời chào nào có vẻ tốt đến mức khó tin.
- Sử dụng các phương thức thanh toán an toàn và tránh chuyển khoản trực tiếp cho người bán.
- Đừng vội vàng hoặc bị gây áp lực bởi 'khuyến mại có giới hạn' hoặc sắp sửa kết thúc đợt giảm giá.

Đe dọa và Hình phạt

Những kẻ lừa đảo mạo danh cơ quan thẩm quyền hoặc tổ chức đáng tin cậy để tống tiền thông qua việc đe dọa phạt tiền hoặc khởi kiện.

Hướng dẫn cách bảo vệ bản thân:

- Hãy cúp máy đối với những người gọi đe dọa, và liên lạc trực tiếp với tổ chức đó.
- Một tổ chức hợp pháp sẽ không bao giờ yêu cầu quý vị thanh toán bằng các phương thức bất thường như bằng quà tặng hoặc thẻ mua hàng, phiếu iTunes, chuyển khoản ngân hàng hoặc Bitcoin.
- Nếu quý vị lo lắng cho sự an toàn của mình, hãy liên lạc với đường dây hỗ trợ của cảnh sát.

