Ấn Bản Của Consumer Action

Khóa Lại

Bảo Vệ Sự Riêng Tư Của Quý Vị Trên Mạng Điện ToánMạng Điện Toán

Mạng điện toán giúp cá nhân và gia đình có thể giao lưu, mua sắm, viếng ngân hàng, làm việc, học hỏi và giải trí trên mạng ở bất cứ đâu, bất cứ lúc nào dùng máy điện toán hay điện thoại di động. Mạng cung cấp rất nhiều lợi lộc –và đa phần, đó là nơi an toàn. Được như vậy là vì hầu hết các công ty đặt nặng tầm quan trọng trọng bảo vệ tin tức riêng tư và giữ an ninh cho trương mục của khách hàng, họ dùng các kỹ thuật hiện đại nhất để bảo đảm khách hàng lên mạng điện toán an toàn.

Thế nhưng, bảo vệ tin tức riêng tư và sự an toàn là trách nhiệm chung của cả hai phía. Để đạt được mức độ tin tức riêng tư được bảo vệ như ý muốn và sự an toàn được bảo đảm tốt nhất, người sử dụng máy điện toán và di động cần có trách nhiệm tự bảo vệ chính họ bằng cách dùng trực giác và tận dụng các công cụ an ninh có sẵn, bao gồm các công cụ do các công ty lớn cung cấp miễn phí như Google và Microsoft. Đóng vai trò chủ động quý vị sẽ hưởng thụ đời sống trên mạng thật an toàn.

Khóa Trương Mục (Account) Lại

Kỹ thuật luôn biến đổi để mang lại các phương cách tốt hơn ngăn chặn người ngoài đột nhập vào trương mục và trữ liệu (data) cá nhân của quý vị. Từ việc viếng ngân hàng hay vào mạng xã hội, các trang mạng vận chuyển những tin tức cá nhân quan trọng đều cung cấp các công cụ bảo vệ các trữ liệu của quý vị được an toàn, không bị ai dòm ngó. Một mật mã (password) khó đoán là cách hay nhằm bảo vệ trữ liệu cá nhân của quý vị; cần hai yếu tố để xác minh còn tốt hơn nữa.

Bảo vệ mật mã: Mật mã là hàng phòng vệ đầu tiên và đây là cách được sử dụng rộng rãi nhất để bảo vệ một trương mục. Quý vị cần làm như sau để có một mật mã hữu hiệu bảo vệ trương mục của quý vị.

◆ Tạo một mật mã dài ít nhất tám ký tự và đảo lộn không thứ tự giữa mẫu tự, con số và dấu hiệu với nhau. Nên viếng Google (*bit.ly/1MoNVfk*), Microsoft (*bit.ly/1JnLHbp*) hay ConnectSafely (*bit.ly/1Kyu2i2*) để biết thêm về cách tạo một mật mã thật khó đoán. Quý vị cũng có thể dùng công cụ trên mạng điện toán như "PasswordsGenerator.net" để giúp nghĩ ra một mật mã.

◆ Dấu kín mật mã. Thay vì viết xuống cho nhớ, quý vị nên dùng một công cụ lưu trữ tất cả các mật mã và quý vị chỉ cần nhớ một mật mã duy nhất. Quý vị có thể tìm hiểu thêm về cách quản lý mật mã tại PCMag.com (*bit.ly/1Otbirr*) và Lifehacker (*bit.ly/1QXEc1b*).

◆ Dùng mật mã khác nhau cho mỗi trương mục. Thay đổi nó thường xuyên khi cần—thí dụ, khi ai đó biết được mật mã của quý vị hay trữ liệu đã bị đột nhập (bị lộ hay cả một khối lượng trữ liệu của người dùng bị trộm).

◆ Chọn các câu hỏi không ai biết câu trả lời để bảo vệ sự an toàn. Nên cẩn thận khi chọn các câu hỏi người khác dễ tìm ra câu trả lời, như "Họ mẹ của quý vị là gì?" hay "Tên con thú kiểng của quý vị là gì?" (Các câu hỏi bảo vệ an toàn thường được sử dụng cho một số trương mục để kiểm chứng danh tánh cá nhân của quý vị, khi quý vị quên mật mã hay cố gắng vào trương mục từ một máy điện toán hoặc thiết bị lạ.)

◆ Đăng xuất (log out) trương mục khi quý vị dùng xong và đừng để trang chủ (browser) lưu trữ thông tin đăng nhập (log in). (Bấm "Not now," (chưa cần) "Never for this site" (không bao giờ ở trang chủ này" hay tìm lựa chọn nào tương tự như vậy khi hàng chữ hiện lên hỏi quý vị có cho phép trang chủ lưu lại mật mã, hoặc đánh dấu/không đánh dấu phù hợp vào các ô trong mục An Ninh (Security), Mật mã (password), Sync hay AutoFill trong mục "Setting" của trang chủ hoặc trong mục "Preferences.")

◆ Bắt buộc phải có mật mã để đăng nhập khi quý vị mở máy lên hay "đánh thức" nó. Làm như vậy để tạo thêm một lớp bảo vệ không cho người nào ráng vào trương mục của quý vị bằng máy của quý vị. Cách tạo mật mã cho Apple (Mac) (*apple.co/1V9p5Yt*) và cho PC (*abt.cm/1Wiy72s*). (Tạo mật mã, PIN, hay dấu vân tay cho máy di động của quý vị luôn.)

Cần hai yếu tố xác minh (2YT): Đây là cách bảo vệ mạnh hơn là chỉ dùng mật mã. Nó đòi hỏi phải có hai chứng minh để vào được trương mục (thí dụ, một mật mã và xác nhận một hình ảnh trên màn hình/hình vẽ quý vị đã chọn, hay một trương mục và rà vân tay, hay một mật mã với một bí số (passcode) được gởi đến cho quý vị bằng tin nhắn chữ hay email)--giống như quý vị cà thẻ khấu trừ (debit card) và bấm số PIN tại quầy tính tiền trong tiệm bán thực phẩm. Quý vị có thể tìm hiểu thêm về tính năng cần hai yếu tố xác minh tại trang Stop.Think.Connect. (*bit.ly/1DQlzpY*).

Bật tính năng cần hai yếu tố xác minh trong máy, nếu có ở bất cứ chỗ nào. Không phải trang mạng nào cũng cho tính năng này, nhưng nhiều trang có, bao gồm Google, Apple, Facebook, Twitter và PayPal, đó chỉ là vài thí dụ điển hình. Trong danh sách này: *bit.ly/1JpGz6w* có liệt kê nhiều trang mạng cung ứng 2YT và nhiều trang không có. (Quý vị có thể yêu cầu trang mạng quý vị dùng chưa có tính năng cần hai yếu tố xác minh, nên bắt đầu có.) Mỗi trang mạng có hướng dẫn riêng để khởi động tính năng 2YT. Xin coi trong mục "Setting" trước. Nếu quý vị không tìm ra, liên lạc với Đội hỗ trợ của trang mạng đó.

Bảo đảm an toàn trên mạng và các giao dịch trong máy di động

Mua sắm và vô ngân hàng trên mạng tiết kiệm thời gian và tiền bạc cho quý vị, đó là hai lý do lớn nhất để chi tiêu và quản lý tiền của quý vị bằng kỹ thuật điện số (digital). Và quý vị có thể bảo vệ các trương mục của quý vị bằng cách làm các bước thận trọng đơn giản và hữu hiệu, giống như quý vị bảo vệ ví tiền. Quý vị cứ an tâm thư giãn, một số công cụ bảo vệ an ninh chặt chẽ sẵn sàng giúp quý vị.

Mật hóa (Encryption): Đây là kỹ thuật đảo lộn (mật hóa) các tin tức được gởi qua mạng điện toán khiến những tên tin tặc (hackers) khó có thể dò ra các hoạt động trên mạng của quý vị để lấy trộm trữ liệu.

Để biết nếu một trang mạng quý vị đang dùng có mật hóa để bảo vệ quý vị hay không khi tin tức truyền đi từ quý vị qua trang mạng, hãy nhìn vào chữ "s," viết tắt của "secure," trong URL (https:// thay vì chỉ có http://). Quý vị cũng có thể thấy ổ khóa, hay chính trong khung địa chỉ có thể chuyển sang màu xanh lá cây khi quý vị vào một trang mạng bảo đảm an toàn. Tìm một hay hơn các dấu hiệu bảo đảm sự an toàn này trước khi quý vị mua hàng, vô trương mục tài chánh hay làm bất cứ giao dịch nào.

Nên cảnh giác vì một số email và tin nhắn chữ thông thường không được mật hóa, vì thế quý vị đừng gởi các số trương mục, số An Sinh Xã Hội hay các tin tức nhạy cảm qua cách này.

Nếu có Wi-Fi ở nhà, quý vị có hộp "router" bắt sóng không dây. Để chặn người nào ở gần nhà quý vị đọc được các tin tức quý vị gởi đi qua mạng điện toán bằng sóng không dây, quý vị nên biết chắc tính năng mật hóa trong hộp "router" của quý vị đã được bật lên (thường bắt đầu ở trạng thái tắt). Đồng thời, tạo một mật mã thật khó đoán (ít nhất là 14 ký tự lộn xộn) cho hộp "router" để ngăn chặn người nào ở gần tín hiệu phát sóng Wi-Fi của quý vị không kết nối vào được. Muốn biết thêm chi tiết về bảo vệ mạng điện toán không dây của quý vị, xin vào trang OnGuardOnline.gov (*1.usa.gov/1G2Eiya*).

Vì quý vị không phải lúc nào cũng chắc chắn mạng lưới Wi-Fi ở ngoài được mật hóa, vì thế cách an toàn nhất là dùng riêng mạng điện toán không dây của quý vị thay vì dùng mạng Wi-Fi công cộng để mua sắm hay vô ngân hàng trên mạng khi quý vị không có ở nhà. Nếu quý vị dùng chung máy điện toán hay máy di động, luôn luôn nhớ đăng xuất ra khỏi trang ngân hàng hay trang mua sắm khi quý vị hoàn tất để không ai có thể vào được trương mục của quý vị sau khi quý vị hết sử dụng. Quý vị có thể tìm hiểu thêm về cách dùng Wi-Fi công cộng cho an toàn tại trang mạng của Nha Thanh Tra Mậu Dịch Liên Bang Federal Trade Commission (FTC) (*1.usa.gov/1L62Nlr*).

Tường lửa (Firewall): Hầu hết các hệ điều hành của máy điện toán có sẵn tường lửa---tường ngăn giữa thế giới bên ngoài và máy điện toán của quý vị. Tường lửa có sẵn, nhưng không phải lúc nào cũng được bật "On" lên. Quý vị kiểm tra trong mục "Security settings" (Điều Chỉnh An Toàn) (thường tìm thấy dưới mục Tham Chiếu "Preferences") để biết chắc tường lửa đã bật lên. Nếu không tìm ra, dò trên mạng chữ "firewall" cùng với tên hệ điều hành máy điện toán của quý vị để được hướng dẫn.

Máy Di Động An Toàn

Điện thoại thông minh hay máy phiến bảng rờ giúp quý vị sử dụng tất cả các tính năng của mạng điện toán ở bất cứ đâu. Vì dễ cầm theo và kỹ thuật của nó đem đến quá nhiều tiện lợi cho người sử dụng, nên các máy di động cũng đưa đến nhiều bất ổn cụ thể về tin tức riêng tư và sự an toàn cho người dùng. Nó không có nghĩa quý vị đừng nên sử dụng các thiết bị này cho mọi chuyện quý vị thích, quý vị chỉ cần làm thêm hay thay đổi vài bước, để có thể bảo vệ tin tức riêng tư và trữ liệu của quý vị.

Bảo vệ máy cho an toàn: vì dễ cầm theo nên các máy di động cũng dễ mất hay bị trộm nhiều nhất so với máy điện toán để bàn. Ngoài chuyện để ý giữ máy di động, quý vị có thể tận dụng tất cả các công cụ được thiết kế đặc biệt cho máy để giúp quý vị giữ máy và bảo vệ trữ liệu được an toàn.

Bắt đầu khóa máy lại bằng một mật mã (hay dấu vân tay của ngón cái, tùy theo đời máy). Mặc định máy ở chế độ tự động tắt sau vài phút. Cùng một lúc, ghi tên vào chương trình tìm địa điểm/khóa/xóa như "Find My iPhone" (Tìm iPhone của tôi) (Apple) hay Android Device Manager (Quản Lý Thiết Bị của Android). Nó cho quý vị kiếm máy nếu quý vị làm rớt ở đâu, hay tự động khóa máy hay xóa dữ liệu của quý vị nếu máy bị cướp mất.

Đừng quên "xóa sạch" các trữ liệu trước khi quý vị bán, cho hay vứt máy đi để không ai có thể vào được các tin tức cá nhân của quý vị. CTIA-The Wireless Association là hiệp hội cung cấp các hướng dẫn và các đường truyền hướng dẫn cách xóa các tin tức cho từng loại máy di động cá biệt (*bit.ly/1jeEDZN*).

Để biết thêm về cách bảo vệ điện thoại của quý vị cho an toàn, xin vào AARP (*bit.ly/1FfksoF*).

Ứng dụng (Apps): "Apps" là các ứng dụng phần mềm ("software") được thiết kế đặc biệt cho các máy di động. Nhiều hoạt động của điện thoại thông minh hay phiến bản rờ là từ tải xuống các "apps"--giúp quý vị theo dõi sâu xát việc tập luyện cơ thể, chia sẻ hình "tự chụp," báo cho bạn bè biết quý vị đang ăn tối ở đâu, theo dõi tình hình đầu tư, chơi "Words With Friends" (chơi chữ với bạn) và nhiều thứ khác. Nên biết chắc "software" đầy quyền lực này làm việc cho quý vị, không hại quý vị.

◆ Chọn lọc "apps." Chỉ tải xuống apps (ứng dụng) nào từ nguồn cung cấp đáng tin cậy. Đọc các bình phẩm của người dùng và biết chắc nó từ công ty kiến tạo có uy tín trước khi tải xuống.

◆ Chỉnh apps cho phù hợp với mức riêng tư quý vị muốn. Nhiều apps dựa vào khả năng truy cập và chia sẻ tin tức cá nhân của người dùng, như liên lạc, lịch và ngay cả địa điểm. Để kiểm soát một apps thâu thập và chia sẻ tin tức, quý vị kiểm tra tại mục "settings" (điều chỉnh) của app (khác với phần "settings" trong máy). Nếu app muốn thâu thập nhiều trữ liệu cá nhân nhiều hơn quý vị muốn, đừng tải nó xuống. Duyệt qua nội quy của app về sự riêng tư, nếu có. Nếu app không có, quý vị nên nghĩ đến chọn một app khác.

◆ Tránh loại apps nào tuyên bố cho mọi người biết quý vị đang ở đâu, hay tắt tính năng này đi nếu có. Quý vị chia sẻ đang ở đâu với người lạ có thể đặt quý vị trong nguy cơ bị trộm vào nhà hay sự an toàn và riêng tư của quý vị có thể bị nguy hiểm. (Một số apps như các apps cung ứng bản đồ và đường đi, dùng nơi quý vị đang có mặt để cung ứng dịch vụ nhưng nó không tiết lộ ra chốn công cộng.)

◆ Cập nhật "software" (chương trình vi tính) mới nhất có sẵn để biết chắc quý vị luôn có phiên bản mới nhất của các apps đã có.

◆ Đọc thông báo khi có sự thay đổi về sử dụng apps hay nội quy về sự riêng tư để quý vị có thể tháo app ra nếu nó định thâu thập hay chia sẻ nhiều trữ liệu của quý vị hơn là quý vị muốn. Tùy theo loại app và sự thay đổi đáng kể ra sao, quý vị có thể nhận được thông báo trực tiếp (thường qua email hay từ trong app, gọi là "push notification"). Trong trường hợp khác, chỉ có một cách để biết về các thay đổi là đọc lại các điều lệ trong app hay tại trang mạng của nó.

Mạng xã hội an toàn và bảo đảm

Đối với nhiều người, dùng mạng xã hội là một phần trong sinh hoạt thường nhật của họ. Chia sẻ có thể là điều tốt—nếu quý vị tiết lộ những gì quý vị muốn với thành phần khán giả quý vị chọn. Để tránh mầm mống chia sẻ quá lố, quý vị nên nghĩ đi nghĩ lại trước khi chia sẻ, "tweet" (nhắn tin) hay tiết lộ tin tức cá nhân, và nên dùng các công cụ cho sẵn để kiểm soát người nào được xem. **Phòng vệ tin tức riêng tư của quý vị:** Không phải ai cũng có ý tốt khi sử dụng mạng xã hội. Điều quan trọng quý vị nên sáng suốt chọn chia sẻ điều gì và với ai để các trữ liệu cá nhân của quý vị không bị dùng sai lạc.

Bắt đầu bằng cách điều chỉnh chế độ bảo vệ tin tức riêng tư trên mạng xã hội ở mục "settings" (điều chỉnh) để tương xứng với mức độ thoải mái của quý vị--từ không chia sẻ với ai đến chỉ chia sẻ trong một nhóm bạn hoặc chia sẻ ở chốn công cộng. Trước tiên, đăng nhập (log on) vào trương mục của quý vị, sau đó tìm nút nhấn hay tựa đề như "Privacy" (riêng tư), "Privacy Controls" (Kiểm soát Riêng Tư), "Account Settings" (Điều Chỉnh Trương mục), hay "Preferences" (Tham Chiếu). Nếu không kiếm ra, quý vị vào phần "Giúp Đỡ ("Help")," hay email cho đội Hỗ Trợ của trang mạng.

Đừng chia sẻ các tin tức cá nhân, thí dụ, tên họ, địa chỉ, số điện thoại, họ mẹ bên ngoại, ngày tháng năm sinh, nó có thể bị dùng cho mục đích mạo nhận danh tánh (và giả mạo ID). Và đừng chia sẻ tin tức quý vị đang ở đâu và các chương trình đi du lịch, vì tính mạng và tài sản của quý vị có thể bị nguy hiểm.

Nên theo quy định tốt là không nhận người nào yêu cầu muốn làm "friend," (bạn) nếu quý vị không biết người đó.

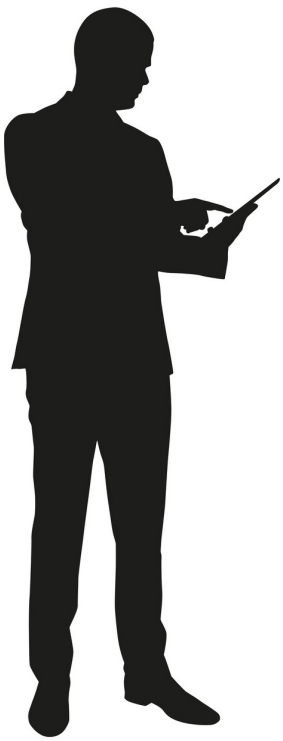
Muốn biết thêm, nên đọc ấn bản Consumer Action's publication Privacy and Control for Social Media Users (*bit.ly/1xPC8PO*).

Bảo vệ e-thanh danh của quý vị: Những thứ quý vị chia sẻ--hình ảnh, videos, sinh hoạt, ý kiến--tiết lộ về quý vị. Quản lý và bảo vệ uy tín của quý vị trong xã hội điện số có thể cứu quý vị không bị xấu hổ và giúp tránh bị các hậu quả không tốt. Đây là một số "thực hành tốt" để bảo vệ quý vị không bị hớ hênh trong mạng xã hội

◆ Nên nghĩ đến cảnh chủ nhân, nhân viên tuyển dụng, viên chức tuyển lựa sinh viên đại học, chủ nợ, chủ thuê nhà, khách hàng/thân chủ, cơ quan nhà nước, hãng bảo hiểm hay người có thẩm quyền sẽ nghĩ sao về quý vị, khi họ nhìn thấy những gì quý vị chia sẻ. Nên ý thức rằng có nhiều người không biết gì về cá nhân quý vị, có thể lên mạng xã hội để tìm hiểu về quý vị.

◆ Nên ý thức rằng một "friend" (bạn) có thể đăng lại, chuyển lại tin nhắn hay phô bày những gì quý vị cứ tưởng nó chỉ được chia sẻ trong số khán giả chọn lọc. Và nếu quý vị đăng trên tường của người khác, quý vị không kiểm soát được những ai sẽ đọc được.

◆ Sửa lại nếu cần thiết. Một số mạng xã hội có chức năng cho quý vị xoá tin đăng, bỏ hình xuống, thay đổi khán giả, v.v.. vì thế những gì quý vị chia sẻ trong quá khứ không còn thấy nữa cho những người sau này. (Dĩ nhiên, quý vị không thể làm gì khác hơn với những người đã đọc được các tin quý vị đăng.)



◆ Sử dụng "Google" đánh tên quý vị vào để xem nó có hiện lên không. Yêu cầu người khác xoá đi các hình ảnh hay video không hay ho gì mà có quý vị trong đó.

◆ Nên biết chắc trương mục của quý vị an toàn để tin tặc không xâm nhập vào được nhằm đánh phá quý vị.

Muốn biết thêm về cách quản lý thanh danh của quý vị trên mạng, xin xem Google's Safety Center (*bit.ly/1FunANi*).

Mạng Điện Toán Thân Thiện Với Gia Đình

Mạng điện toán cung cấp nội dung với phẩm chất phong phú không chỉ cho người lớn, nhưng còn cho trẻ em đủ mọi lứa tuổi. Tuy nhiên, nó cũng có một số nội dung không phù hợp. Để bảo đảm quý vị và gia đình tránh gặp các chuyện không hay khi đang hưởng những gì tốt nhất do Mạng điện toán cung cấp, có các cách bảo vệ và cảnh báo để quý vị có thể sử dụng.

Chặn nội dung không phù hợp: Có rất nhiều nội dung đặc sắc, phù hợp cho từng lứa tuổi của

trẻ em. Nhưng cũng có một số nội dung không phù hợp. Nhiều công ty - từ dịch vụ "broadband" tới mạng xã hội- là nhịp cầu phổ biến các nội dung- có cung cấp tính năng giúp phụ huynh giới hạn mọi thứ, từ số lượng giờ được lên mạng cho đến trang mạng nào được viếng, videos nào có thể xem, và tường nhắn tin và phòng "chat" nào được vào.

Để biết thêm về các tính năng cho phụ huynh quyền kiểm soát, xin viếng trang Family Online Safety Institute (*bit.ly/1L63Emf*) và Google Safety Center (*bit.ly/1G2F7XP*).

Dòm chừng sâu xát các giao tiếp: Không phải chỉ dòm chừng các nội dung không phù hợp cho trẻ em là xong, vì không phải người nào vào mạng xã hội cũng đều nghĩ đến sự an sinh của trẻ em. Là phụ huynh, quý vị là người gác cửa cho mối quan hệ giữa con em của quý vị với mạng điện toán.

Nói chuyện với con em của quý vị về sự an toàn và trách nhiệm khi lên mạng điện toán. Đặt luật lệ rõ ràng về trang nào con em có thể viếng và ai nó có thể giao tiếp được. Nên gia nhập vào "Friend" của con em quý vị--nên biết chắc quý vị có thể nhìn thấy nó chia sẻ cái gì trên mạng xã hội, và người khác chia sẻ cái gì với tụi nó. Nên khẳng định rõ cho con em của quý vị rằng nó không được tự ý đi một mình gặp mặt người nào nó "quen" trên mạng xã hội. Quý vị hứa sẽ không phạt hay không cho nó lên mạng nữa nếu nó nói cho quý vị biết các mối liên lạc không phù hợp của nó trên mạng. Nên tìm đọc các hướng dẫn tại OnGuardOnline.gov (*http://bit.ly/2eewlAl*).

Báo cáo các hành vi xách nhiễu và cạm bẫy cho cơ quan thẩm quyền, bao gồm ban giảng huấn nhà trường, cảnh sát địa phương hay CyberTipline (*bit.ly/1NMiQDY* hay gọi số 800-843-5678).

Tránh bị quảng cáo phiền nhiễu: Nhiều công ty quảng cáo thâu thập tin tức cá nhân của người dùng mạng điện toán. Một số công ty dùng trữ liệu để chọn lựa cho phù hợp và phong phú thêm kinh nghiệm của người dùng --đề nghị các cuốn phim và sách quý vị có thể thích--trong khi một số khác dùng trữ liệu để làm các quảng cáo đặc biệt thu hút những người có cùng sở thích. Còn một số khác--là thành phần môi giới trữ liệu—thâu thập trữ liệu về người tiêu thụ để bán cho các hãng quảng cáo trung gian và các công ty khác dùng các trữ liệu này để nhắm vào lời rao quảng cáo và dịch vụ. Các công ty uy tín thường minh bạch về cách thức họ dùng tin tức của quý vị, và họ cho quý vị lựa chọn về tin tức cá nhân nào của quý vị họ được chia sẻ và cái nào quý vị muốn giữ kín.

Quý vị có thể làm các bước sau để hiểu tin tức về quý vị sẽ được dùng ra sao và cách quý vị có thể gia tăng sự kiểm soát các trữ liệu của quý vị.

◆ Đọc "Nội Quy về Sự Riêng Tư" của công ty hay "Nội Quy về Sử Dụng Trữ Liệu" để biết cách nào và khi nào trang mạng thâu thập, sử dụng và chia sẻ tin tức cá nhân của quý vị. Nếu quý vị không hài lòng với việc làm này của công ty, nên tìm trang mạng nào cho quý vị nhiều kiểm soát hơn.

◆ Nếu quý vị có con nhỏ, dạy cho tụi nó đừng tiết lộ các tin tức cá nhân trên trang mạng tụi nó viếng. Sắc Luật Bảo Vệ Tin Tức Cá Nhân của Trẻ Em Trên Mạng Điện Toán (COPPA - Children's Online Privacy Protection Act) buộc các trang mạng phải có sự cho phép của phụ huynh mới được thâu thập hay dùng bất kỳ tin tức cá nhân nào của trẻ em dưới 13 tuổi. Nên báo cáo các sự vi phạm đến Nha Thanh Tra Mậu Dịch Liên Bang (FTC - Federal Trade Commission) (*www.ftccomplaintassistant.gov* hay gọi số 877-FTC-HELP).

◆ Nếu phù hợp, bật chức năng "Private browsing" (trang chủ riêng tư) trong trang chủ của quý vị, nó cho quý vị lướt qua Trang Mạng nhưng không lưu lại tin tức về mạng hay trang nào quý vị đã viếng, và dùng "pop-up blocker" (chặn quảng cáo đột ngột hiện ra) để tránh mở các cửa sổ quảng cáo không muốn (Nên để ý chức năng này có thể cản trở một số hoạt động cần thiết, như trang mạng bán hàng lẻ nhớ trong "xe đẩy" hay "túi mua sắm" của quý vị có cái gì trong đó.

◆ Cân nhắc có nên cho thêm tin tức cá nhân nào khác, ngoài các tin tức tối thiểu bắt buộc phải cho (thường ám chỉ bằng dấu hoa thị) để ghi danh hay để sử dụng dịch vụ. Chia sẻ tin tức cá nhân càng ít càng tốt nếu được.

◆ Nên hiểu rằng bất cứ khi nào quý vị tự ý đưa tin tức cá nhân của quý vị cho một nguồn không chính đáng--ngay cả khi trả lời các câu hỏi vô thưởng vô phạt trong một cuộc thi ngắn hoặc tham gia vào các trò chơi--nó có thể bị sử dụng cho các mục đích không chủ tâm.

Kỹ thuật không ngừng cho chúng ta các cách thức mới để giao tiếp, làm việc, học hỏi, sáng tạo, chia sẻ và giải trí. Đừng bỏ sót cái gì--nhưng phải cẩn thận. Quý vị nên sát cánh cùng với đội ngũ cố gắng bảo vệ thật an toàn cho chính quý vị và gia đình khi lên mạng. ■

Giới Thiệu Về Consumer Action

www.consumer-action.org

Qua các tài liệu hướng dẫn, tiếp cận với cộng đồng và lên tiếng bênh vực cho người tiêu thụ về các đề tài cụ thể bằng nhiều thứ tiếng, Consumer Action (Cơ Quan Tác Động Giới Tiêu Thụ) hỗ trợ cho người tiêu thụ thấp cổ bé họng toàn quốc tự tin vào quyền của họ trong thị trường và gầy dựng tài chánh thịnh vượng.

Consumer Action Cố Vấn và Trợ Giúp: Người tiêu thụ hãy gởi khiếu nại đến đường dây khẩn của chuyên viên cố vấn và giới thiệu: *http://www.consumer-action.org/hotline/complaint_form* hay gọi số 415-777-9635.

Chúng tôi có nói tiếng Trung Hoa, Anh, và Tây Ban Nha

Ấn bản này được biên soạn với sự hợp tác của Google