Tech Savvy Seniors

Giới thiệu về an toàn trên mạng: Cách để giữ an toàn trên mạng

Internet đã trở thành một phần không thể thiếu được trong cuộc sống của chúng ta và chúng ta có thể làm được nhiều thứ trên mạng.
Chúng tôi muốn nói với bạn về cách dùng Internet an toàn hơn và sự cẩn thận tổng quát để bảo vệ sự riêng tư của bạn.

1. Tôi có cần tự bảo vệ mình trên internet?

Trên internet, ai cũng có thể giả danh một người nào đó, vì vậy bạn cần phải biết nên nhận emails của ai, nơi an toàn để mua hàng, và với ai bạn nên cho các chi tiết riêng tư.

Phần mềm bảo vệ internet đóng vai trò quan trọng giữ sự an toàn cho bạn trên mạng.

Một vài bước ý thức căn bản sẽ giúp bạn khó bị lường gạt:

- Bảo vệ máy vi tính và các hệ thống không dây bằng mật khẩu?
- Không bao giờ cho các chi tiết ảnh hưởng, riêng tư cho người lạ trên mạng.
- Lắp đặt một phần mềm bảo vệ.

2. Các mối đe dọa bạn có thể gặp

1. Phần mềm độc hại

Phần mềm độc hại (phần mềm độc): được tạo nên với ý định xâm nhập máy vi tính của bạn và thu thập tin tức, thường là để bán cho những ai muốn mua. Phần mềm độc hại phổ biến là một loại vi khuẩn. Bạn phải cẩn thận về các chương trình bạn tải xuống và chạy trên máy điện toán của bạn. Nếu bạn tải xuống từ một nguồn không tin cậy, nó có thể đã nhiễm khuẩn.

Ngay cả khi bạn lướt mạng một cách an toàn, bạn vẫn không thể ngăn chặn 100% các mã độc mới nhất hay do bạn bất cẩn. Vì vậy, bạn phải cài đặt phần mềm chống khuẩn lên máy vi tính của bạn để có được sự bảo vệ đúng lúc.
Loại vắc xin nầy là chính yếu cho máy vi tính của bạn bởi vì nó xem xét không chỉ mạng internet mà còn cả các dụng cụ ngoại vi như USB và CD nũa.

2. Các tin tặc

Tin tặc (hay bot): là kẻ lợi dụng sự dễ bị tổn thương về an toàn trên máy vi tính cũa bạn đễ lấy thông tin cá nhân của bạn.

Thí dụ, bạn có biết về chia xẽ dữ liệu trên Windows? Điều này cho phép một máy vi tính gởi văn kiên đến một máy khác qua 1 mạng liên lạc. Nhưng nếu nó không được bảo vệ bằng mật khẩu, một tin tặc có thể phát hiện và sữ dụng nó để lấy thông tin của bạn hay cấy vi khuẩn hoặc 1 phần mềm độc hại lên máy vi tính của bạn.

3. Trộm danh tính, lường gạt và lừa đảo

Không có một luật lệ nào quy định việc bạn nói bạn là ai trên internet, vì thế ai cũng có thể giả làm một thứ gì đó hay ai đó để làm cho bạn đưa tiền hoặc thông tin cá nhân như số thẻ tín dụng hay chi tiết vào ngân hàng mạng. Chủ yếu, nghệ thuật lừa đảo nầy được tiến hành trên mạng, và chúng cố lợi dụng bạn. Một cách lường gạt phổ biến là kẻ lừa đảo giả vờ là người hoặc tổ chức mà bạn có liên hệ và làm cho bạn đưa ra thông tin cá nhân, như các chi tiết ngân hàng của bạn.

Có một vài cách đơn giản để giúp nhận ra sự lường gạt và lừa đảo và tránh gặp rắc rối trên internet. Đây là một vài thứ cần phải để ý.

- Kiểm tra đề tựa của emails và người gởi. Nó có đến từ một người mà bạn biết, và nó mô tả điều gì mà bạn nhớ? Nếu không, có thể là thư rác.
- Nó có hứa đưa tiền cho bạn để đổi lấy thông tin cá nhân của bạn? Nó có đe dọa một hậu quả nếu bạn không trả lời với các thông tin cá nhân, hay phải nhấn chuột vào đường nối? Nó có để tên bạn sẵn vào ô tới? Đây là các dấu hiệu của một sự lường gạt.
- Nếu email có lỗi văn phạm hoặc chính tã, và trình bày một cách tệ hại? Nếu email đó lại đến từ một tài khoản email 'tự do' (như outlook.com, yahoo.com, gmail.com)? Nếu đúng vậy, và người gởi lại là người lạ bạn không biết, hãy nghi ngờ nó.

Các email 'lừa đảo mơ hồ' có thể trông rất mời gọi, và đa số trông rất thật. Nếu bạn bị lôi cuốn hãy tự hỏi tại sao bạn lại nhận được email này, xem lại các tên, các địa chỉ, và các trang mạng. .

4. Phần mềm bảo vệ làm được những gì?

Các loại phần mềm bảo vệ

Tin mừng là bạn có thể tự bảo vệ mình từ hầu hết các cuộc tấn công bằng cách dùng phần mềm bảo vệ. Máy vi tính của bạn đã có sẵn một vài phần mềm bảo vệ, nhưng bạn nên có thêm phần mềm bảo vệ nữa. Có nhiều loại phần mềm bảo vệ khác nhau mà bạn có thể thêm vào:

1. Chống vi khuẩn: Phần mềm này bảo vệ máy vi tính của bạn từ hầu hết các loại phần mềm độc hại (và tùy thuộc vào phần mềm có sẵn trong máy vi tính của bạn cho phần còn lại). Bạn có thể có được phần mềm này miễn phí hay chỉ trã 1 số tiền nhỏ.
2. Trọn bộ bảo vệ internet: Một phần mềm trọn gói sẽ bảo vệ máy vi tính của bạn từ một loạt đe dọa, bao gồm phần mềm độc hại, lừa đảo, thư rác, các trang web lừa gạt, tin tặc, và nhiều nữa. Trọn bộ bảo vệ internet có kèm theo lệ phí hàng năm (thường từ $60 đến $130).

Bảo vệ máy vi tính của bạn

1. Một tường lửa hoạt động như là một trạm kiểm soát an toàn cho lưu thông internet – nó chỉ cho phép các lưu thông thực sự đi qua.
2. Phần mềm chống khuẩn truy tìm và loại bỏ các phần mềm độc hại – bao gồm vi khuẩn, phần mềm gián điệp, phần mềm quảng cáo – đang tìm đến máy vi tính của bạn. Máy vi tính của bạn hầu như không có phần mềm chống khuẩn, và bạn nên có nó.

5. Chọn phần mềm bảo vệ

Bạn được khuyên là các dụng cụ nối mạng internet – máy vi tính của bạn, máy tính bảng hay điện thoại thông minh – nên được bảo vệ với phần mềm chống vi khuẩn hay, lý tưởng hơn trọn bộ bảo vệ internet. Nếu bạn không thể trả nổi lệ phí hàng năm, bạn nên chọn một ứng dụng chống vi khuẩn miễn phí. Nó không tốt bằng trọn bộ bảo vệ, nhưng nó sẽ cho bạn một sự bảo vệ căn bản.

Các chương trình chống vi khuẩn miễn phí kèm theo dưới đây:

Microsoft: www.microsoft.com/securityessentials

AVG: www.avgfree.com.au

Avast!: www.avast.com

Comodo: www.antivirus.comodo.com

6. Giử an toàn cho chính bạn (phần mềm bảo vệ là không đủ)

Cài đặt phần mềm bảo vệ trên máy vi tính của bạn là một bước to lớn và quan trọng để bảo vệ bạn trên mạng. Nhưng nó không phải là tất cả: phần mềm bảo vệ không thể bảo vệ bạn từ các kẻ lừa đảo và tội phạm trên mạng. Nhiều thứ chúng ta làm trên mạng có các thông tin quan trọng, cá nhân và riêng tư. Thông tin cá nhân là những thông tin về danh tính của bạn. Để bảo vệ thông tin cá nhân, bạn nên cẩn thận về các điều bạn chia xẻ công cộng trên mạng.

Ý thức căn bản và một mức nghi ngờ lành mạnh sẽ làm cho bạn khó bị lừa gạt!

Có vài thứ đơn giản bạn có thể làm để giử an toàn cho mình:

1. Hãy dùng một mật khẩu/cụm từ mạnh mẻ và duy nhất, và thay đổi nó thường xuyên
2. Đừng đưa thông tin cá nhân lên các trang mạng công cộng
3. Đừng mỡ các phần đính kèm email trừ khi bạn biết chắc
4. Cẩn thận về các emails mà bạn trả lời
5. Cẩn thận về người mà bạn cho các chi tiết về thẻ tín dụng
6. Đừng cài đặt các chương trình từ các nguồn không đáng tin cậy