7 sai lầm khiến bảo mật Internet gặp rủi ro

Mỗi tuần, chúng ta lại thấy số vụ trộm cắp dữ liệu trực tuyến tăng lên. Bị hack tài khoản đang là mối đe dọa thường trực. Nhưng chúng ta vẫn có thể dễ dàng tự bảo vệ mình khỏi những cuộc tấn công này bằng cách sửa đổi một số thói quen xấu. Bài viết sau đây sẽ liệt kê những sai lầm phổ biến nhất khiến bảo mật Internet của bạn gặp rủi ro và cách khắc phục chúng.

Sai lầm 1: Bạn không sử dụng mật khẩu đủ mạnh

Mật khẩu phổ biến nhất trong năm 2016, cũng như năm 2015 và 2014 là "**123456**.", tiếp theo là "**123456789**" và "**qwerty**". Có thể nói đây là nguyên nhân của rất nhiều cuộc tấn công mạng đang diễn ra.

Một nghiên cứu gần đây của công ty an ninh mạng Preempt đã tiết lộ rằng 35% người dùng LinkedIn sử dụng mật khẩu yếu, do đó làm tăng nguy cơ tài khoản của họ bị tấn công.

Vậy mật khẩu mạnh nên có những yếu tố gì? Lưu ý những điều sau đây:

- Tối thiểu 12 ký tự. Càng nhiều càng tốt.
- Phải bao gồm số, ký hiệu, chữ hoa và chữ thường.

- Không được là một từ đơn hoặc cụm từ đơn giản có nghĩa.
- Thay thế một số chữ cái bằng ký tự khác thay thế. Ví dụ, **r0bber** thay vì **robber**.
- Trên mạng, bạn có thể tìm thấy nhiều công cụ giúp bạn phân tích và đánh giá mức độ mạnh, yếu của các mật khẩu bạn định dùng. Một ví dụ điển hình là The Password Meter. (Link tải The Password Meter: http://www.passwordmeter.com/)

Nhưng điều đó cũng có nghĩa rằng, bạn phải tạo ra hàng trăm mật khẩu dài và ghi nhớ hết chúng. Thật kinh khủng! Tuy nhiên, đừng quá lo lắng vì bạn sẽ tìm thấy một giải pháp hữu ích cho điều này trong phần tiếp theo.

Sai lầm 2: Bạn không sử dụng trình quản lý mật khẩu

Các chuyên gia bảo mật khuyên chúng ta nên sử dụng mật khẩu khác nhau cho mỗi tài khoản. Bằng cách này, nếu một trong các tài khoản này bị tấn công, các tài khoản khác của chúng ta sẽ vẫn an toàn.

Tuy nhiên, ngày nay, chúng ta có thể cần phải tạo ra từ 20-50 mật khẩu khác nhau. Con số đó là quá nhiều! May mắn thay, quá trình này có thể được đơn giản hóa với trình quản lý mật khẩu - công cụ không chỉ giúp ghi nhớ mật khẩu mà còn cung cấp thêm một lớp bảo mật khác.

Trình quản lý mật khẩu là chương trình tạo, lưu trữ và tổ chức tất cả mật khẩu trên thiết bị, mạng xã hội và ứng dụng của bạn. Tất cả những gì bạn phải làm là nhớ mật khẩu chính kích hoạt trình quản lý mật khẩu này.

Nếu bạn tạo mật khẩu chính dài và có độ bảo mật cao, như chúng tôi đã đề cập ở phần trước, đảm bảo rằng không ai khác có thể truy cập bất kỳ tài khoản nào của bạn.

Có rất nhiều trình quản lý mật khẩu, nhưng một trong những trình quản lý mật khẩu an toàn và mạnh mẽ nhất là Keeper Password Manager. Công cụ này tự hào có một hệ thống mã hóa quân sự để bảo vệ mật khẩu của bạn, tương thích với tất cả các thiết bị chính và cũng có hệ thống tự hủy xóa tất cả các bản ghi nếu mật khẩu chính được nhập sai năm lần liên tiếp.

Sai lầm 3: Bạn không sử dụng hệ thống xác minh hai bước

Xác minh hai bước là lớp bảo mật bổ sung giúp bảo mật tài khoản của bạn, bất kể mật khẩu của bạn có mạnh như "**8$&]$@I)9[P&4^s**" hay yếu như "**123456**".

Hệ thống này được kích hoạt khi bạn cố truy cập tài khoản của mình từ một thiết bị không xác định, vì hệ thống không biết đó có phải là tin tặc hay chủ sở hữu tài khoản sử dụng thiết bị khác với thông thường hay không. Thông điệp "cảnh báo" sẽ được gửi tới cho chủ sở hữu qua SMS tới điện thoại di động của họ kèm theo một mã bảo mật. Bạn cần phải nhập mã đó trong một khoảng thời gian ngắn để truy cập vào tài khoản được đề cập.

Nếu các dịch vụ bạn sử dụng, chẳng hạn như Google, Facebook, cung cấp xác minh hai bước, thì đừng ngần ngại kích hoạt nó. Có thể nó sẽ gây khó chịu một chút nhưng rất hữu ích.

Ngoài ra, bạn còn có các ứng dụng quản lý xác minh hai bước khác, chẳng hạn như Authy. Trong trường hợp của Authy, tất cả các mã đều ở cùng một nơi, làm cho quy trình được đơn giản hóa hơn nữa.

Sai lầm 4: Bạn bất cẩn với Wi-Fi công cộng

Hầu hết Wi-Fi công cộng đều nguy hiểm và không an toàn. Xin lưu ý rằng khi bạn kết nối với Wi-Fi, bạn đang cấp cho chủ sở hữu quyền truy cập vào danh tính cá nhân của bạn. Bạn có thể gặp phải một sự ngạc nhiên khó chịu nếu bạn kết nối với bất kỳ điểm truy cập Wi-Fi nào mà không nghĩ đến việc ai đó có thể theo dõi bạn.

Điều đó có nghĩa là bạn nên nghi ngờ tất cả truy cập Wi-Fi công cộng? Không hẳn là như vậy, vẫn có những ngoại lệ. Bạn có thể tin tưởng truy cập Wi-Fi tại các sân bay, quán cà phê, nhà hàng, khách sạn…

Mặt khác, Norton đã đưa ra một loạt các mẹo để giảm thiểu rủi ro cho bạn khi kết nối với Wi-Fi công cộng:

- Trước khi kết nối, hãy thiết lập cài đặt bảo mật trên thiết bị của bạn.
- Nếu bạn đang đi du lịch, hãy thay đổi mật khẩu của bạn trước và sau chuyến đi.
- Cập nhật phần mềm và ứng dụng của bạn (chúng tôi sẽ nói thêm ở phần sau).
- Tránh đăng nhập vào bất kỳ tài khoản trực tuyến nào lưu trữ thông tin cá nhân. Vì vậy, đừng kiểm tra tài khoản ngân hàng của bạn qua Wi-Fi công cộng.
- Đảm bảo URL bạn đang truy cập bắt đầu bằng HTTPS. “S” chỉ ra rằng dữ liệu được mã hóa.

Sai lầm 5: Bạn không cập nhật phần mềm của mình

Tội phạm mạng rất nhanh chóng tìm thấy lỗ hổng trong phần mềm phổ biến như Windows hoặc Chrome. Để chống lại vấn đề này, các nhà phát triển khởi chạy các bản cập nhật với tốc độ nhanh chóng để khắc phục những vi phạm bảo mật này.

Điều gì sẽ xảy ra với những người không cập nhật phần mềm của họ? Họ sẽ trở thành mục tiêu hoàn hảo trong không gian mạng. Ví dụ, phần mềm độc hại WannaCry nổi tiếng là hậu quả trực tiếp của các công ty bỏ qua vấn đề cập nhật phần mềm.

Điều quan trọng là phải cập nhật tất cả phần mềm và hệ điều hành của bạn. Tin tốt là đôi khi, các phần mềm này tự cập nhật. Tuy nhiên, một số phần mềm khác lại yêu cầu bạn cho phép "cập nhật". Điều này thường xảy ra với Windows. Chúng tôi đã biết rằng bạn rất ngại khi phải cập nhật mọi thứ trên máy tính, nhưng việc này rất quan trọng!

Ngoài ra, những phần mềm lỗi thời thường ảnh hưởng đến hiệu suất của máy tính. Nếu máy tính của bạn chạy chậm, hoặc trình duyệt của bạn mất nhiều thời gian để tải trang… thì đó cũng là lý do để cập nhật các phần mềm!

Sai lầm 6: Bạn không cẩn thận khi ở trên các mạng xã hội

Chúng ta đều biết rằng các mạng xã hội (Facebook, Twitter, Instagram...) là những nơi tuyệt vời để chia sẻ suy nghĩ, mối quan tâm và bất cứ điều gì làm cho chúng ta hạnh phúc. Tuy nhiên, chúng ta đang sử dụng chúng như một thói quen mà ít khi nghĩ tới những hậu quả chúng có thể mang lại. Chúng ta đang chia sẻ quá nhiều thông tin ở một nơi mà hầu hết mọi người đều có thể nhìn thấy.

Vì vậy, hãy dành thời gian và xem lại cài đặt bảo mật của các tài khoản mạng xã hội, đặc biệt là trên Facebook. Nhiều người dùng Facebook thường ngạc nhiên khi biết những người mà họ thậm chí không biết đã đọc được thông tin về họ và điều này là do cài đặt bảo mật trên tài khoản Facebook. Hãy kiểm tra cài đặt bảo mật tài khoản Facebook của bạn ngay bây giờ.

Ngoài ra, chúng tôi cũng khuyên bạn đừng nói về một số vấn đề nhất định trên mạng xã hội vì nhiều mạng xã hội được coi là cánh cửa mở cho bọn tin tặc.

NHỮNG GÌ KHÔNG NÊN CHIA SẺ TRÊN MẠNG XÃ HỘI?

- Thông tin rất cá nhân có thể giúp tin tặc đoán mật khẩu của bạn.
- Vị trí của bạn mọi lúc, đặc biệt nếu bạn không ở nhà trong một thời gian dài.
- Ảnh của trẻ em hoặc trẻ vị thành niên (và nếu bạn chia sẻ hình ảnh về bọn trẻ, hãy đảm bảo cài đặt bảo mật của bạn được đặt ở mức tối đa).
- Chi tiết rất cụ thể về công việc, có thể gây ra vấn đề cho bạn.

Sai lầm 7: Bạn không kiểm tra chi tiết trong các email bạn nhận được

Lừa đảo là khi ai đó trên Internet giả vờ là người khác hoặc thậm chí là một công ty để họ có thể lấy cắp dữ liệu của bạn hoặc lây nhiễm virus sang PC của bạn. Email là nền tảng sinh sản hoàn hảo cho loại lừa đảo này, cho dù đó là email từ bạn bè, gia đình hay thậm chí là các cửa hàng trực tuyến hoặc ngân hàng của chúng ta.

Vì vậy, bất cứ khi nào bạn nhận được email yêu cầu bạn cung cấp dữ liệu hoặc kèm theo tệp đính kèm hoặc liên kết, hãy đảm bảo rằng chính cá nhân hoặc tổ chức mà bạn đang liên hệ đã gửi email. Lỗi chính tả hoặc thông tin không rõ ràng thường đồng nghĩa với lừa đảo.

Ngoài ra, hãy nhớ rằng một công ty thông thường sẽ không bao giờ yêu cầu bạn gửi cho họ chi tiết đăng nhập, mật khẩu hoặc số thẻ tín dụng của bạn qua email. Ngoài ra, nếu bạn không mong đợi file đính kèm, không mở bất kỳ file đính kèm nào.