# Hãy thông minh khi lên mạng:  Trang bị "Shields Up" (Lá chắn)

## Các Bước Đơn Giản Để An Toàn Trực Tuyến

Lừa đảo qua mạng không có gì mới. Mỗi ngày, các tin tặc và tội phạm mạng khác đang tìm kiếm mục tiêu dễ dàng nhất trên mạng. Quý vị có nghĩ mình không đáng để trở thành mục tiêu của những kẻ săn mồi trực tuyến không? Nghĩ lại đi!

Cho dù đó là danh tính của quý vị, thông tin tài khoản ngân hàng của quý vị, hay chỉ đơn giản là những gì trong email của quý vị, thông tin của quý vị đều có giá trị và bọn tội phạm mạng sẽ làm bất cứ điều gì có thể được để truy cập thông tin đó. Họ đang trông cậy vào quý vị nghĩ rằng mình không phải là mục tiêu. Đã đến lúc quý vị nên trang bị ***Shields Up*** và thực hiện các bước để ngăn chặn việc mình trở thành nạn nhân của tội phạm mạng.

Hãy bắt đầu với những điều cơ bản về vệ sinh mạng - những cách dễ dàng và thông thường để bảo vệ bản thân khi trực tuyến. Đây là bốn điều đơn giản quý vị có thể làm hôm nay để giữ cho mình an toàn trên mạng:

- **Sử dụng nhiều hơn một loại xác thực trên tất cả các tài khoản của quý vị.** Mật mã không đủ để giúp quý vị trực tuyến an toàn. Bằng cách sử dụng một lớp nhận dạng thứ hai, chẳng hạn như tin nhắn xác nhận, mã số từ một ứng dụng  xác thực, xác minh bằng diện mạo hoặc vân tay, hay chìa khóa bảo mật, mà quý vị đang cung cấp cho ngân hàng, nhà cung cấp thư điện tử, hay bất kỳ trang mạng nào khác mà quý vị đang đăng nhập vào trở thành một lớp bảo mật bổ sung. Xác thực đa yếu tố có thể giúp quý vị giảm đến 99% khả năng bị tấn công hoặc thông tin của quý vị bị đánh cắp!
- **Cập nhật phần mềm của quý vị.** Tin tặc sẽ cố gắng khai thác các lỗi và lỗ hổng của phần mềm. Cập nhật hệ thống phần mềm trên tất cả các thiết bị của quý vị, chẳng hạn như điện thoại di động, máy tính bảng và máy tính xách tay.  Bảo đảm việc kiểm tra các ứng dụng của quý vị thường xuyên trên tất cả các thiết bị của quý vị - đặc biệt là các trình duyệt mạng . Giúp dễ dàng cho bản thân hơn bằng cách chỉ cần khởi động cập nhật tự động cho tất cả các thiết bị, ứng dụng và hệ thống điều hành.
- **Hãy suy nghĩ trước khi quý vị nhấp vào.** Hơn 90% các cuộc tấn công mạng thành công bắt đầu khi quý vị nhấp vào một liên kết lạ trong thư điện tử nhằm lấy trộm thông tin cá nhân. Mưu đồ lừa đảo là khi một liên kết hoặc trang mạng có vẻ hợp pháp, nhưng đó là một mánh khóe được sắp đặt để quý vị tiết lộ mật mã, số thẻ tín dụng hoặc thông tin nhạy cảm khác. Ngoài ra, thư điện tử lừa đảo có thể là những nỗ lực cố gắng để quý vị chạy phần mềm hiểm độc, còn được gọi là phần mềm độc hại. Nếu đó là một liên kết mà quý vị không nhận ra, hãy tin vào linh tính của mình và suy nghĩ trước khi nhấp vào.
- Sử dụng mật mã mạnh mẽ. Mật mã mạnh mẽ phải có tám ký tự trở lên sử dụng với sự kết hợp của các chữ cái, số và ký tự đặc biệt. Tránh sử dụng cùng một mật mã trên các tài khoản khác nhau. Tốt nhất, các cá nhân cũng nên sử dụng một ứng dụng quản lý mật mã để tạo và lưu trữ các mật mã duy nhất.

Thế giới của chúng ta ngày càng tăng trưởng về kỹ thuật số và ngày càng tăng trưởng kết nối với nhau, và tất cả chúng ta đều có trách nhiệm thực sự bảo vệ các hệ thống mạng mà tất cả chúng ta dựa vào. Trở thành nhà vô địch về an ninh mạng và chia sẻ những bí quyết này với bạn bè, gia đình và hàng xóm của quý vị.

Để có thêm thông tin vui lòng vào trang nhà CISA's Shields Up