Australian Banking Association

Hãy cảnh giác:

Đề phòng các mánh khoé chiếm đoạt tiền và lừa đảo.

Các mánh khoé chiếm đoạt tiền và lừa đảo liên quan đến COVID-19 có thể gia tăng trong vài tháng tới.

Bọn lừa đảo dùng email giả, gọi điện hoặc nhắn tin nhằm lấy thông tin cá nhân. Bọn chúng giả danh gọi từ ngân hàng của quý vị, Tổ Chức Y Tế Thế Giới, chính phủ, tổ chức từ thiện, hoặc cơ sở kinh doanh hợp pháp như các công ty lữ hành, công ty dịch vụ điện, điện thoại hoặc Internet, hoặc siêu thị gần nhà quý vị.

Hãy bảo vệ bản thân.

Ngân hàng của quý vị sẽ KHÔNG BAO GIỜ gửi email hoặc nhắn tin yêu cầu thông tin tài khoản hoặc tài chính, kể cả việc cập nhật địa chỉ hoặc thông tin truy cập điện thoại, điện thoại di động hoặc ngân hàng trực tuyến.

Chính phủ và các tổ chức hợp pháp khác sẽ KHÔNG BAO GIỜ yêu cầu quý vị cập nhật thông tin bằng cách nhấp vào đường dẫn đến các trang mạng nào đó. Nếu nghi ngờ, hãy nói chuyện với bạn bè hoặc gia đình hoặc trực tiếp liên lạc tổ chức đó để hỏi.

Nếu một ai đó quý vị không quen biết gọi hỏi quý vị thông tin cá nhân, HÃY CÚP MÁY. Hãy gọi trực tiếp công ty đó và kiểm tra xem họ có gọi quý vị không.

ĐỪNG BAO GIỜ mở tài liệu đính kèm email từ bất kỳ cá nhân hoặc tổ chức nào đó quý vị không biết. Hãy cẩn trọng đối với những chào mời quá hấp dẫn không thực tế hoặc yêu cầu cung cấp quá nhiều thông tin.

Ngân hàng có thể hỗ trợ quý vị, hãy liên hệ họ ngay nếu:

- quý vị đã trả lời email, điện thoại hoặc tin nhắn lừa đảo và đã cung cấp thông tin tài khoản ngân hàng của mình
- quý vị đã vô tình nhấp vào đường dẫn đến những trang mạng hoặc tải các tài liệu đính kèm email.
- quý vị phát hiện bất kỳ các giao dịch bất thường từ tài khoản của mình

Làm thế nào để phát hiện mánh khoé chiếm đoạt tiền.

- Quý vị được yêu cầu cập nhật hoặc xác nhận thông tin cá nhân như địa chỉ, ngày sinh, thông tin tài khoản ngân hàng, mã số thuế hoặc bất kỳ mã số cá nhân hoặc mật khẩu.
- Email hoặc tin nhắn có những đường dẫn đến những trang mạng đáng nghi ngờ. Nếu quý vị không chắc, hãy nhờ bạn bè hoặc gia đình giúp đỡ.
- Nếu quý vị được yêu cầu thanh toán ngay hoặc đặt cọc trước.
- Nếu lời chào mời quá hấp dẫn không thực tế, lời chào mời đó có thể không có thực.
- Địa chỉ email không khớp với công ty.
- Người gọi yêu cầu truy cập máy tính của quý vị từ xa.

Australian Banking Association

www.ausbanking.org.au

Các mẹo phổ biến giúp quý vị bảo vệ thông tin ngân hàng khỏi bị chiếm đoạt tiền và lừa đảo.

- Cúp máy các cuộc gọi đáng nghi ngờ, thay vào đó vào trang web công ty đó hoặc tìm số điện thoại và liên lạc trực tiếp với họ.
- Đừng bao giờ cung cấp mật khẩu hoặc mã số cá nhân. Cài mật khẩu cho tất cả thiết bị của quý vị. Nếu quý vị dùng chung máy tính, đừng bao giờ chia sẻ mật khẩu và luôn đăng xuất khỏi tài khoản của minh.
- Kiểm tra tài khoản định kỳ để quý vị phát hiện ra các giao dịch đáng ngờ một cách nhanh chóng.
- Hãy tránh cà thẻ qua khe đọc thẻ khi thanh toán. Thường quẹt thẻ và đút thẻ vào máy thanh toán an toàn hơn.
- Chặn chức năng rút tiền mặt của thẻ tín dụng.
- Hãy nói chuyện với ngân hàng về cách thức tốt nhất để bảo vệ tài khoản quý vị.
- Nếu quý vị tin rằng quý vị đã bị chiếm đoạt tiền, hãy báo với ngân hàng ngay lập tức.

Bọn lừa đảo sẽ chiếm đoạt tiền của quý vị bằng nhiều cách, dưới đây là những cách chính:

Đánh cắp thông tin cá nhân qua Internet hoặc email – Dùng email hoặc tin nhắn dưới danh nghĩa các tổ chức đáng tin cậy như ngân hàng, tổ chức từ thiện hoặc chính phủ để đánh cắp thông tin cá nhân của quý vị. Tin nhắn có vẻ như thật và thường sẽ yêu cầu quý vị nhập thông tin cá nhân vào trang web giả hoặc yêu cầu quý vị nhấp vào đường dẫn - việc này tạo điều kiện cho bọn lừa đảo truy cập vào máy tính và thông tin cá nhân của quý vị.

Trò chiếm đoạt tiền qua hình thức mua sắm trực tuyến– bọn lừa đảo giả danh là các cửa hàng trực tuyến thật thông qua trang web giả hoặc quảng cáo lừa đảo trên trang bán hàng có thật. Các trang bán hàng trực tuyến giả thường sẽ yêu cầu phương thức thanh toán bất thường như trả trước bằng lệnh chuyển tiền, chuyển khoản, thanh toán quốc tế hoặc thẻ quà tặng.

Trò chiếm đoạt tiền qua hình thức đầu tư– bọn lừa đảo tự phong là người môi giới hoặc quản lý danh mục đầu tư cho lời khuyên về tài chính hoặc đầu tư. Bọn chúng sẽ yêu cầu quý vị giao tiền cho một cơ hội đầu tư nào đó có thể thật có thể không rồi bọn chúng giữ tiền.

Trò chiếm đoạt tiền bằng cách truy cập từ xa – bọn lừa đảo sẽ quả quyết rằng máy tính hoặc kết nối Internet của quý vị có vấn đề hoặc máy tính quý vị bị nhiễm phần mềm có hại. Bọn chúng sẽ thuyết phục quý vị cài đặt một ứng dụng nào đó hoặc cho bọn chúng truy cập máy tính của quý vị. Bọn chúng sẽ dùng cách này để truy cập thông tin cá nhân của quý vị hoặc đòi trả 'phí ' để xử lý vấn đề.

Trò chiếm đoạt tiền dựa trên mối quan hệ tình cảm -bọn lừa đảo tạo mối quan hệ với quý vị nhằm bòn rút tiền hoặc quà tặng. Mối quan hệ tiến triển theo thời gian và bọn chúng có thể yêu cầu quý vị chuyển sở hữu tài sản sang tên bọn chúng hoặc yêu cầu là người thừa kế tài sản trong di chúc của quý vị. Thông thường bọn chúng sẽ xin tiền để chữa bệnh, giải quyết nhu cầu đi lại hoặc chuyện gia đình.

Các đường dẫn hữu ích:

www.ausbanking.org.au/safe-savvy-a-guide-to-help-older-people-avoid-abuse-scams-and-fraud

www.esafety.gov.au/seniors/staying-safer-online

www.scamwatch.gov.au/