Cẩn thận! Trong tháng rồi trên Internet và smartphone vừa có thêm những chiêu mới đánh cắp hoặc làm lộ dữ liệu cá nhân của người dùng.

5 mối đe dọa mới nhắm vào dữ liệu cá nhân

Những mối đe dọa cũ vẫn còn đó, giờ thêm những mối đe dọa mới. Các công ty như Google và Facebook vẫn theo dõi và thu thập dữ liệu cá nhân của bạn; tin tặc vẫn chực chờ đánh cắp dữ liệu của bạn. Và giờ, 5 xu hướng mới cho thấy sự an toàn thông tin và riêng tư của bạn có thể bị xâm phạm theo những cách không ai ngờ.

1. Dấu vân tay có thể bị đánh cắp từ ảnh chụp 'tự sướng'

Các nhà nghiên cứu tại Viện Tin học Quốc gia Nhật Bản (NII) vừa đưa ra khuyến cáo dấu vân tay có thể bị đánh cắp từ ảnh chụp và có thể sử dụng để đánh lừa hệ thống bảo mật vân tay.

Máy ảnh của smartphone ngày càng tốt với độ phân giải ảnh ngày càng cao, đường nét dấu vân tay của bạn trong ảnh giờ rõ mồn một và có thể sao chép dễ dàng. Đây là một mối đe dọa đặc biệt đối với nhiều người có thói quen giơ hai ngón tay hình chữ V trong các bức ảnh đăng trên mạng.

Không ít người hoài nghi. Trước hết vì "giải pháp" kỳ quặc mà các nhà nghiên cứu đưa ra: dùng một tấm phim trong có mẫu vân và bằng cách nào đó đặt lên ngón tay của bạn để che vân tay khi chụp ảnh.

Ngoài ra việc đánh cắp ảnh vân tay từ ảnh cần nhiều điều kiện như các ngón tay phải được lấy nét, ánh sáng hoàn hảo, khoảng cách từ máy ảnh khoảng dưới 3m và người chụp phải sử dụng smartphone thật cao cấp (nhưng smartphone cao cấp thường lấy nét khuôn mặt chứ không phải ngón tay).

Nhưng những người hoài nghi đã sai.

Đầu tiên, việc đánh cắp ảnh vân tay đã xảy ra. Hai năm trước, một người Đức tên Jan Krissler đã tái tạo dấu vân tay của Bộ trưởng Quốc phòng Đức Ursula von der Leyen từ các bức ảnh công bố công khai để mở khóa smartphone.

Thứ hai, công nghệ này đã tồn tại chứ không phải đang nghiên cứu.

Thứ ba, dấu vân tay là vĩnh viễn và không thể thay đổi như mật khẩu.

Thứ tư, máy ảnh smartphone ngày càng tốt. Vấn đề chỉ là thời gian, rồi mọi người sẽ luôn có bên mình máy ảnh tốt không thua gì máy ảnh của iPhone 7 hay Samsung Galaxy S7.

Và cuối cùng, tin tặc có thể sử dụng hình ảnh trên mạng làm "bàn đạp". Có cả trăm ngàn ảnh vân tay chất lượng cao trên Goolge Images.

2. Chính trị gia 'chơi' nhau bằng cách công bố thông tin cá nhân

Xu hướng mới nhất trong các cuộc đấu đá chính trị đó là tiết lộ thông tin cá nhân của ai đó trên mạng.

Một số thông tin, như số điện thoại hay địa chỉ nhà riêng, rất dễ tìm thấy trên mạng. Một người tìm được thông tin, và thế là cả trăm người khác 'ăn

theo tới tấp gọi điện thoại đe dọa, hay người ta cũng có thể gọi cảnh sát báo giả có một vụ hành hung đang diễn ra tại nhà của ai đó, khiến cảnh sát phải cử người đến.

Vấn đề này nghiêm trọng đến nỗi một số mạng xã hội gần đây phải xóa và cấm hẳn một số nội dung nhạy cảm.

Thật đáng ngại, thông tin cá nhân rất dễ tìm trên mạng vì...

3. Các trang web gia phả đầy thông tin cá nhân

Các trang web có thông tin cá nhân, như gia phả và "tìm người", đã có nhiều năm nay. Và việc chào bán thông tin trên các trang web này đã có từ lâu.

Giờ có thêm 2 xu hướng mới làm lộ thông tin cá nhân.

Đầu tiên là sự xuất hiện của siêu trang web thông tin cá nhân có tên là Family Tree Now. Trang web này cung cấp miễn phí thông tin mà các trang web khác bán. Từ chỗ vô danh, giờ trang web này đã nổi như cồn sau khi một người đăng trên Twitter về nó hồi tháng 1 năm nay. Chỉ cần nhập tên và thành phố nơi người nào đó sống, Family Tree Now có thể cho bạn biết các thành viên khác trong gia đình của người đó cùng với tuổi tác và địa chỉ nhà hiện tại và trước đây.

Xu hướng thứ hai đó là một số trang web "tìm người" sử dụng kỹ thuật xã hội để dụ bạn cung cấp thông tin. Ví dụ, trang TruthFinder hỏi bạn một loạt câu hỏi, hứa hẹn các câu trả lời của bạn sẽ giúp trang web đưa ra thông tin chính xác hơn. Thực ra, TruthFinder thu thập thông tin của bạn.

4. Ứng dụng di động gửi dữ liệu cá nhân đến máy chủ ở xa

Đầu năm nay ứng dụng iPhone chỉnh sửa ảnh chụp Meitu của Trung Quốc bỗng nổi đình nổi đám nhờ những hiệu ứng khác lạ. Nó cho phép biến hình chân dung thành ảnh hoạt hình siêu thực, làm trắng da, sáng mắt, to mắt và nhiều hiệu ứng khác. Nhưng đến đêm nó bật ứng dụng gửi mọi thông tin về Trung Quốc, bao gồm vị trí, thông tin về mạng di động và địa chỉ IP của bạn, và cả số IMEI của thiết bị Android. Đối phó làn sóng phẫn nộ của cộng đồng người dùng trên mạng, công ty này nói chỉ sử dụng dữ liệu để cải thiện ứng dụng chứ không có bán.

Giờ người ta biết một thực tế khó chịu, đó là nhiều ứng dụng thu thập dữ liệu mà bạn không hề biết hoặc cho phép.

Thế ứng dụng bảo mật có phải là giải pháp? Không may...

5. Ngay cả ứng dụng bảo mật cũng có thể là mối đe dọa

Một trong những cách tốt nhất để bảo vệ thông tin riêng tư trên mạng là sử dụng mạng riêng ảo (VPN). VPN về lý thuyết cho phép bạn sử dụng internet công cộng như mạng riêng. Nó che dấu và mã hóa hoạt động trực tuyến của bạn, ngay cả ISP (nhà cung cấp dịch vụ Internet) cũng không dò ra; và có thể dấu cả vị trí (địa lý), cho phép bạn giả đang ở thành phố hoặc quốc gia nào đó khác vị trí thực sự hiện tại.

Tuy nhiên, một nghiên cứu gần đây cho thấy khá nhiều dịch vụ VPN thông qua ứng dụng Android vi phạm quyền riêng tư chứ không phải bảo vệ.

Nghiên cứu được thực hiện bởi Đại học South Wales cho thấy 38% ứng dụng VPN cho Android bị nhiễm mã độc, 18% không hề mã hóa lưu lượng truyền và 75% theo dõi hoạt động người dùng. Một số VPN Android chèn mã JavaScript để theo dõi hoặc chuyển hướng truy vấn mua sắm trực tuyến đến trang web của đối tác.

THANH PHONG

Nguồn: Computerworld

ĐỐI PHÓ VỚI CÁC MỐI ĐE DỌA MỚI

Các chuyên gia bảo mật thường khuyên, để bảo vệ sự riêng tư bạn cần bật xác thực hai yếu tố nếu có thể; sử dụng trình quản lý mật khẩu như LastPass; chỉ tải ứng dụng ở những site đáng tin cậy. Nhưng với những mối đe dọa mới, giờ đây cần thêm các bước bổ sung sau.

1. **Hãy đăng ký ở trang web có tên là " Have I Been Pwned?" (*haveibeenpwned.com*). Nó sẽ cảnh báo khi thông tin cá nhân của bạn xuất hiện trên mạng do bị 'hack'. Thường tin tặc tấn công một trang web nào đó, tải về tất cả dữ liệu người dùng, sau đó tung lên mạng hoặc bán nó trên "thị trường đen".**
2. **Cố nhớ tất cả các trang web mà bạn đã đăng ký nhưng rồi không dùng. Vào lại các trang đó và xóa tài khoản.**
3. **Xem xét dùng thông tin giả. Mỗi khi một trang web nào đó đòi dữ liệu cá nhân, hãy cung cấp thông tin giả để phòng khi thông tin của bạn bị 'hack', bị dò tìm hoặc bị lộ.**
4. **Tìm các bức ảnh của bạn có hình bàn tay và ngón tay, xử lý sao cho không có dấu vân tay nào bị lộ.**
5. **Đừng sa vào những cuộc tranh cãi nảy lửa với những kẻ hay bới móc, cay cú hoặc cực đoan trên mạng.**
6. **Vào trang Family Tree Now và loại bỏ thông tin cá nhân của bạn.**

Internet luôn có những cách thức mới vi phạm sự riêng tư và bảo mật thông tin của bạn. Nhưng bạn có thể chống lại.