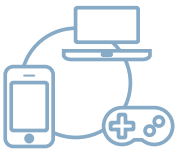
CHUẨN BỊ CHO CUỘC TẤN CÔNG MẠNG

Các cuộc tấn công mạng có thể dẫn đến mất tiền, đánh cắp thông tin cá nhân và gây thiệt hại cho danh tiếng và sự an toàn của bạn.

FEMA

FEMA P-2264/Tháng 6 năm 2018

Tấn công mạng là những nỗ lực độc hại nhằm truy cập hoặc làm hỏng hệ thống máy tính.



Có thể sử dụng máy tính, điện thoại di động, hệ thống chơi game và các thiết bị khác

Có thể bao gồm gian lận hoặc đánh cắp danh tính

Có thể chặn quyền truy cập của bạn hoặc xóa tài liệu và hình ảnh cá nhân của bạn

Có thể nhắm mục tiêu đến trẻ em

Có thể gây ra các vấn đề với dịch vụ kinh doanh, vận chuyển và nguồn điện

BẢO VỆ CHÍNH BẠN CHỐNG LẠI MỘT CUỘC TẤN CÔNG MẠNG

Luôn cập nhật phần mềm và hệ điều hành.

Sử dụng liên lạc internet được mã hóa (an toàn).

Sử dụng mật khẩu mạnh và xác thực hai yếu tố để xác minh (hai phương pháp xác minh).

Tạo tệp sao lưu.

Theo dõi hoạt động đáng ngờ. Khi nghi ngờ, đừng nhấp chuột vào. Không cung cấp thông tin cá nhân.

Bảo vệ mạng lưới Wi-Fi của nhà bạn.

CÁCH GIỮ AN TOÀN
KHI MỘT CUỘC TẤN CÔNG MẠNG ĐE DỌA

Ngăn chặn NGAY BÂY GIỜ

Luôn cập nhật phần mềm chống vi-rút của bạn.

Sử dụng mật khẩu mạnh có 12 ký tự trở lên. Sử dụng chữ hoa và chữ thường, số và các ký tự đặc biệt. Thay đổi mật khẩu hàng tháng. Sử dụng trình quản lý mật khẩu.

Sử dụng xác thực mạnh hơn như mã PIN hoặc mật khẩu mà chỉ **bạn mới biết.** Cân nhắc sử dụng một thiết bị riêng biệt có thể nhận mã hoặc sử dụng **quét sinh trắc học** (ví dụ: máy quét dấu vân tay).

Theo dõi hoạt động đáng ngờ yêu cầu bạn làm điều gì đó ngay lập tức, cung cấp điều gì đó nghe có vẻ quá tốt để trở thành sự thật hoặc cần thông tin cá nhân của bạn. **Hãy suy nghĩ trước khi bạn nhấp chuột vào.**

Kiểm tra bảng sao kê tài khoản của bạn và báo cáo tín dụng thường xuyên.

Sử dụng kết nối Internet an toàn. Sử dụng các trang web sử dụng "HTTPS" nếu bạn sẽ truy cập hoặc cung cấp bất kỳ thông tin cá nhân nào. Không sử dụng các trang web có chứng nhận không hợp lệ. Sử Dụng Mạng Riêng Trực Ảo (VPN) tạo kết nối an toàn.

Sử dụng các giải pháp chống vi-rút, phần mềm độc hại và tường lửa để chặn các mối đe dọa.

Thường xuyên sao lưu tệp của bạn trong tệp được mã hóa hoặc thiết bị lưu trữ tệp được mã hóa.

Hạn chế thông tin cá nhân bạn chia sẻ trực tuyến. Thay đổi cài đặt quyền riêng tư và không sử dụng các tính năng vị trí.

Bảo vệ mạng gia đình của bạn bằng cách thay đổi mật khẩu quản trị và Wi-Fi thường xuyên. Khi định cấu hình bộ định tuyến của bạn, hãy chọn cài đặt Tiêu Chuẩn Mã Hóa Nâng Cao (Advanced Encryption Standard, AES) Quyền Truy Cập Wi-Fi được Bảo Vệ 2 (Wi-Fi Protected Access, WPA2), là tùy chọn mã hóa mạnh nhất.

Hạn Chế Thiệt Hại TRONG THỜI GIAN

Hạn chế thiệt hại. Tìm các khoản phí không giải thích được, các tài khoản lạ trên báo cáo tín dụng của bạn, thẻ tín dụng bị từ chối đột xuất, các bài đăng bạn không thực hiện hiển thị trên mạng xã hội và những người nhận được email bạn chưa từng gửi.

Thay đổi mật khẩu ngay lập tức cho tất cả các tài khoản trực tuyến của bạn.

Quét và làm sạch thiết bị của bạn.

Cân nhắc tắt thiết bị. Hãy mang nó đến nhà cung cấp chuyên nghiệp để quét và sửa chữa.

Cho cơ quan, trường học hoặc các chủ sở hữu hệ thống khác biết. Các Bộ phận IT có thể cần phải cảnh báo những người khác và nâng cấp hệ thống.

Liên hệ với các ngân hàng, công ty phát hành thẻ tín dụng và các tài khoản tài chính khác. Bạn có thể cần giữ các tài khoản đã bị tấn công. Đóng mọi tài khoản tín dụng hoặc tài khoản phí trái phép. Báo cáo rằng ai đó có thể đang sử dụng danh tính của bạn.

Báo cáo SAU KHI

Nộp báo cáo cho **Văn Phòng Tổng Thanh Tra (Office of the Inspector General, OIG)** nếu bạn cho rằng ai đó đang sử dụng bất hợp pháp số An Sinh Xã Hội của bạn. **OIG xem xét các trường hợp lãng phí, gian lận và lạm dụng.** Để gửi báo cáo, hãy truy cập www.idtheft.gov.

Bạn cũng có thể gọi cho đường dây nóng của Cơ Quan An Sinh Xã Hội theo số 1-800-269-0271. Để biết thêm tài nguyên và biết thêm thông tin, hãy truy cập http://oig.ssa.gov/report.

Gửi đơn khiếu nại đến FBI Trung tâm Khiếu nại Tội phạm Internet (IC3) tại www.IC3.gov. Họ sẽ xem xét đơn khiếu nại và chuyển đến cơ quan thích hợp.

Tìm hiểu các mẹo, công cụ và hơn thế nữa tại www.stopthinkconnect.org.

FEMA

FEMA P-2264

Giữ một Vai trò Tích cực trong sự An toàn của Bạn

Truy cập **Ready.gov/vi/cybersecurity.** Tải xuống **ứng dụng FEMA** để biết thêm thông tin về cách chuẩn bị cho một **tấn công mạng.**