Phòng Chống Tội Phạm Mạng

Internet là cách tuyệt vời để kết nối trực tuyến, nhưng nó cũng có thể là mối nguy hiểm. Cũng giống như khi quý vị chuẩn bị rời khỏi nhà, quý vị nên đề phòng trước khi sử dụng internet nhằm đảm bảo rằng quý vị và thông tin của quý vị được an toàn và bảo mật, bởi vậy quý vị sẽ không trở thành nạn nhân của tội phạm mạng.

Cách Giữ An Toàn Trên Internet

Tội Phạm Mạng Là Gì?

Tội phạm mạng là tội phạm xảy ra với những người sử dụng internet. Chúng xảy ra khi thông tin cá nhân hoặc tiền của người dùng bị đánh cắp. Nhiều người không biết khi nào tội phạm mạng sẽ xảy ra với họ, vì vậy điều quan trọng là phải biết cách nhận biết tội phạm mạng để phòng chống hoặc tìm sự giúp đỡ và ngăn chặn tội phạm mạng tái diễn.

Internet Là Một Không Gian Công Cộng

- Mọi người có thể nhìn thấy trang web mà quý vị đang truy cập và đôi khi cả thông tin mà quý vị nhập vào.
- Bất kỳ thông tin nào quý vị chia sẻ trên internet đều có thể bị người khác thấy được.
- Quý vị hãy hết sức thận trọng khi chia sẻ thông tin cá nhân của mình (như số an sinh xã hội, thông tin tài khoản ngân hàng và thông tin y tế) trên internet khi việc chia sẻ đó không phải vì lý do công việc hợp lệ, chẳng hạn như giao dịch ngân hàng.
- Quý vị hãy huôn thận trọng khi sử dụng mạng Wi-Fi công cộng tại các cửa hàng và nhà hàng cho phép sử dụng miễn phí.
- Mặc dù sử dụng Wi-Fi công cộng rất tiện lợi nhưng nó thường có bảo mật kém. Điều này có nghĩa là thông tin cá nhân của quý vị (chẳng hạn như tên người dùng và mật khẩu đăng nhập tài khoản ngân hàng của quý vị) có thể bị người khác nhìn thấy hoặc đánh cắp.

Kiểm Tra Cài Đặt Quyền Riêng Tư Thường Xuyên

- Cài đặt quyền riêng tư cho phép quý vị chọn thông tin quý vị muốn chia sẻ và người có thể xem thông tin của quý vị.
  - Trên phương tiện truyền thông xã hội (như Facebook hoặc Instagram), quý vị có thể sử dụng cài đặt quyền riêng tư để kiểm soát thông tin được chia sẻ với người khác.
- Thiết lập cài đặt quyền riêng tư cho các ứng dụng khác nhau trên điện thoại di động để giới hạn những gì được chia sẻ với các ứng dụng (như chia sẻ vị trí của quý vị hoặc quyền dữ liệu).
- Đảm bảo rằng cài đặt quyền riêng tư trên các tài khoản trực tuyến của quý vị yêu cầu mật khẩu trước khi truy cập vào tài khoản.
  - Xác Thực Hai Yếu Tố là quý vị nhận được tin nhắn văn bản, cuộc gọi hoặc email có mã đặc biệt mỗi khi quý vị đăng nhập vào tài khoản trực tuyến của mình (như ngân hàng hoặc công ty phát hành thẻ tín dụng). Điều này giúp bảo đảm rằng chính quý vị đang đăng nhập vào tài khoản của mình.
  - Quý vị nên thiết lập Xác Thực Hai Yếu Tố cho các tài khoản trực tuyến.

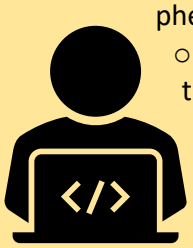
Bản Tin Sức Khỏe Và An Toàn do Sở Dịch Vụ Phát Triển ấn hành để cảnh báo cho các cá nhân, gia đình và những người khác về những rủi ro cụ thể được xác định trong cộng đồng của chúng ta.
Vui lòng cung cấp phản hồi về bản tin này và những gì chúng tôi có thể làm tốt hơn thông qua khảo sát này: Khảo Sát Về Bản Tin

Sử Dụng Mật Khẩu Mạnh Cho Tài Khoản Trực Tuyến

- Đặt mật khẩu mạnh và nhớ thay đổi mật khẩu thường xuyên. Điều này sẽ bảo vệ các tài khoản trực tuyến của quý vị.
- Mật khẩu mạnh có ít nhất 8 ký tự và bao gồm sự kết hợp của chữ hoa và chữ thường, ký hiệu và số. Mật khẩu càng dài thì càng an toàn.
    - **Ví dụ về mật khẩu yếu**: password, YourName, 12345
    - **Ví dụ về mật khẩu an toàn**: 8blu3Car$dr1vinG, 1&n%00Xb#, Y3!!oWfL0w3rs
- Tránh những mật khẩu dễ đoán, chẳng hạn như ngày sinh hoặc tên của quý vị.
- Mỗi tài khoản phải có một mật khẩu riêng.
- Đừng ghi danh sách mật khẩu trên một tờ giấy, đặc biệt là gần máy tính của quý vị.
- Mật khẩu chỉ nên được chia sẻ với những người mà quý vị biết và tin tưởng và nên được cất giữ ở nơi an toàn.

Đề Phòng Vi-rút Và Phần Mềm Độc Hại

- ***Phần mềm độc hại*** là một loại phần mềm có hại cho máy tính. ***Vi-rút*** là một loại phần mềm độc hại.
    - Vi-rút và phần mềm độc hại xâm nhập vào hệ thống máy tính mà không được cho phép và "lây nhiễm" cho máy tính.



    - Vi-rút và phần mềm độc hại có thể lấy cắp thông tin của quý vị, làm chậm và làm hỏng máy tính hoặc kiểm soát hoàn toàn máy tính của quý vị.
    - Vi-rút và phần mềm độc hại xâm nhập vào máy tính của quý vị khi quý vị nhấp vào liên kết hoặc mở email bị nhiễm vi-rút và phần mềm độc hại.
    - Hãy cẩn trọng trước khi nhấp vào liên kết chào mời giải thưởng hoặc thứ gì đó miễn phí.
    - Những thứ này có thể trông giống như trò chơi, màn hình chờ hoặc nội dung tải xuống nhưng đó có thể là phần mềm độc hại hoặc vi-rút.

Suy Nghĩ Trước Khi Nhấp Vào

- Để ý người gửi email và thư quý vị nhận được trực tuyến.

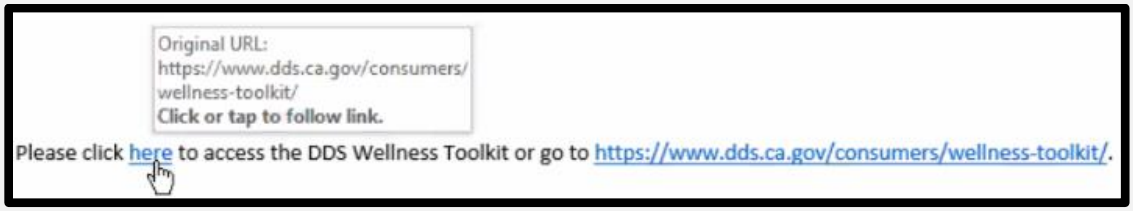
    - Kiểm tra địa chỉ email của họ để xem có khớp với địa chỉ mà mà quý vị đã có với họ hay không.
- Hãy đặc biệt cẩn thận nếu người gửi thúc giục quý vị trả lời ngay lập tức hoặc làm như đang có vấn đề cấp bách, chẳng hạn như vấn đề với tài khoản ngân hàng của quý vị. Những loại thư này rất có thể là lừa đảo.
- Tấn công giả mạo là một hình thức lừa đảo trên internet nhằm lừa mọi người chia sẻ thông tin cá nhân của họ bằng cách sử dụng các tin nhắn giả trông giống như thật.
    - Trước khi trả lời thư, hãy kiểm tra người gửi lạ, lỗi chính tả hoặc ngữ pháp, liên kết không khớp với nội dung thư, tệp đính kèm ngẫu nhiên và yêu cầu quý vị phải thực hiện gấp.

    - Không mở tệp đính kèm hoặc nhấp vào các liên kết mà quý vị không nhận diện. Chúng có thể là giả mạo và dẫn đến việc cài đặt vi-rút có thể gây hại cho máy tính hoặc điện thoại của quý vị hoặc lấy cắp thêm thông tin từ quý vị.
    - Khi quý vị nhận được một email bất ngờ với các liên kết hoặc tệp đính kèm, hãy luôn kiểm tra với người gửi (qua điện thoại hoặc tin nhắn) để đảm bảo rằng chính họ đã gửi email đó.
- IRS sẽ chỉ gửi cho quý vị các thông báo bằng thư gửi qua đường bưu điện Hoa Kỳ. Không trả lời các cuộc gọi, email hoặc tin nhắn văn bản nói rằng họ là người của IRS.

Bản Tin Sức Khỏe Và An Toàn do Sở Dịch Vụ Phát Triển ấn hành để cảnh báo cho các cá nhân, gia đình và những người khác về những rủi ro cụ thể được xác định trong cộng đồng của chúng ta.
Vui lòng cung cấp phản hồi về bản tin này và những gì chúng tôi có thể làm tốt hơn thông qua khảo sát này: Khảo Sát Về Bản Tin

Biết Quý Vị Đang Gửi Email Hoặc Nhắn Tin Cho Ai

- Hãy nhớ rằng những người quý vị tiếp xúc qua mạng có thể không phải như họ nói.
- Không bao giờ chia sẻ thông tin cá nhân hoặc gửi ảnh của quý vị cho người lạ hoặc người nào đó mà quý vị chưa từng gặp trực tiếp.
- Không bao giờ gửi tiền cho người mà quý vị chỉ mới gặp gần đây hoặc chưa từng gặp trực tiếp.
- Trước khi quý vị nhập số an sinh xã hội hoặc bất kỳ số tài khoản nào vào biểu mẫu trực tuyến hoặc trang web, hãy đảm bảo rằng người gửi hỏi thông tin này chính là người như họ nói.
    - Kiểm tra địa chỉ email của người gửi bằng cách di chuyển con trỏ qua tên của họ hoặc liên kết để đảm bảo rằng địa chỉ này có vẻ như đến đúng doanh nghiệp.



- Họ có thể sao chép biểu trưng và làm cho email trông giống như thật, vì vậy hãy xem xét chúng cẩn thận để phát hiện lỗi chính tả, nội dung kỳ quặc hoặc hình ảnh mờ.
- Nếu quý vị không chắc người gửi là thật, hãy liên hệ với công ty hoặc tổ chức từ tài khoản trực tuyến của quý vị hoặc gọi điện trực tiếp cho họ.

Phải Làm Gì Nếu Quý Vị Là Nạn Nhân Của Tội Phạm Mạng

- Nói với người mà quý vị tin tưởng ngay lập tức.
- Nếu tội phạm liên quan đến hành vi truy cập vào tài khoản cá nhân của quý vị, hãy gọi cho ngân hàng hoặc công ty phát hành thẻ tín dụng của quý vị và thông báo cho họ biết ngay lập tức. Ngừng sử dụng bất kỳ thẻ ghi nợ hoặc thẻ tín dụng nào cho các tài khoản đã được truy cập.
- Thay đổi mật khẩu của quý vị đối với bất kỳ tài khoản hoặc thông tin đăng nhập nào đã bị tấn công.
- Theo dõi tài khoản của quý vị để phát hiện hoạt động bất thường.

Bản Tin Sức Khỏe Và An Toàn do Sở Dịch Vụ Phát Triển ấn hành để cảnh báo cho các cá nhân, gia đình và những người khác về những rủi ro cụ thể được xác định trong cộng đồng của chúng ta.
Vui lòng cung cấp phản hồi về bản tin này và những gì chúng tôi có thể làm tốt hơn thông qua khảo sát này: Khảo Sát Về Bản Tin