Ấn Bản Của Consumer Action

Đừng nên "Like" cái gì?

Bảo vệ tin tức riêng tư của quý vị trên mạng xã hội

YouTube, Instagram, Facebook, Twiter và các mạng xã hội khác được người tiêu thụ thích "kết nối" đều biết đến ngay. Thực ra, nhiều người lớn và giới trẻ thích vào mạng xã hội vì đó là thú vui của họ.

Chia sẻ thông tin có thể vui thú và bổ ích, nhưng nó cũng có thể mang hậu quả nếu quý vị không cẩn thận về những gì quý vị tiết lộ và với ai. Rất may là bây giờ có nhiều cách để người vào mạng xã hội giới hạn những gì họ muốn chia sẻ và bảo vệ tin tức riêng tư của họ. Nếu quý vị cảnh giác và chủ động, quý vị có thể vui thú khi vào mạng nhưng vẫn bảo vệ tin tức riêng tư.

Tầm Quan Trọng Của Sự Riêng Tư

Người ta chia sẻ nhiều chuyện khác nhau trên mạng xã hội. Thí dụ như video các con thú kiểng của quý vị đang làm cái gì ngớ ngẩn - có thể được chia sẻ với cả thế giới mà không đem lại hậu quả xấu nào. Một mặt khác, tuyên bố quý vị trúng số, có thể nguy hiểm. Bước đầu tiên tự bảo vệ mình là quý vị có thể nhận thức được sự khác biệt. Thử nhận ra các nguy cơ trong các thông tin đã được chia sẻ công khai trên mạng xã hội sau đây:

Xuân ở San Francisco, nhắn tin trên twitter từ Hawaii rằng cô ấy đang tận hưởng các giây phút vui vẻ nhất trong tuần nghỉ hè. (Khi Xuân về lại nhà, cô phát giác ra đã có người nào đó đột nhập vào căn nhà chung cư của cô).

Dũng, ông đang hy vọng được lên chức, đã đăng tin than phiền về công ty của ông "Công ty tôi đang làm đối xử với nhân viên như nô lệ!" (Giám Đốc của Dũng đọc được qua trang facebook của đồng nghiệp – không chắc ông Dũng được lên chức trong tương lai.)

Anh Rô thích nhận được tin nhắn chúc mừng sinh nhật, nên anh đã đăng ngày và tháng anh sinh ra trong phần tiểu sử của anh, cùng với năm anh tốt nghiệp trung học (Học kỳ "82"). Rô là nạn nhân của vụ trộm danh tính cá nhân. Một người nào đó có khả năng tìm ra hết ngày tháng năm sanh cùng với tên họ của anh cũng như các chi tiết thâu thập khác qua các tin tức anh đăng, kẻ trộm đã dùng nó để vào được một trong các trương mục của anh.)

Duyên, 17 tuổi, học sinh trung học lớp 12 vừa mới gởi đơn xin học đại học, cô đăng trên "instagram" hình cô ta đang uống beer tại một party của người bạn. (Các trường Duyên mong muốn được nhận nhất kiểm tra sinh hoạt của người nộp đơn trên mạng xã hội và sẽ từ chối nhận các sinh viên nào có các hành vi hồ nghi như uống rượu khi chưa đủ tuổi.)

Chia sẻ hình ảnh, video để giữ liên lạc với bạn bè và gia đình hay cổ động các sáng kiến hoặc dự án không có gì là sai trái cả, nhưng quý vị trước tiên nên để ý bất kỳ tin tức chia sẻ nào được tiết lộ và sẽ được sử dụng ra sao – nhất là khi nó bị người lạ đọc được.

Chọn người đọc

Khi quý vị mở một trương mục trên mạng xã hội, quý vị thường có các lựa chọn để đổi thành phần người đọc đã chọn trước đó (định vị). Trong một số trường hợp, quý vị cũng có thể điều chỉnh chế độ định vị cho từng đề mục quý vị đăng hay chia sẻ. Trước khi bắt đầu chia sẻ, quý vị nên học về các lựa chọn cụ thể để bảo vệ tin tức riêng tư trên mạng xã hội và điều chỉnh khi cần.

Các định vị này có thể hữu hiệu, nhưng quý vị đừng có ảo tưởng là nó an toàn. Quý vị giới hạn người xem, không có nghĩa người khác không đọc được những gì quý vị chia sẻ. Thí dụ, quý vị không kiểm soát được ai nhìn thấy các bài quý vị đăng vào trang chủ của người khác, và quý vị không thể ngăn người khác sao chép lại và tung ra những gì quý vị đã chia sẻ với họ. Hình ảnh, trương mục của trang chủ và nội dung trang chủ của quý vị cũng có thể dễ dàng tìm thấy bằng cách tìm tên của quý vị trên hệ thống dò tìm (browser).

Vì lý do này, quý vị nên thận trọng nhiều hơn. Trước khi chia sẻ điều gì, nên nghĩ mọi người đều có thể đọc được bây giờ hay trong tương lai – sở làm, thân chủ, đồng nghiệp, giáo viên, cơ quan chính quyền, chủ thuê, hãng bảo hiểm, ông bà.

Cho dù quý vị đã cẩn thận giới hạn người đọc, nhưng ***đừng bao giờ*** chia sẻ các điều này:

- Số an sinh xã hội
- Họ mẹ, sinh nhật (tháng, ngày và năm) hay các chi tiết khác để chứng minh danh tánh cá nhân
- Địa chỉ cá nhân hay số điện thoại
- Quý vị hiện đang ở đâu (giờ xác thực hay các chi tiết nào có thể tìm ra quý vị)
- Các chi tiết nào tiết lộ nhà của quý vị bỏ trống hay quý vị và con em của quý vị ở nhà một mình

Các điều nên làm và đừng làm để bảo vệ sự riêng tư

Có các phương cách khác quan trọng hơn – ngoài cách giới hạn người đọc – để tự bảo vệ tin tức riêng tư của quý vị khi vào mạng xã hội.

Đây là 16 điều nên làm và không nên làm rất hữu ích:

Đừng cảm thấy quý vị phải điền từng đề mục khi tạo tiểu sử của quý vị – tất cả đều là tùy ý.

Đừng đồng ý hay nhận lời mời kết bạn từ những người quý vị không biết để tăng số lượng "bạn" hay "người theo dõi." Và đừng trả lời các tin nhắn từ người lạ.

Đừng đăng các chi tiết hay hình ảnh – xe thể thao mới của quý vị, nội thất trong nhà, v.v... – hay chia sẻ các hoạch định đi du ngoạn khiến các nghệ sĩ lừa đảo và kẻ trộm để ý.

Đừng giải đáp các cuộc thi ngắn, trò chơi, phiếu tặng hay các trò dụ dỗ đòi hỏi quý vị phải tiết lộ tin tức cá nhân. Nó chỉ mở đường cho các dịch vụ quảng cáo rác rưởi tràn vào và ngay cả lừa đảo.

Cá nhân hóa các thiết lập riêng tư của quí vị

Vào trương mục của quý vị và tìm đề mục "Privacy, Setting hay Preferences," hay dùng mục "Help" để tìm và hiểu các tính năng cũng như các công cụ của trang mạng. Nếu quý vị vẫn cần giúp đỡ, liên lạc với nhân viên hỗ trợ của của trang mạng qua đường "link" của trang mạng hay app, đặt câu hỏi trong khu "Cộng đồng" (Community) hay "Diễn Đàn" (forum), hoặc tìm trên mạng câu hỏi của quý vị (thí dụ: "Làm thế nào để tôi dùng chế độ định vị bảo vệ sự riêng tư trong [tên của trang mạng xã hội]?"

Từ đó, quý vị có thể điều chỉnh chế độ định vị để giới hạn ai có thể xem được trang chủ của quý vị, liên lạc, hay đọc được những gì quý vị chia sẻ. Nếu cần, tận dụng các lựa chọn thay đổi thành phần độc giả cho mỗi đề mục cá nhân quý vị chia sẻ, và "chặn" hay "hủy kết bạn" (unfriend) người nào để kiểm soát sự tiếp cận của quý vị. (Nên cảnh giác cho dù quý vị có lựa chọn trở lại và thay đổi thành phần độc giả của các tin đã đăng hay xoá hoàn toàn, nó có thể quá trễ để giữ tin tức riêng tư.)

Nếu còn đắn đo, đừng chia sẻ!

Đừng nhấn vào các đường "links" lạ, vì nó có thể được thiết kế để làm hư máy điện toán của quý vị bằng virus hay nhu liệu trộm trữ liệu của quý vị.

Nên định vị máy điện toán và thiết bị di động của quý vị phải có mật mã hay PIN mới mở lên hay khởi động được.

Nên chọn một mật mã khó đoán cho trương mục (trộn lẫn tối thiểu 8 con số, mẫu tự và dấu hiệu) và đổi nó thường xuyên. Đừng dùng cùng một mật mã cho tất cả trương mục của quý vị, hay dùng tên thú kiểng hoặc tên con em của quý vị nếu quý vị chia sẻ các chi tiết này trên mạng xã hội. Khi được hỏi chọn các câu hỏi bảo vệ sự an toàn, quý vị nên chọn câu nào không ai biết câu trả lời.

Nên biết chắc đã đi ra (log out) nếu quý vị dùng máy điện toán công cộng để vào trương mục của quý vị. "Log out" luôn sau khi dùng máy ở nhà cho dù đó là máy và thiết bị riêng của quý vị.

Đừng để hệ thống dò tìm (browser) lưu trữ thông tin vô mạng (log in) nếu nó nổi lên các lựa chọn, hay check/uncheck các ô phù hợp trong phần "Security, Passwords, Sync hay AutoFill" của mục "setting" (định vị) hay "preferences" của hệ thống dò tìm.

Nên tiếp nhận và cập nhật nhu liệu bảo vệ (mật hoá, tường lửa, chương trình chống virus/spyware).

Nên xem qua các điều lệ về tin tức riêng tư của công ty trước khi mở một trương mục để biết các tin tức cá nhân và/hay trữ liệu của quý vị trong hệ thống được công ty dùng ra sao.

Đừng tải xuống một "apps" (ứng dụng) trừ khi nó từ nguồn tin cậy và quý vị đã coi qua các phê bình của người sử dụng và đọc điều lệ về tin tức riêng tư.

Nên đọc tất cả các thông báo của công ty mạng xã hội và apps để quý vị không bỏ sót các thay đổi về điều lệ

Điều khiển apps của quý vị

Nói chung, apps – nhu liệu tải xuống được để thăng tiến chức năng của điện thoại di động hay máy tính bảng của quý vị – nó có thể vào trong các tin tức trong máy của quý vị, bao gồm địa chỉ liên lạc và tin nhắn. Một số apps, nhưng không phải tất cả, sẽ xin phép quý vị trước khi nó vào các tin tức này và/hay cho biết quý vị đang ở đâu.

Để quản lý chế độ định vị (setting) cho apps, quý vị tìm Apps, Trữ liệu chia sẻ (Data Sharing) hay đại loại giống vậy trong mục "Preferences, Setting, hay Help" của trang mạng xã hội. Sau đó điều chỉnh chế độ định vị phù hợp với sự thoải mái của quý vị. Để kiểm soát apps thâu thập và chia sẻ ra ngoài mạng xã hội cái gì, kiểm tra phần "setting" của chính app đó. Đọc phần điều lệ của apps về tin tức riêng tư và trữ liệu sử dụng, và sau đó quý vị quyết định có thoải mái với các điều lệ này hay muốn tháo nó ra và tìm một app khác.

nào. Nếu quý vị không hài lòng với sự thay đổi, hủy trương mục và/hay gỡ app ra.

Đừng cho apps tuyên bố quý vị đang ở đâu.

Nên nói chuyện với con em của quý vị về làm sao để được an toàn và trách nhiệm khi lên mạng điện toán (bao gồm cảnh báo về "nhắn tin tình dục"), và dùng mật mã khó đoán cho trương mục của tụi nó, tận dụng chương trình "phụ huynh kiểm soát" để kiểm tra định kỳ các cuộc trò truyện của con em trên mạng điện toán.

Nên tuân hành các quy định của sở làm về mạng xã hội, nếu có.

Giới Thiệu Về Consumer Action

www.consumer-action.org

Qua các tài liệu hướng dẫn người tiêu thụ bằng nhiều ngôn ngữ khác nhau, qua tiếp cận với cộng đồng và tập trung vào vấn đề cụ thể để lên tiếng bênh vực cho người tiêu thụ, Consumer Action (Cơ Quan Tác Động Giới Tiêu Thụ) tiếp sức cho những người tiêu thụ thấp cổ bé họng trên toàn quốc vững tin vào các quyền của họ và tài chánh thịnh vượng.

Trợ giúp và cố vấn cho người tiêu thụ: Xin gởi các khiếu nại của người tiêu thụ đến: *https://complaints.consumer-action.org/forms/english-form* hay gọi 415-777-9635 (chúng tôi có nói tiếng Hoa, Anh và Tây Ban Nha).

Nguồn giúp đỡ

Xin xem các đường links này để biết thêm về cách bảo vệ tin tức riêng tư của quý vị và giữ an toàn khi vào mạng điện toán:

StaySafeOnline.com [*https://www.staysafeonline.org*]

Privacy Rights Clearinghouse (bảo vệ riêng tư trên mạng xã hội) [*https://www.privacyrights.org/social-networking-privacy-how-be-safe-secure-and-social*]

Google Safety Center [*https://www.google.com/safetycenter/*]

Online Safety Institute (dạy con cách hay để lên mạng cho an toàn) [*https://www.fosi.org/good-digital-parenting/*]

OnGuardOnline.gov (bảo vệ trẻ em chơi trên mạng) [*http://www.onguardonline.gov/topics/protecting-kids-online*]

Common Sense Media (bổn phận của mạng xã hội với giới trẻ) [*http://www.commonsensemedia.org/blog/talking-about-sexting*]

TrustArc (các chỉ dẫn về bảo vệ tin tức riêng tư) [*https://www.trustarc.com/blog/2011/04/27/5-privacy-tips-for-mobile-app-users/*]

Cách đọc điều lệ về tin tức riêng tư trên mạng điện toán [*http://oag.ca.gov/privacy/facts/online-privacy/privacy-policy*]

CNET (bảo vệ uy tín của quý vị trên mạng điện toán) [*http://www.cnet.com/how-to/how-to-manage-your-online-reputation-for-free/*]

CTIA-The Wireless Association (giữ an toàn trong thiết bị di động) [*https://www.ctia.org/consumer-resources/protecting-your-data*]

AARP (bảo vệ điện thoại khỏi bị trộm trên mạng điện toán) [*http://www.aarp.org/home-family/personal-technology/info-2014/cyberproof-stolen-phone-kirchheimer.html*]

Federal Trade Commission (FTC) (dùng mạng Wi-Fi miễn phí an toàn) [*http://www.consumer.ftc.gov/articles/0014-tips-using-public-wi-fi-networks#Mobile*]

Apple (Mac) [*http://www.apple.com/support/osx/passwords/*] or PC [*http://pcsupport.about.com/od/tipstricks/ht/newxppassword.htm*] (cách định vị máy phải đánh mật mã hay số PIN khi mở hay khởi động máy)

ConnectSafely (tạo một mật mã khó đoán) [*http://www.connectsafely.org/tips-to-create-and-manage-strong-passwords/*]

PasswordsGenerator.net [*http://www.passwordsgenerator.net*]

PCMag.com (mật mã miễn phí "tốt nhất) [*http://www.pcmag.com/article2/0,2817,2475964,00.asp*]

Giới Thiệu về ấn bản này

Cơ quan Consumer Action đã biên soạn ra tập cẩm nang hướng dẫn này với sự tài trợ của Rose Foundation.

© Consumer Action 2016