

Máy điện toán và mạng điện toán đã thay đổi thế giới của chúng ta. Bây giờ, chúng ta có thể làm việc, học hỏi, vui chơi, chuyện trò, mua sắm và quản lý đời sống hàng ngày của mình trên mạng mà không phải ra khỏi căn nhà yên ấm của chúng ta.

Tuy nhiên, không phải người nào chúng ta liên lạc trên mạng điện toán cũng đều đáng tin. Người ẩn danh dùng mạng để xách nhiễu hay quấy rầy người khác, phá hoại hệ thống điện toán hay trữ liệu, hoặc ngay cả phạm tội ác.

May mắn thay, nhờ vào các bước phòng ngừa đơn giản, quý vị có thể tránh trở thành nạn nhân. Bằng cách biết mình muốn gì, cẩn trọng, và dùng các thiết bị bảo vệ, quý vị có thể thụ hưởng các lợi ích của mạng điện toán mà vẫn bảo vệ sự an toàn và an ninh cho các trữ liệu và các tin tức cá nhân của quý vị và gia đình trong máy điện toán.

### Mầm Mống Nguy Hiểm cho Người Dùng Mạng Điện Toán

Tùy vào cách dùng mạng của quý vị để có thể phạm vào và các nguy cơ không cần thiết, quý vị có thể gặp nguy cơ của nạn trộm danh tính cá nhân (khi có ai ăn cắp và dùng các tin tức cá nhân của quý vị, có lẽ để mở các trương mục tín dụng mới; hay các hãm đoạ đến an ninh cá nhân (đôi khi còn gọi là “*cyberstalking*” nghĩa là đeo đuôi trên mạng hay “*cyberbullying*” uy hiếp trên mạng). Dưới đây là các cách kẻ gian và lừa đảo tìm các nạn nhân trên mạng:

- Phishing (mạo nhận)*** — ránh “câu” quý vị vào chuyện tiết lộ tin tức cá nhân và các chi tiết bảo mật khác bằng cách gửi các email giả mạo nhìn giống như từ các cơ sở thương mại đáng hoàng.

- Spam (thư tạp nhạp)*** — các *email* và lời nhắn liền (instant message) không mời mà gửi, rêu rao bán các hàng hoá khả nghi hay hứa tặng tiền thường nếu quý vị gửi tiền cho người gửi thư.

- Malware (phần mềm độc hại)*** — các phần mềm độc hại (*spyware*, *Trojans*, *viruses* và *worms*) có thể tự động cài vào trong máy điện toán của quý vị, nó để cho người kiểm soát các phần mềm độc hại này căn cấp, hủy hoại hay xoá các hồ sơ và trữ liệu khác của quý vị.

- Các chuyển dịch không an toàn*** —các trang điện toán không có sự bảo vệ các mẫu đơn trả tiền trên mạng cho an toàn, hay các công ty lưu trữ tin tức về thẻ khấu trừ (*debit*) và thẻ tín dụng không có hệ thống bảo vệ đáng hoàng và kẻ gian có cơ hội đột nhập vào các tin tức cá nhân của quý vị.

- Mạng lưới chuyện trò*** — người sử dụng có thể bị nguy hiểm nếu họ

tiết lộ quá nhiều về các tin tức cá nhân, hay họ đồng ý đích thân đến gặp người họ mới quen lần đầu trên mạng. Ngay cả một số trang chuyện trò trên mạng cũng có thể không bảo vệ an ninh cho các tin tức cá nhân.

### Bảo Vệ Máy Điện Toán và Trữ Liệu của Quý Vị

Có rất nhiều cách để ai đó có thể coi được các tin tức cá nhân của quý vị. Cũng may quý vị tự bảo vệ mình bằng nhiều cách.

- Dùng tường chắn firewall.*** Hệ thống firewall là bức tường chắn vô hình giữa máy điện toán của quý vị và mạng điện toán. Mọi thứ vào trong hay rời máy điện toán của quý vị phải đi ngang qua firewall để ngăn cản bất kỳ thứ gì không đạt tới điều kiện an ninh ấn định. Trước khi mua riêng một tường firewall phần cứng hay mềm, quý vị nên kiểm qua hệ thống hoạt động (hay *OS-operating system*) để xem đã có sẵn firewall trong đó và nó đã được bật lên chưa. (*Mac OS X* hay *Windows Vista* là hai hệ thống hoạt động được trung dụng rộng rãi.)

- Gắn antivirus software (phần mềm chống vi khuẩn).*** Phần mềm antivirus thanh lọc mọi thứ đi vô trong máy điện toán của quý vị, tìm kiếm các loại vi khuẩn đã biết tên. Vì vi khuẩn mới lúc nào cũng được tạo ra, quý vị cần phải thường xuyên cập nhật phần mềm chống vi khuẩn.

- Gắn antispyware software (phần mềm chống spyware).*** Spyware là phần mềm đi lẩn theo hoạt động trong máy điện toán để thu thập dữ kiện mà quý vị không biết. Phần mềm chống spyware ngăn chặn hay xoá bỏ spyware. Một số sản phẩm chống vi khuẩn có luôn phần mềm chống spyware.

- Dùng bộ phận gạn lọc spam.*** Đa số các hãng cung ứng mạng điện toán (*Internet service providers –ISPs*) và các chương trình email hiện bao gồm luôn bộ phận gạn lọc spam tự động để giảm thiểu số lượng emails không chính thức lọt vô được hộp thư của quý vị. Bấm “*delete*,” không cần phải mở ra bất cứ thư spam hay “thư tạp nhạp” đã lọt qua được bộ phận gạn lọc.

- Cập nhật thường xuyên.*** Các công ty điện toán và phần mềm thường cập nhật các chương trình của họ cũng kèm theo sự bảo vệ chống vi khuẩn. Vì vậy, chỉ việc cập nhật hệ thống hoạt động và phần mềm khi có bản mới nhất sẽ cho quý vị tăng phần bảo vệ. Nếu có được, hãy bật phần cập nhật tự động để quý vị được báo ngay khi có cập nhật.

- Tạo các mật mã khó đoán.*** Một mật mã khó đoán bao gồm các mẫu tự, con số, và dấu hiệu lẫn lộn. Đừng bao giờ dùng các tin tức cá nhân, chẳng hạn như ngày sinh tháng đẻ của quý vị, địa chỉ hay tên thú vật trong nhà. Nên bao gồm ít nhất tám chữ trong mật mã của quý vị. Mật mã càng dài càng khó cho kẻ đột nhập đoán hay giải.

- Bảo vệ sự an toàn cho hệ thống mạng không dây (wireless network) của quý vị.*** Để hệ thống mạng “không khoá” có nghĩa bất cứ người nào ở trong phạm vi tín hiệu *wifi* của quý vị cũng có thể sử dụng được – và họ có thể bắt được trữ liệu quý vị gửi đi hay nhận vào. Bảo vệ sự an toàn cho hệ thống mạng không dây của quý vị không khó, nó giống như tạo một mật mã khó đoán cho “*router*” (máy phát sóng) và bộ phận hoạt động *encryption* (mật mã hoá) của quý vị.

### Ghi Chú Quan Trọng Về Các Máy Điện Toán Cũ

Nếu quý vị có một máy điện toán cũ, quý vị có thể không còn nhận được các cập nhật và các “*patches*” để bảo vệ các yếu điểm trong máy, cũng như hãng chế tạo chắc chắn không cung ứng sự trợ giúp cho máy điện toán của quý vị. Bộ phận dò tìm sử dụng trong ấn bản mới không hoạt động trong máy có hệ thống hoạt động cũ hơn. Tường *firewall* tương đối mới và được bật lên tự động bằng bộ phận “*default*” (mở lên tự động) của hãng chế tạo sử dụng cho các máy điện toán mới hơn. Nhưng tường firewall có thể không bật lên được trong các máy cũ. Hậu quả là máy cũ với “*always on*” nghĩa là đường dây lúc nào cũng nối vào mạng với tốc độ cao (*high-speed*) có thể bị nguy cơ về mất an ninh và bảo mật.

### Bảo Vệ Sự Kín Đáo của Quý Vị Đối Với Các Quảng Cáo Trên

### Mạng

Canh chừng tin tức cá nhân của quý vị khi viếng mạng điện toán không những ngừa được kẻ gian, nó còn giúp giảm thiểu các rắc rối như các tin nhắn quảng cáo gửi tới ấu tả.

Cách đơn giản nhưng hữu hiệu để duy trì sự kín đáo là tiết lộ thật ít về quý vị đối với các trang điện toán không quen thuộc cho đến khi quý vị quyết định muốn giao dịch với họ. Bất kỳ khi nào quý vị điền mẫu đơn, tham dự cuộc thi trên mạng, hay gửi các dữ kiện qua đường điện tử, mà nó có thể bị dùng cho mục đích quảng cáo bởi công ty của trang điện toán quý vị đang viếng, hay bởi thành phần trung gian mua các tin tức này, quý vị nên đọc “*Privacy Policy*” (nội quy về sự bảo mật) của mạng điện toán mà quý vị tiếp xúc để biết chắc họ sẽ không bán hay trao đổi các thông tin liên lạc của quý vị.

Quý vị cũng nên quản lý các “*cookies*.” *Cookies* có thể được gài trong cơ phận máy điện toán sau khi quý vị đã viếng trang điện toán đó. *Cookie* sẽ để cho người chủ trang điện toán đó biết các trang nào quý vị đã viếng, và quý vị khi mua sắm đã bỏ món hàng nào vào trong xe đẩy. Các dữ kiện này sẽ lưu lại mỗi khi quý vị viếng trang điện toán. Các công ty đôi khi dùng *cookies* để họ tập trung vào nỗ lực quảng cáo. Nếu quý vị không muốn trang

điện toán lưu giữ bất kỳ các dữ kiện nào về quý vị hay nhận ra quý vị là khách viếng trở lại, quý vị vặn lên bộ phận xoá tự động các cookies của hệ thống dò tìm mạng (*internet browser*) bất cứ khi nào quý vị hết dò tìm. Quý vị cũng có thể chỉnh *browser* không cho nhận *cookies*, nhưng nó cũng có thể giới hạn quý vị viếng các trang điện toán nào đó.

Để giới hạn số lượng *emails* tạp nhạp vào trong hộp thư *email* cá nhân, quý vị có thể tạo một địa chỉ *email* khác để dùng cho các sinh hoạt nhất định trên mạng. Có nhiều dịch vụ *emails* để quý vị chọn.

Tình bơ và bấm “*delete*” các thư tạp nhạp (*spam*). Đừng hồi đáp, ngay cả bấm “*unsubscribe*” (từ chối nhận), vì sự hồi đáp của quý khẳng định rằng địa chỉ của quý vị “hoạt động.”

Các công ty chính đáng sẽ có nội quy về bảo vệ sự riêng tư cá nhân. Nội quy phải tuyên bố rõ ràng khi nào và cách công ty có thể sử dụng dữ kiện cá nhân của quý vị. nếu quý vị không hài lòng với cách công ty bảo vệ tin tức cá nhân của quý vị, ra khỏi trang điện toán đó. Tìm nhãn hiệu “*trust mark*” (dấu ấn tin cậy), như TRUSTe, đó là dấu hiệu có cầu chứng các nội quy bảo vệ sự riêng tư đáng tin.

Nếu quý vị có con cái, hãy dạy con biết đừng tiết lộ chi tiết cá nhân trên các trang điện toán. (Luật Children’s Online Privacy Protection Act [COPPA] bảo vệ dữ kiện cá nhân của trẻ em trên mạng điện toán đòi hỏi các trang điện toán phải xin phép sự đồng ý của phụ huynh khi gom tụ hay sử dụng bất kỳ chi tiết cá nhân nào của trẻ em dưới 13 tuổi.)

#### Bảo Vệ Con Em của Quý Vị Trên Mạng

Trẻ em có thể học hỏi rất nhiều qua mạng điện toán, nhưng không phải tất cả các thông tin hay nội dung trên mạng phù hợp cho trẻ em hay thiếu niên. Để giúp bảo đảm con em của quý vị có các kinh nghiệm tốt và an toàn khi dùng mạng, quý vị nên chủ động trong các sinh hoạt trên mạng mà con quý vị chú ý tới.

Đọc các “*blogs*” (chữ tắt của *web log*) mà con em quý vị ưa thích, viếng và trở thành “bạn” của mạng lưới trò chuyện trong mạng của tụi nó. Nói chuyện với con các tin tức nào phù hợp để chia sẻ và cái nào cần được giữ kín. Giải thích cho con hiểu sự không an toàn nếu nó đi một mình để gặp người nào nó “quen” trên mạng điện toán. Quý vị cũng cho con mình biết không nên cho đám bạn quen trên mạng lưới chuyện trò hay bạn ở các trang điện toán khác biết mật mã của mình. Hồ sơ (*account*) và dữ kiện cá nhân có thể bị tiết lộ và bị đánh cắp.

Giữ đường giây đối thoại mở rộng. Khuyến khích con cái đặt câu hỏi và chia sẻ kinh nghiệm dùng mạng điện toán với quý vị. Hãy cho chúng hiểu quý vị

sẽ không trừng phạt hay sẽ không cho con lên mạng nữa nếu chúng cho quý vị biết bất cứ đối thoại nào trên mạng có tính cách đe dọa hay không thích hợp, kể cả việc bắt nạt. Hãy giải thích vì sao bắt nạt trẻ con khác là điều không đúng.

Báo các hành vi xấu nhiều và lừa lọc tới các cơ quan thẩm quyền bao gồm nhà trường, sở cảnh sát địa phương, hay *CyberTipline* ([www.cybertipline.com](http://www.cybertipline.com) hoặc gọi số 800-843-5678).

Nói chuyện với con cái về các nguy cơ khi dùng mạng điện toán, và đặt ra các luật lệ về những gì con của quý vị có thể làm và các trang điện toán nào tự nó có thể viếng trên mạng. Các bộ phận phần mềm được chế tạo đặc biệt để quản lý việc dùng mạng điện toán có thể giúp quý vị bảo vệ sự an ninh cho con của mình. Nên học qua về các cách thức bảo vệ an ninh tại [kids.getnetwise.org/tools](http://kids.getnetwise.org/tools).

### Các Hướng Dẫn và Cách Thức Giữ An Ninh Khác

Dưới đây liệt kê các cách để gia tăng sự an ninh và bảo mật cho quý vị trên mạng:

- **Lập hồ sơ lưu** các hồ sơ của quý vị (ít ra mỗi tuần một lần).
- **Bật hệ thống** hoạt động và các phần mềm khác tự động cập nhật. Quý vị có thể chọn cập nhật trong giờ thuận tiện, khi không dùng máy điện toán.
- **Xoá** hết mọi thứ trong máy trước khi bán, tặng hay thải máy đi.
- **Bảo đảm** rằng mạng điện toán có an ninh bằng cách tìm *SSL encryption* (mật mã hoá) là ("<https://>" chứ không phải chỉ là "<http://>") và có dấu hiệu ổ khoá đóng hay hình chiếc chìa khoá nguyên vẹn trong khung dò tìm. Đừng bao giờ đánh số thẻ khấu trừ hay thẻ tín dụng hoặc trương mục nhà băng trừ khi quý vị đã kiểm qua các điều trên. Đa số các trang điện toán thương mại có *SSL encryption* an toàn để mua sắm trên mạng.
- **Khi mua sắm trên mạng điện toán** nên dùng thẻ tín dụng vì nó an toàn hơn là thẻ khấu trừ. Số tiền quý vị chịu trách nhiệm phải trả là \$50 nếu có sự dùng trái phép thẻ của quý vị. Trách nhiệm phải trả cho sự sử dụng thẻ trái phép cao hơn nhiều cho thẻ khấu trừ, tùy thuộc vào lúc nào quý vị khai mất thẻ, và đa số thẻ khấu trừ liên kết với trương mục nhà băng của quý vị, có nghĩa là kẻ trộm có thể vét sạch hết tiền của quý vị.
- **Đừng** để bộ phận dò tìm của quý vị giữ lại danh tính cá nhân trọng yếu và mật mã của quý vị khi "*log in*" (vào) trương mục nhà băng hay bất kỳ các

trang nào có lưu trữ tin tức về thẻ khấu trừ và thẻ tín dụng của quý vị cho "*one stop shopping*" (một cửa hàng bán đủ mọi thứ). Điều này vô cùng quan trọng nhất là khi quý vị dùng chung máy hay sử dụng máy ở thư viện công cộng. Xoá sạch các tin tức này bằng cách bấm vào chữ "*Tools*" đa số nằm trên các chỗ dò tìm và chọn "*Delete Browsing History*" hay "*Clear Private Data*." (các chữ có thể khác nhau một chút tùy vào chương trình dò tìm nào quý vị sử dụng.)

- **Chỉ mua sắm** với cửa hàng trên mạng nào quý vị tin tưởng.
- **Nếu quý vị nghi** một thư email nào mạo nhận tên, liên lạc trực tiếp tới công ty. Một cơ sở thương mại đứng đắn sẽ không bao giờ hỏi các dữ kiện cá nhân của quý vị trong *email*. Bấm bỏ thư *email* này và đừng hồi đáp.
- **Cẩn thận** về việc mở hồ sơ đính kèm "*attachments*," viếng các trang điện toán xa lạ, và tải xuống (download) các phần mềm "miễn phí." Đừng tải hay chia chung hồ sơ nhạc hay phim truyện với người lạ – hồ sơ quý vị nhận được có thể mang *virus*, *spyware* hay nội dung không thích hợp. (Và dùng chung các tài liệu đã có bản quyền là vi phạm luật.)
- **Đừng chuyển** các "*chain letters*" (thư truyền tay) và các email tạp nham tới người khác, cho dù quý vị nghĩ nó tức cười hay hữu ích. Quý vị có thể bị xem là người gửi thư bậy bạ hay tệ hơn nữa là đã chuyển một hồ sơ phá hoại đến cho người khác. Kiểm tất cả các *emails* trên trang chống lừa phỉnh ([www.snopes.com](http://www.snopes.com) hay [www.quatloos.com](http://www.quatloos.com)) trước khi quý vị bấm nút "*forward*" để quý vị đừng loan tải các tin tức thất thiệt "*urban myths*" này.
- **Tin vào linh cảm của quý vị.** Nếu điều gì có vẻ khó tin, nó đúng là như vậy. Sự phòng thủ an toàn nhất cho quý vị khi lên mạng là sự xét đoán đúng của quý vị.
- **Suy nghĩ kỹ** trước khi bấm và các bảng quảng cáo hay các quảng cáo hiện lên bắt ngờ "*pop up window*." Bấm vào dấu X ở phía góc trên bên phải cửa sổ để ngưng các quảng cáo này.
- **Nên cảnh giác** các nhạc, trò chơi và các download khác thường vì nó bao gồm luôn các phần mềm vô dụng trong đó.
- **Đừng dùng email** hay lời nhắn liền, hoặc IM, để gửi đi các tin tức cá nhân trọng yếu như số thẻ tín dụng, mật mã, ngày sinh tháng đẻ hay số thẻ an sinh xã hội của quý vị.
- **Cũng áp dụng** các điều cẩn trọng như vậy nếu quý vị nối mạng điện toán qua đường dây điện thoại smart phone hay các bộ phận nối mạng điện toán khác.

### Trợ Giúp và Hướng Dẫn

Các cơ quan dưới đây là nơi đáng tin cậy để quý vị muốn tìm hiểu thêm về sự an toàn trên mạng điện toán.

**Family Online Safety Institute** • [www.fosi.org](http://www.fosi.org)

Family Online Safety Institute là học viện vô vụ lợi giúp mạng điện toán sẽ là nơi an toàn hơn cho trẻ em và gia đình của các em.

**OnGuard Online** • [www.onguardonline.gov](http://www.onguardonline.gov)

Chính quyền Liên Bang Hoa Kỳ và các hãng kỹ thuật cung ứng các hướng dẫn và chỉ dẫn để khuyến khích việc sử dụng mạng điện toán cho an toàn và an ninh.

**Privacy Rights Clearinghouse** • [www.privacyrights.org](http://www.privacyrights.org)

Privacy Rights Clearinghouse là cơ quan vô vụ lợi cung ứng một thư viện tin tức, từ các chỉ dẫn cho người tìm việc trên mạng cho đến cách mua sắm an toàn trên mạng điện toán.

**Cơ Quan Tác Động Giới Tiêu Thụ (Consumer Action)** là một cơ quan vô vụ lợi giáo dục và bênh vực cho người tiêu thụ, cung ứng tin tức và hướng dẫn về sự bảo mật, bao gồm các quyền hạn của quý vị và cách tránh bị lừa lọc.

### Consumer Action

[www.consumer-action.org](http://www.consumer-action.org)

221 Main Street, Suite 480

San Francisco, CA 94105

415-777-9635 / TTY: 415-777-9456

[hotline@consumer-action.org](mailto:hotline@consumer-action.org)

523 W. Sixth Street, Suite 1105

Los Angeles, CA 90014

213-624-8327

Có nói tiếng Trung Hoa, Anh và Tây Ban Nha

Ấn bản này do Consumer Action biên soạn với sự hợp tác của Microsoft. © Consumer Action 2009.

Internet Safety (Vietnamese Version)



# AN TOÀN TRÊN MẠNG ĐIỆN TOÁN

**Cẩm Nang Bảo Vệ  
Sự Kín Đáo và An Ninh  
Cho Người Sử Dụng Máy Điện Toán**

Ấn bản của  
**Cơ Quan Tác Động Giới Tiêu Thụ  
(Consumer Action)**