MẸO HÀNG ĐẦU CHO AN NINH MẠNG

CÁC CÁCH THỨC THỰC TIỄN ĐỂ BẢO VỆ BẢN THÂN TRỰC TUYẾN

cyber.gov.au/learn

Cập nhật các ứng dụng và thiết bị của bạn

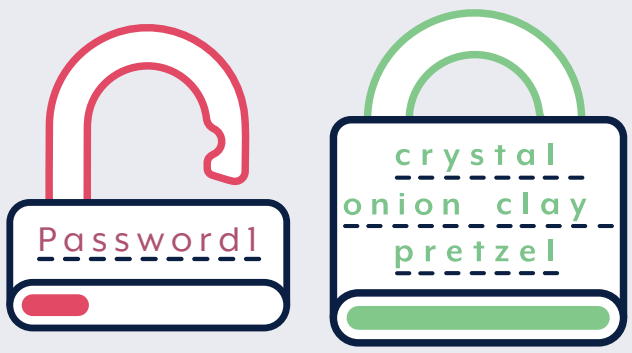
Cập nhật các ứng dụng và thiết bị của bạn có thể khắc phục vấn đề và giải quyết các mối lo ngại mới về bảo mật hoặc các điểm yếu.

Bật tính năng xác thực đa yếu tố (MFA)

MFA nghĩa là có hơn một cách kiểm tra để xác minh danh tính của bạn trên một tài khoản.

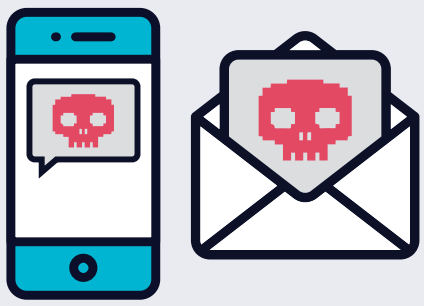
Thiết lập và thực hiện sao lưu thường xuyên

Bản sao lưu là bản sao kỹ thuật số các thông tin của bạn vào thiết bị lưu trữ bên ngoài hoặc máy chủ, chẳng hạn như đám mây.



Thiết lập cụm mật mã an toàn

Khi không có MFA, hãy sử dụng cụm mật mã để bảo mật tài khoản của bạn. Một cụm mật mã là một loại mật mã mạnh kết hợp bốn từ ngẫu nhiên trở lên.



Nhận biết và trình báo lừa đảo

Đừng tin cậy tất cả mọi thứ bạn đọc. Luôn cảnh giác khi nhấp vào tập hồ sơ đính kèm hoặc các đường dẫn trong email hoặc tin nhắn.

Nâng cấp an ninh mạng của bạn bằng cách truy cập cyber.gov.au

Tìm hiểu thêm tại trang mạng **cyber.gov.au/learn**

Trình báo các vấn đề an ninh mạng:
cyber.gov.au | 1300 CYBER1 (1300 292 371)
Số điện thoại này chỉ để sử dụng trong nước Úc mà thôi.

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Bạn có các ý kiến đóng góp về sản phẩm này không? Hãy truy cập trang mạng **cyber.gov.au** và cho chúng tôi biết.