

Chia sẻ thông tin cá nhân quá nhiều trên mạng xã hội

Sử dụng mật khẩu mạnh và đa dạng cho mỗi tài khoản trực tuyến

Luôn kiểm tra tính đáng tin cậy của các trang web và nguồn tài về trước khi cung cấp thông tin cá nhân hoặc tải xuống

Sử dụng kết nối VPN khi kết nối với mạng Wi-Fi công cộng để mã hóa dữ liệu và bảo vệ quyền riêng tư

Sử dụng kết nối Wi-Fi công cộng mà không sử dụng VPN để bảo vệ thông tin cá nhân

Mở các email hoặc tin nhắn từ nguồn không tin cậy và nhấp vào các liên kết bất kỳ

Kích hoạt xác thực hai yếu tố (2FA) cho tài khoản trực tuyến để bảo vệ thêm lớp bảo mật

Sử dụng phần mềm mã hóa để bảo vệ dữ liệu quan trọng trên máy tính và thiết bị di động

Cập nhật định kỳ phần mềm, hệ điều hành và ứng dụng để bảo vệ khỏi các lỗ hổng bảo mật mới

Kiểm tra quyền truy cập của ứng dụng trước khi cung cấp quyền truy cập vào thông tin cá nhân hoặc thiết bị

Chấp nhận kết bạn hoặc kết nối với người lạ trên các nền tảng mạng xã hội

Tải xuống phần mềm từ các nguồn không đáng tin cậy hoặc không được kiểm tra

Sử dụng phần mềm diệt virus và firewall để bảo vệ thiết bị khỏi các mối đe dọa trực tuyến

Sử dụng mật khẩu dễ đoán hoặc mật khẩu giống nhau cho nhiều tài khoản

Tin tưởng vào các tin đồn hoặc thông tin không được xác nhận từ nguồn không chính thống

Sử dụng tài liệu hướng dẫn và các nguồn thông tin đáng tin cậy để giáo dục bản thân về an ninh mạng và bảo mật trực tuyến

Cho phép các ứng dụng truy cập vào thông tin cá nhân mà không kiểm tra quyền truy cập của chúng

Sử dụng một tài khoản ngân hàng hoặc thanh toán riêng cho mua sắm trực tuyến

Bỏ qua cập nhật phần mềm và hệ điều hành, làm tăng nguy cơ bị tấn công từ các lỗ hổng bảo mật đã được vá

Phóng to hình ảnh, văn bản hoặc liên kết không xác định nguồn gốc có thể chứa mã độc