5 cách giữ tài khoản mạng xã hội luôn an toàn

Mạng xã hội mang lại nhiều lợi ích nhưng cũng là nơi ẩn chứa những hiểm họa mà bạn cần tỉnh táo đề phòng. Dưới đây là những giải pháp giúp bảo vệ tài khoản mạng xã hội an toàn hơn mà bạn nên áp dụng.

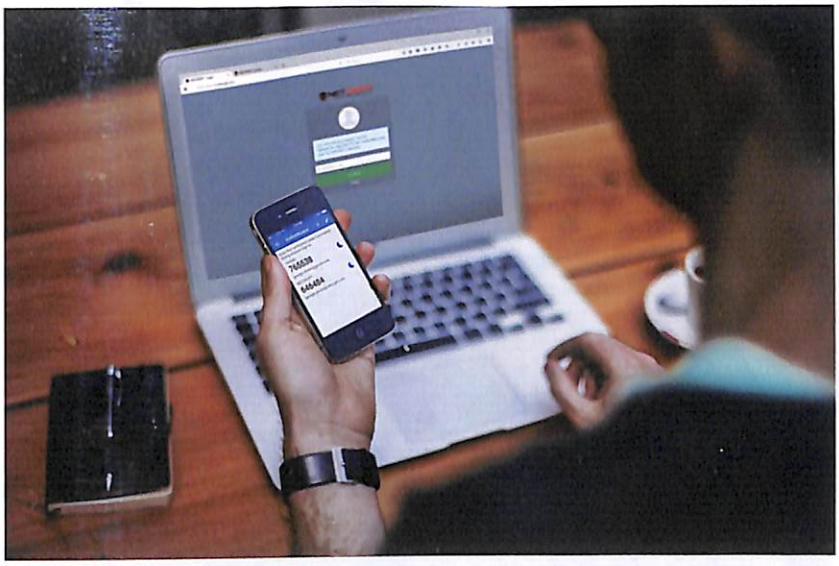
1. Dùng mật khẩu mạnh

Các chuyên gia bảo mật thường khuyến cáo người dùng nên sử dụng mật khẩu mạnh, phức tạp cho tài khoản mạng xã hội để giảm rủi ro bị bẻ khóa. Tin tặc thường dùng phương pháp tấn công dựa trên danh sách có sẵn (*dictionary attack*) để dò tìm mật khẩu. Vì vậy, bạn không nên đặt mật khẩu đơn giản như những tên gọi quen thuộc, những cụm từ phổ biến hoặc thông tin cá nhân liên quan đến mình mà nhiều người biết (ngày tháng năm sinh, số điện thoại, bảng số xe,...).

Bạn có thể thêm vào một chút phức tạp bằng cách đặt mật khẩu càng khó đoán càng tốt, nhưng yếu tố này không tăng mức phòng vệ lên là mấy mà đôi khi còn khiến bạn không thể nhớ mật khẩu của chính mình. Cách đặt mật khẩu hiệu quả nhất là kết hợp giữa số, chữ hoa, chữ thường, có ký tự đặc biệt và đủ dài. Về mặt kỹ thuật, mật khẩu với độ dài khoảng từ 8-12 ký tự thường rất khó bị phá.

2. Kích hoạt tính năng xác thực hai bước

Hiện nay, thủ thuật đánh cắp thông tin ngày càng tinh vi hơn và người dùng rất dễ bị mất tài khoản mạng xã hội của mình. Chính vì thế, các nhà cung cấp dịch vụ đã tăng cường cơ chế bảo vệ tài khoản của người dùng khi cung cấp thêm tính năng xác thực hai bước (*two-factor authentication*). Hiện nay, hầu như các mạng xã hội như Facebook, Twitter, Google,... đều đã áp dụng chính sách bảo mật xác thực hai bước cho tài khoản người dùng. Dù không đảm bảo an toàn tuyệt đối nhưng cơ chế bảo mật này sẽ giúp bạn bảo vệ dữ liệu hiệu quả hơn và ngăn chặn hậu quả tốt hơn trong kỷ nguyên số ngày nay.



Tính năng xác thực hai bước đang được các mạng xã hội áp dụng để bảo vệ người dùng.

Như tên gọi, phương pháp này buộc người dùng phải thực hiện hai bước để xác thực khi đăng nhập vào tài khoản mạng xã hội. Để có thể hình dung cách thức hoạt động của bảo mật xác thực hai bước, ta hãy lấy ví dụ khi truy cập Facebook trên một thiết bị khác không cùng địa chỉ IP, mạng xã hội này sẽ bắt người dùng trải qua một số công đoạn như phải nhập mã an toàn được gửi vào hộp thư email hoặc qua số điện thoại đã đăng ký trước đó. Thậm chí nếu mật khẩu bị lộ và tin tặc có truy cập vào tài khoản của bạn thì chúng cũng khó lòng chiếm đoạt được email hay đánh cắp tin nhắn gửi tới điện thoại của bạn.

3. Cài đặt trình diệt virus

Theo các chuyên gia bảo mật, người dùng Internet ngày nay ưa chuộng các đường dẫn rút gọn chia sẻ trên mạng xã hội mà không lường được rất nhiều mã độc phân tán kèm theo. Cụ thể, các tài khoản trên Facebook và Twitter ngày càng xuất hiện nhiều đường dẫn được rút gọn bởi các dịch vụ nổi tiếng như bit.ly và alturl.com. Các liên kết này có thể bị đổi hướng khiến người dùng bị lừa đến các trang web có chứa mã độc.

Để ngăn ngừa tình trạng trên, các nhà cung cấp dịch vụ Internet (*ISP – Internet Service Provider*) thường đưa ra một số chính sách bảo vệ ngay từ chính máy chủ của họ. Tuy nhiên, tốt nhất là bạn nên tự bảo vệ mình trước bằng cách cài đặt một chương trình chống virus hiệu quả, được cung cấp bởi những hãng bảo mật nổi tiếng. Tin tặc thường sử dụng hình thức tấn công mã độc và ngày càng hoàn thiện chiến thuật của mình. Tuy nhiên, kiểu tấn công này hầu như thường bị chặn lại bởi những chương trình chống virus chính thống.

4. Sử dụng trình quản lý mật khẩu

Hiện nay, một người dùng thường sở hữu tài khoản nhiều mạng xã hội khác nhau cùng với hàng loạt mật khẩu đăng nhập tương ứng. Việc ghi nhớ nhiều mật khẩu phức tạp là điều rất u "bất khả thi", trong khi giải pháp viết tắt cả mật khẩu đang dùng lên một mẩu giấy để luôn mang theo bên mình thì lại bị đánh giá là cực kỳ bất cập.

Để tiện ghi nhớ, nhiều người thường dùng chung một mật khẩu cho mọi dịch vụ, trang web và cả ứng dụng. Chính thói quen đó đã đặt ra lo ngại nếu hacker biết được mật khẩu của một dịch vụ thì chúng có thể sử dụng để tấn công tài khoản của nạn nhân trên đồng loạt các trang web khác. Đó chính là lý do các công cụ quản lý mật khẩu xuất hiện. Một số công cụ dạng này được nhiều người tin cậy như LastPass, 1Password, PasswordBox .

Sử dụng trình quản lý mật khẩu để lưu mật khẩu các dịch vụ mạng.

5. Lựa chọn ứng dụng bên thứ ba phù hợp

Một trong những lưu ý mà người dùng cần ghi nhớ để đảm bảo thông tin cá nhân khi lên mạng xã hội là nên chọn lựa kỹ những ứng dụng của bên thứ ba. Khi bạn sử dụng một ứng dụng của bên thứ ba chẳng hạn như trình lên lịch đăng bài trên mạng xã hội, nó sẽ yêu cầu quyền truy cập vào tài khoản của bạn. Hãy chắc chắn rằng bạn đang cho phép ứng dụng hợp pháp truy cập và hãy chắc chắn đọc kỹ chi tiết về những gì bạn đang cho phép ứng dụng có quyền truy cập vào.

Một số ứng dụng chỉ yêu cầu các quyền tối thiểu chẳng hạn như khả năng đọc và đăng tải nội dung. Vì vậy, chỉ nên cấp quyền đọc và đăng tải thay vì gán tất cả quyền cho ứng dụng đó. Tốt nhất là bạn nên đăng nhập vào tất cả tài khoản mạng xã hội của mình và kiểm tra những ứng dụng hiện tại đang có những quyền truy cập nào. Bạn có thể vô hiệu hóa bất cứ những quyền truy cập nào mà mình cảm thấy không tin tưởng hoặc gỡ bỏ bất kỳ ứng dụng nào không sử dụng.

HUY THẮNG