

NHỮNG HIỂM HỌA MỚI

Khi bạn đã biết cách đề phòng những hiểm họa thường thấy như phần mềm gián điệp và web giả mạo, thì dữ liệu của bạn lại có cơ rò rỉ thông qua những công ty hợp pháp. Định vị GPS, gọi điện di động, tìm kiếm trên web, mọi thứ đều là những công cụ thuận tiện.

Khi bạn đã biết cách đề phòng những hiểm họa thường thấy như phần mềm gián điệp và web giả mạo, thì dữ liệu của bạn lại có cơ rò rỉ thông qua những công ty hợp pháp. Định vị GPS, gọi điện di động, tìm kiếm trên web, mọi thứ đều là những công cụ thuận tiện. Bạn dùng chúng để tìm đường, trò chuyện cùng bạn bè, tìm trang web và chẳng bao giờ lưu tâm đến giao dịch dữ liệu đó. Theo các chuyên gia bảo mật, những việc như thế còn nảy sinh một vấn đề mới: chúng để lại "dấu vết số" khá chi tiết về việc bạn đi đâu, nói chuyện với ai, thậm chí cả việc bạn nghĩ gì. Những dấu vết này có thể tồn tại hàng thập kỷ và chẳng có luật lệ nào bảo vệ loại dữ liệu như vậy. Khi nào dấu vết số của bạn còn tồn tại thì dữ liệu có thể bị bán sạch, hoặc có thể bị tin tặc, đối thủ cạnh tranh... "viếng thăm". Tất cả những dấu vết cá nhân này của chúng ta đang ngày một nhiều và một số trường hợp gần đây cho thấy chúng có thể dễ dàng bị "soi mói". Vượt qua giới hạn Thiết bị GPS có thể là trợ thủ tốt để giúp bạn tìm đường, tiết kiệm thời gian và nhiều việc khác. Có một vụ việc gần đây được lôi ra tòa cho thấy những chi tiết cá nhân dày đặc về vị trí địa lý và cách lái xe của bạn có thể bị thu thập và tận dụng để chống lại bạn. Tại bang Connecticut, Mỹ, công ty cho thuê xe American Car Rental đã cài thiết bị GPS vào xe hơi của họ để theo dõi tốc độ và vị trí người thuê. Các thiết bị này báo cáo không dây về trụ sở mỗi khi khách hàng lái xe nhanh hơn 127km/h liên tục từ 2 phút trở lên để phạt tiền. American Car Rental bị kiện và tòa phán quyết công ty không được lấy thêm tiền chạy xe quá tốc độ của khách, nhưng tòa lại không cấm công ty sử dụng thiết bị GPS để theo dõi tốc độ và vị trí của khách hàng. Rắc rối về luật Vì chưa có luật nào quy định về vấn đề này, chỉ rõ cho doanh nghiệp (hay cơ quan nhà nước) có thể làm gì với dữ liệu của bạn. Theo một chuyên gia thì một công ty có thể bị 7 hay 8 loại luật về bảo vệ tính riêng tư người dùng ràng buộc. Nhiều năm nay, các nhà làm luật cố gắng đưa ra một chuẩn thống nhất chung nhưng vẫn chưa có kết quả. Hãy xem xét tính riêng tư cá nhân giống như việc bạn xem TV. Các công ty cáp phải tuân theo luật hiện hành, luật quy định rạch ròi: họ được và không được làm gì về thói quen xem TV của người xem. Ví dụ, họ bị cấm chia sẻ thông tin của người xem với các công ty thứ 3. Nhưng những đầu thu video số như TiVo lại nằm ngoài "vùng phủ sóng" của bộ luật này. Thật ra TiVo cũng có chính sách bảo mật tính riêng tư khá gắt gao, tuy vậy chính sách này xuất phát từ động cơ kinh doanh nên có thể thay đổi bất cứ lúc nào. Theo một chuyên gia về bảo mật, khó khăn hiện nay đối với người dùng là những sản phẩm hoặc dịch vụ có thể có nhiều chính sách bảo mật thông tin cá nhân khác nhau và không phải ai cũng biết tỏ tường mọi chính sách như thế. Tìm và bắt Người dùng quan tâm đến bảo mật cá nhân cũng nên biết tường tận một công ty thực sự làm được gì với thông tin của họ. Ví dụ như công ty đó có thể biết được thói quen tìm kiếm trên internet của bạn. Một khi bạn có được các kết quả tìm kiếm thì bạn thường quên chuyện tìm kiếm đó và tiếp tục công việc. Nhưng các công ty tìm kiếm thì không quên. Họ lưu lại những dữ liệu tìm kiếm, thường đi kèm với một định danh chỉ ra ai thực hiện việc tìm kiếm đó; mức độ bảo mật dữ liệu này khác nhau tùy thuộc vào dịch vụ tìm kiếm. Theo một chuyên gia, điều quan trọng là dữ liệu cá nhân được các công ty giữ lại trong bao lâu, mục đích sử dụng là gì và các công ty sẽ làm gì nếu cảnh sát "gõ cửa" văn phòng họ? Đã xảy ra một trường hợp: bộ tư pháp Mỹ gần đây đã tìm thấy một lượng thông tin khổng lồ từ chỉ mục tìm kiếm của Google và yêu cầu Google cung cấp các truy vấn tìm kiếm mà người dùng Google gõ vào. Google đã phản bác và

đã thành công. Tòa án phán quyết chính phủ có thể có danh sách một số địa chỉ trang web trong chỉ mục của Google, nhưng không được biết từ mà người dùng gõ vào để tìm kiếm. Chính phủ cũng sẽ không có được thông tin về ai gõ vào thông tin tìm kiếm đó. Google không "phơi ra" các chính sách lưu trữ dữ liệu của mình và hãng không trả lời những câu hỏi về các chính sách đó. Nhưng theo một chuyên gia thì dữ liệu quá 180 ngày có thể dễ bị yêu cầu "trưng ra" hơn những thông tin mới. Giống với Google, tìm kiếm của Yahoo dùng cookie với mã độc nhất; mỗi tìm kiếm được gắn với mã định danh đó. Mã này không liên kết đến dữ liệu cá nhân, như là tuổi hay vị trí của bạn nhưng nếu bạn tìm trong khi đã đăng nhập Yahoo thì lần tìm kiếm đó sẽ được gắn với hồ sơ Yahoo của bạn. Yahoo lưu trữ những chi tiết tìm kiếm này "lâu đến khi nào nó còn cần thiết", theo lời người phát ngôn của Yahoo. Tuy vậy, cũng theo người phát ngôn của Yahoo, hãng giữ các thông tin cá nhân chỉ cho riêng mình: thậm chí khi Yahoo làm việc với đối tác về các chiến dịch quảng cáo và khuyến mãi đặc biệt cho người dùng thì hãng cũng không bao giờ đưa dữ liệu người dùng cho đối tác. Tiết lộ điện thoại Thậm chí nếu một công ty không sẵn sàng chia sẻ thông tin cá nhân của bạn với đối tác thứ 3 thì bạn vẫn không an toàn. Hóa đơn chi tiết điện thoại của bạn rất dễ dàng lọt vào tay người ngoài. Họ có thể làm một chuyện đơn giản như gọi cho công ty cung cấp dịch vụ điện thoại, giả là một khách hàng, và họ sẽ có được một bản sao hóa đơn điện thoại của bạn, với đầy đủ danh sách cuộc gọi đến và gọi đi. Có một số trang web bán những danh sách như vậy. Một tin tốt lành là những trang web như thế đang dần bị "đóng cửa", nhưng dù sao đi nữa thì dữ liệu của bạn vẫn nằm đó và các chuyên gia nghi ngại là chúng sẽ được chuyển đến "thế giới ngầm".

BỐN CÁCH ĐỂ LẤY LẠI DỮ LIỆU CÁ NHÂN

Lấy lại thông tin cá nhân bằng cách nắm quyền điều khiển thông tin mà doanh nghiệp hay các tổ chức khác có thể truy cập. • Rút khỏi danh sách: các công ty có thể chia sẻ nhiều dữ liệu của bạn, trừ khi bạn cấm họ. Tổ chức Center for Democracy and Technology ở Mỹ đưa ra một dịch vụ miễn phí rất tuyệt tại địa chỉ opt-out.cdt.org, liên kết đến các loại mẫu đơn rút khỏi danh sách đăng ký cho nhiều loại hình dịch vụ. Cũng vậy, khi bạn đăng ký bất kỳ dịch vụ mới nào, hãy cẩn thận với các khuyến mãi đặc biệt và phải chắc chắn rằng bạn không tự động đăng nhập dịch vụ đó. • Bảo vệ danh sách cuộc gọi: liên lạc với nhà cung cấp dịch vụ và thiết lập một mã cho tài khoản của bạn. Bạn cũng có thể yêu cầu nhà cung cấp bỏ các chi tiết cuộc gọi ra khỏi hóa đơn để không cho ai dòm ngó (đương nhiên là bạn cũng không thể biết được thông tin này). Để kiểm tra liệu yêu cầu của bạn có được chấp nhận hay không, hỏi nhà cung cấp xem có ai truy cập vào tài khoản trực tuyến với tên của bạn hay không. • Đọc chính sách: đọc các chính sách về bảo mật cá nhân hay End-User License Agreements (EULAs) thường bị xem là chuyện mất nhiều thời gian. Ta biết đó là việc có ích, nhưng chúng ta thường không xem trọng chuyện này. Công cụ EULalyzer miễn phí của Javacool Software (find.pcworld.com/52876) giúp bạn việc này bằng cách kiểm tra chính sách hoặc EULA giúp bạn và tìm những từ khóa như "third party". Sau đó, công cụ này đánh giá những gì nó tìm được và báo cáo lại cho bạn những điểm nào nên chú ý. • Lướt web và tìm kiếm nặc danh: có một công cụ giúp bạn sẽ xóa định danh của bạn khỏi cookie của Google. Công cụ

này sẽ xóa mọi thiết lập Google của bạn, như mỗi trang hiển thị bao nhiêu kết quả tìm kiếm. Tại find.pcworld.com/52880 còn có nhiều tiện ích giúp bạn dấu đi định danh khi duyệt web.

PC World Mỹ 06/2006