HÃY TRÌNH BÁO CUỘC TẤN CÔNG MẠNG VÀ CÁC SỰ CỐ BỊ TẤN CÔNG ĐỂ GIỮ CHO NƯỚC ÚC ĐƯỢC AN NINH.

ĐĂNG KÝ

DÙNG DỊCH VỤ CẢNH BÁO MIỄN PHÍ TẠI **CYBER.GOV.AU**

TRÌNH BÁO

TỘI PHẠM MẠNG CHO REPORTCYBER: **CYBER.GOV.AU/REPORT**

LIÊN LẠC

GỌI SỐ 1300 CYBER1 HOẶC VÀO TRANG MẠNG CYBER.GOV.AU

Số điện thoại này chỉ để sử dụng trong nước Úc mà thôi.

THEO DÕI CHÚNG TÔI

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

5. CẢNH GIÁC VẤN ĐỀ LỪA ĐẢO

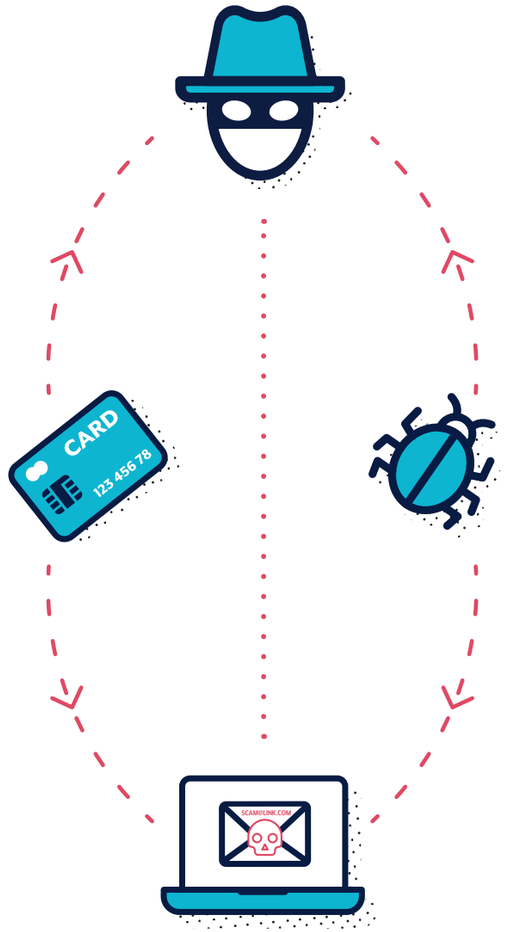
Tội phạm mạng dùng email, tin nhắn SMS, các cuộc gọi điện thoại và mạng xã hội để lừa quý vị mở tài liệu đính kèm, vào một trang mạng, làm lộ chi tiết đăng nhập tài khoản, làm lộ các thông tin nhậy cảm hoặc chuyển tiền hoặc phiếu quà tặng. Các tin nhắn được soạn ra để trông có vẻ như được gửi từ các cá nhân hoặc tổ chức mà quý vị cho là mình có biết họ, hoặc quý vị cho là mình nên tin tưởng họ.

Để phát hiện tin nhắn lừa đảo, hãy ngừng lại và suy nghĩ:

- **Người có thẩm quyền:** Tin nhắn này có tự nhận là của người nào đó là viên chức không?
- **Khẩn cấp:** Người ta có bảo là quý vị chỉ có ít thời gian để hồi âm không?
- **Tình cảm:** Tin nhắn có làm cho quý vị hoảng hốt, sợ hãi, hi vọng hoặc tò mò không?
- **Khan hiếm:** Tin nhắn có chào mời quý vị món gì đang rất khan hiếm không?
- **Sự kiện hiện tại:** Thông điệp có liên quan đến tin tức thời sự, sự kiện lớn hoặc thời điểm cụ thể trong năm (như mùa khai thuế) không?

Kiểm tra xem tin nhắn có hợp pháp không:

- Quay trở lại với cái gì đó mà quý vị có thể tin tưởng. Vào trang mạng chính thức, đăng nhập vào tài khoản của quý vị hoặc gọi tới số điện thoại họ quảng cáo. Không sử dụng đường dẫn hoặc chi tiết liên lạc được ghi trong tin nhắn họ gửi cho quý vị hoặc báo cho quý vị qua điện thoại.
- Kiểm tra xem liệu có nguồn chính thức nào đã báo cho quý vị những điều họ không bao giờ hỏi quý vị. Ví dụ như, ngân hàng của quý vị có thể đã từng báo cho quý vị rằng họ sẽ không bao giờ hỏi mật khẩu của quý vị.



Để biết thêm thông tin về cách phát hiện các tin nhắn lừa đảo, hãy xem tài liệu Phát hiện Tin nhắn Kỹ thuật Xã hội của Trung tâm An ninh Mạng Úc (Australian Cyber Security Centre - ACSC), và nắm được tình hình bằng cách đăng ký vào Dịch vụ Cảnh báo của ACSC tại trang mạng **cyber.gov.au.**

CÁC BƯỚC DỄ DÀNG

ĐỂ GIỮ AN TOÀN CHO THIẾT BỊ VÀ TÀI KHOẢN CỦA QUÝ VỊ

GIẢM NGUY CƠ LÀM MỤC TIÊU CHO TỘI PHẠM MẠNG BẰNG CÁC BƯỚC DƯỚI ĐÂY

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

1. CẬP NHẬT THIẾT BỊ CỦA QUÝ VỊ

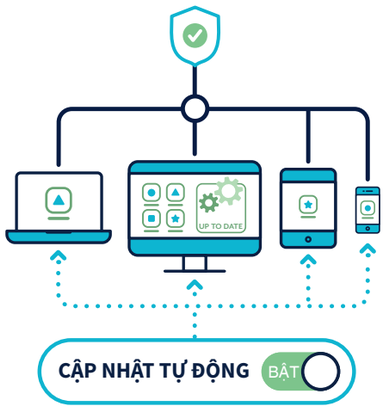
Tội phạm mạng xâm nhập vào thiết bị bằng cách khai thác các điểm yếu đã biết của hệ thống hoặc ứng dụng. Việc cập nhật bao gồm cả các cập nhật an toàn nhằm khắc phục các điểm yếu đó. Hãy bật chức năng cập nhật tự động để được cập nhật mà quý vị không cần làm gì cả.

Bật chế độ cập nhật tự động trên tất cả các thiết bị của quý vị:

- Điện thoại di động
- Máy tính xách tay
- Máy tính để bàn

Thường xuyên kiểm tra cập nhật đối với:

- Các ứng dụng
- Các chương trình
- Các thiết bị thông minh



2. BẬT TÍNH NĂNG XÁC THỰC ĐA YẾU TỐ (MFA)

Multi-Factor Authentication (MFA) tăng cường an ninh bằng cách làm cho tội phạm mạng khó tiếp cận hồ sơ hoặc tài khoản của quý vị hơn.

Hãy kích hoạt MFA, bắt đầu từ những tài khoản quan trọng nhất của quý vị:

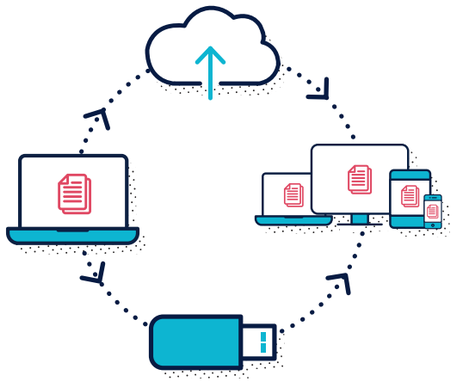
- Các tài khoản email
- Giao dịch ngân hàng trực tuyến và các tài khoản có lưu chi tiết thanh toán
- Mạng xã hội

3. SAO LƯU CÁC THIẾT BỊ CỦA QUÝ VỊ

Sao lưu là bản sao điện tử các thông tin được lưu trữ trên thiết bị của quý vị chẳng hạn như ảnh, tài liệu, video và dữ liệu từ các ứng dụng. Bản sao được lưu tại thiết bị lưu trữ bên ngoài hoặc trên đám mây. Sao lưu tức là quý vị có thể khôi phục được hồ sơ trong trường hợp thiết bị bị thất lạc, bị lấy cắp hoặc bị hư hại.

Thường xuyên sao lưu thiết bị của quý vị:

- Điện thoại di động
- Máy tính xách tay
- Máy tính để bàn
- Máy tính bảng



4. ĐẶT MỘT CỤM MẬT KHẨU AN TOÀN

Trong trường hợp không có MFA, thì cụm mật khẩu an toàn thường có thể là cách duy nhất bảo vệ thông tin và các tài khoản của quý vị chống lại tội phạm.

Cụm mật khẩu an toàn sử dụng bốn từ bất kỳ trở lên làm mật khẩu. Đổi mật khẩu của quý vị thành cụm mật khẩu, đảm bảo cụm mật khẩu cần phải:

- Dài: cụm mật khẩu càng dài bao nhiêu càng tốt bấy nhiêu. Hãy làm cụm mật khẩu dài ít nhất 14 chữ
- Khó đoán: Hãy sử dụng hỗn hợp các từ bất kỳ không liên quan với nhau
- Độc nhất: Không nên tái sử dụng cụm mật khẩu cho nhiều tài khoản