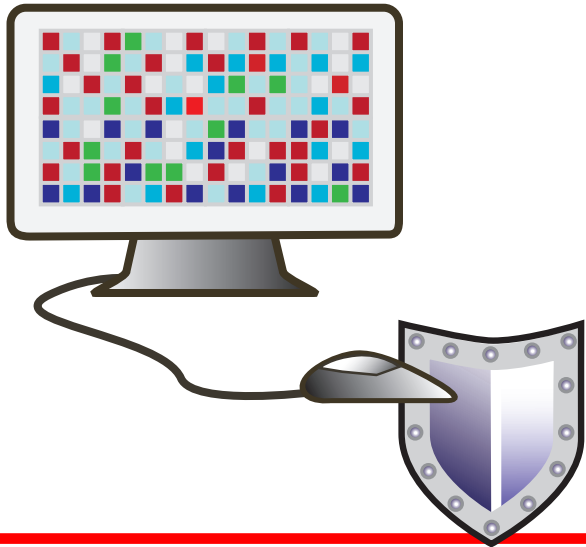


AN TOÀN TRÊN MÁY ĐIỆN TOÁN: Công Việc của Mọi Người

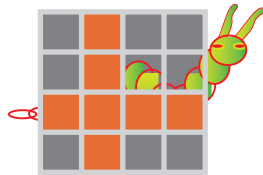
Máy điện toán và mạng lưới Internet là những tiêu điểm ưa chuộng đối với các tên tội phạm. Không có sự bảo vệ, các tên trộm có thể xâm nhập vào máy điện toán của quý vị và lấy trộm số thẻ tín dụng của quý vị, thông tin trương mục ngân hàng, và các tư liệu quan trọng khác của quý vị.

Tất cả những người sử dụng máy điện toán nên thực thi các biện pháp gia tăng sự an toàn và làm giảm nguy cơ bị hư hại cho quý vị và máy điện toán của quý vị. Đây là một vài mẹo thường dùng về an ninh điện toán để quý vị biết cách giữ cho máy điện toán của quý vị được an toàn.



Các Vi-rút & Sâu

Một “vi-rút” điện toán tự kèm nó vào các chương trình trên máy điện toán của quý vị và gây hư hại đến các chương trình, thông tin hoặc thiết bị của máy. Một “sâu” điện toán có tác dụng giống như vậy và còn có thể tự tái tạo nó. Các loại này có thể làm hư hại máy điện toán của quý vị và còn nhiễm cho những người khác nữa.



BIỆN PHÁP:

Đây là những điều quý vị có thể thi hành ngay lập tức mà không mất nhiều thời gian hoặc nhiều tiền. Một số điều chỉ cần thay đổi thói quen.

Mật mã

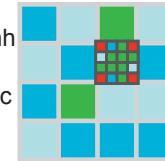
Mật mã bảo vệ dữ liệu quý vị giữ trên máy điện toán của quý vị, bao gồm các trương mục tư mật, tài liệu, và sự tiếp cận đến thông tin có thể nhận dạng quý vị.



Cách tốt nhất để giữ cho các kẻ xâm nhập vào máy điện toán quý vị (“tín tặc”) và những người khác không biết được mật mã của quý vị là hãy cố gắng sử dụng một tổng hợp bằng chữ, số và các dấu hiệu (như là !, @, #, \$, %). Điều quan trọng hơn hết, xin đừng bao giờ cho bất cứ ai biết mật mã của quý vị. Hãy giữ hồ sơ ghi các mật mã ở một nơi an toàn và thay đổi mật mã thường xuyên.

Các Cập Nhật & Sửa Đổi

Cập nhật hoặc sửa đổi là một chương trình nhỏ của máy điện toán để sửa chữa các vấn đề về nhu liệu đã từng được biết. Các công ty sản xuất nhu liệu phát hành các sửa đổi mới thường xuyên và thông báo cho quý vị biết các cập nhật cần thiết qua mạng web hoặc bằng điện thư nếu quý vị có đăng ký sản phẩm nhu liệu của quý vị.



Điều quan trọng là tiếp tục cài đặt các sửa đổi mới nhất. Quý vị có thể sắp đặt cho máy điện toán của mình tự động làm việc này. Máy điện toán sẽ xét với các công ty nhu liệu để sửa đổi hệ thống điều hành của quý vị, hệ trình duyệt và các chương trình chống vi-rút.

“Firewall” & Nhu Liệu Phòng Chống Vi-rút/Nhu Liệu Gián Điệp

“Firewall” là hệ thống sàng lọc hạn chế việc di chuyển thông tin giữa các hệ thống mạng lưới máy điện toán. Hệ thống sàng lọc ngăn ngừa không cho thông tin bị lọt ra ngoài và giữ không cho các chương trình phiền nhiễu được xâm nhập vào.



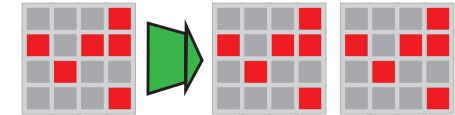
Nhu liệu phòng chống vi-rút, hoặc nhu liệu chống vi-rút, cố gắng nhận ra, vô hiệu hóa hoặc loại bỏ nhu liệu quái ác. Các chương trình này sẽ cố gắng “tắt” hoặc “khử” vi-rút,

“cô lập” nó, hoặc “tiêu hủy” nó, bằng cách rà soát máy điện toán của quý vị thường xuyên.

Trong phần sắp đặt hệ trình duyệt của quý vị, quý vị có thể gia tăng các sắp đặt về an ninh và ngăn chặn các quảng cáo hiện lên trên màn hình (pop-up).

Có các hệ “firewall” và các chương trình chống vi-rút miễn phí và dễ sử dụng. Xin tìm hiểu thông tin về các chương trình này trên mạng trực tuyến bằng cách truy tìm “firewall software” hoặc “anti-virus programs”.

Sao Lưu Tài Liệu



Sao lưu các hồ sơ quan trọng hoặc các tài liệu từ máy điện toán của quý vị cũng quan trọng như có các bản sao giấy khai sanh hoặc giấy thông hành của quý vị. Quý vị có thể bảo vệ tài liệu và hồ sơ của quý vị bằng cách lưu chúng vào một disk, thiết bị “USB thumb drive”, hệ lưu trữ trên web hoặc thiết bị lưu trữ khác. Hãy làm điều này thường xuyên!

BẢN KIỂM KÊ

Đây là một bản kiểm kê các biện pháp mà các người sử dụng máy điện toán tại nhà có thể thi hành để bảo vệ máy điện toán của họ. Bản kiểm kê này từ Trung Tâm Điều Phối của Đội Ngũ Sẵn Sàng Ứng Phó Tình Huống Khẩn Cấp Về Máy Điện Toán (CERT). Quý vị có thể tìm hiểu thêm chi tiết ở: www.cert.org/tech_tips/home_networks.html.

- Dùng nhu liệu phòng chống vi-rút
- Dùng hệ thống “firewall”.
- Đừng mở các tài liệu gửi kèm theo các điện thư mà quý vị không quen biết.
- Đừng sử dụng các chương trình mà quý vị không biết nguồn gốc.
- Khởi động hệ thống cho thấy các chữ cuối của filename (filename extension).
- Tiếp tục cập nhật tất cả các chương trình ứng dụng (bao gồm hệ điều hành).
- Tắt máy điện toán của quý vị hoặc gỡ dây điện ra khỏi hệ Internet khi không sử dụng máy.

Các Nhu Liệu Gián Điệp và Quảng Cáo



Mọi người đều muốn bảo vệ sự riêng tư của mình. Không may là các nhu liệu gián điệp (“spyware”) và các chương trình quảng cáo (“adware”) có thể được đặt vào máy điện toán quý vị mà không có sự cho phép của quý vị.

Quý vị có thể vô tình cài đặt các chương trình này vào máy điện toán của mình bằng cách xem một số website nào đó, bấm vào một số mạch nối, tải xuống các tài liệu từ Internet hoặc mở các tài liệu gửi kèm theo các điện thư.

Nhu liệu gián điệp thu thập thông tin cá nhân và gửi thông tin đó đến các tay tội phạm. Nhu liệu quảng cáo trình bày các bảng quảng cáo mà quý vị không muốn lên các “window” hiện lên trên màn hình hoặc tạo ra một dãy trưng bày quảng cáo trên màn hình máy điện toán của quý vị.

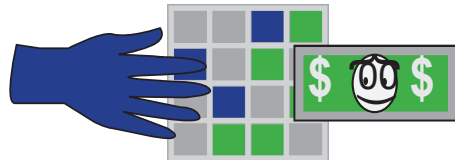
Các Mưu Đồ & Điện Thư Gạt Gỡ để lấy Tiền quý vị

Đừng hồi âm các điện thư “junk” – hãy xóa bỏ chúng!

Chỉ nên mở điện thư và bấm vào các mạch nối từ những người quý vị quen biết và tin cậy.

“Spam” là các điện thư “junk” mà quý vị không bao giờ yêu cầu. Đừng hồi âm chúng, chỉ cần bỏ nó đi.

“Phishing” là một mưu đồ bắt lương qua mạng trực tuyến dùng “spam” hoặc các lời nhắn trên pop-up để lừa cho quý vị chia sẻ thông tin cá nhân như là số An Sinh Xã Hội hoặc mật mã của quý vị. Các tay lường gạt bằng “phishing” gọi là “phisher” và chúng giả mạo điện thư và trang web của chúng như là từ ngân hàng hoặc từ các cơ sở tin cậy khác. Chúng cố gắng lừa gạt cho quý vị cung cấp số trương mục ngân hàng và số mật mã của quý vị. Đừng hồi âm hoặc đừng bấm vào các mạch nối nào yêu cầu quý vị cấp thông tin cá nhân. Hãy xóa bỏ chúng!



Xin quý vị cũng xem website An Ninh về Thông Tin (Information Security) của Seattle ở:
www.seattle.gov/informationsecurity.

Quý vị cũng có thể xem Trang An Ninh của Microsoft để biết thông tin trong nhiều ngôn ngữ khác nhau. Xem các thông tin đó ở: <http://www.microsoft.com/protect> và chọn ngôn ngữ của quý vị bằng cách bấm vào “worldwide sites”.

ĐỂ ĐƯỢC GIÚP ĐỠ:

Quý vị có thể có các bản in của thông tin này bằng cách gọi số (206) 233-7877 hoặc viết thư gửi chúng tôi ở PO Box 94709, Seattle, WA, 98124-4709.

Các thư viện công cộng tại địa phương quý vị và các trung tâm kỹ thuật tại cộng đồng quý vị cũng là nơi lý tưởng để biết thêm thông tin. Xin xem:
www.seattle.gov/tech/techmap

Các công ty trợ giúp kỹ thuật điện toán và các diễn đàn trên mạng trực tuyến cũng cung cấp giúp đỡ. Tạp chí “Consumer Reports”, các tạp chí máy điện toán, các tiệm máy điện toán, các công ty sản xuất máy điện toán và các công ty nhu liệu cũng có thể cung cấp thông tin hữu dụng.

Bản in này được biên soạn do Thành Phố Seattle,
Chương Trình Kỹ Thuật Cộng Đồng của Bộ Kỹ Thuật
Thông Tin và Phòng An Ninh Về Thông Tin.
www.seattle.gov/tech
www.seattle.gov/informationsecurity

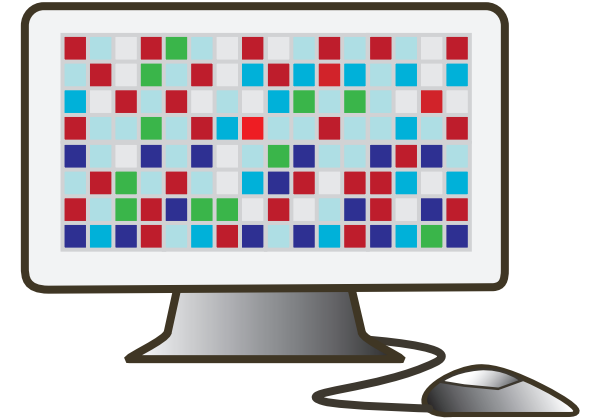
Thông tin này được cung cấp để giáo dục và mang đến cho công chúng sự nhận thức. Dù chúng tôi cố gắng đem lại thông tin càng chính xác càng tốt, nhưng chúng tôi không thể bảo đảm là tất cả các thông tin đều đúng và chúng tôi không chịu trách nhiệm cho bất cứ thiếu sót nào.

Chúng tôi khuyến khích quý vị nên tự tìm tòi thêm và bàn bạc với các chuyên viên giàu kinh nghiệm về an ninh điện toán.

Version 01/2010



MÁY ĐIỆN TOÁN CỦA QUÝ VỊ CÓ AN TOÀN KHÔNG?



Các mẹo để bảo vệ máy điện toán và an ninh của quý vị

