

CÁCH LẤY LẠI FACEBOOK SAU KHI ĐÃ NHẤN LINK LỪA ĐẢO

Gần đây, khá nhiều người dùng đã bị mất tài khoản và không thể lấy lại Facebook do nhấn vào những đường link thông báo trúng thưởng với những giải thưởng rất giá trị như xe Vespa hoặc SH.

Hướng dẫn lấy lại facebook sau khi nhấn link lừa đảo

Xuất hiện khoảng vài tuần nay trên mạng xã hội Facebook, tin nhắn của nickname "Facebook Thông Báo" là một dạng tin nhắn lừa đảo qua hình thức thông báo trúng thưởng. Nhiều người dùng Facebook tại Việt Nam nhận được tin nhắn gửi qua Messenger với nội dung chúc mừng may mắn trúng giải đặc biệt mẫu xe Vespa hoặc SH trong chương trình tri ân khách hàng của Facebook. Sau khi làm theo hướng dẫn để nhận giải, tên tài khoản của người dùng bỗng dưng bị thay đổi, thậm chí không thể lấy lại Facebook.

Nhiều người đã mất và không thể lấy lại Facebook do nhấn vào những đường link lừa đảo

Lừa đảo Facebook tràn lan

Nhiều người đã làm theo hướng dẫn trong nội dung tin nhắn và truy cập vào địa chỉ trang web: <http://Giai.....> Sau đó, nhận được yêu cầu cung cấp thông tin đăng nhập, bao gồm tên người dùng lẫn mật khẩu của tài khoản Facebook. Nghĩ rằng đó là cần thiết để xác nhận thông tin trúng giải như trong hướng dẫn nhận giải, nhiều người đã làm đúng như yêu cầu đưa ra.

Khi đã khai báo thông tin đăng nhập, trang web lừa đảo sẽ đưa người dùng đến trang web với nội dung được thiết kế bắt mắt, tạo cảm giác đây là một trang web có uy tín, thậm chí có cả khẳng định như "Bộ Thông tin - truyền thông cam kết đảm bảo 100% khi làm thủ tục hồ sơ tại <http://.....facebookvn....>". Thậm chí chủ trang web còn trưng cả hình ảnh chứng nhận hạ tầng thanh toán trực tuyến an toàn, phía dưới có cả hình quốc huy và logo Bộ TT&TT.... cùng với đó là hình ảnh hiện ra như xe SH, MacBook Pro, iPhone 6... Nhưng sau đó, người dùng sẽ không thấy bất cứ hồi âm nào.

Tên người dùng sẽ bị thay đổi và không thể lấy lại Facebook. (Ảnh Facebook)

Khi truy cập vào Facebook người dùng mới phát hiện tên FB đã được đổi thành "Thông Báo Sự Kiện" và kẻ lừa đảo sẽ tiếp tục dùng tài khoản Facebook này để đi lừa đảo những người khác trong danh sách bạn bè của nạn nhân.

Cách lấy lại Facebook

Khi nạn nhân bị lừa bấm vào link dẫn tới trang web độc hại, dù họ chưa thao tác gì tại website đó thì về mặt kỹ thuật, kẻ xấu vẫn có thể cài đặt được mã độc lên thiết bị của nạn nhân thông qua các lỗ hổng trình duyệt. Khi đó, hacker đủ quyền để kiểm soát máy tính, đánh cắp dữ liệu và các thông tin về tài khoản. Tuy nhiên, kiểu tấn công qua lỗ hổng này đòi hỏi hacker phải tốn công sức hơn nhiều so với việc lừa nạn nhân tự cài mã độc (ví dụ lừa cài plugin để xem video), hay lừa nạn nhân điền mật khẩu vào website có giao diện và tên miền giống với các website nổi tiếng.

Không nên điền mật khẩu cho bất kể trang web nào

Do đó, hình thức lừa đảo vẫn phổ biến hơn kiểu khai thác lỗ hổng và hacker sẽ nghĩ ra nhiều kịch bản để dụ người dùng. Ví dụ, hacker giả mạo Facebook để trao thưởng, hay giả mạo bạn bè chia sẻ nhau các đoạn video hài.... Trong trường hợp này, nếu vô tình bị lừa vào website mà người dùng không cài phần mềm nào hoặc không điền thông tin mật khẩu thì sẽ không bị ảnh hưởng.

Với trường hợp hacker yêu cầu phải tải phần mềm để xem video, ảnh... và người dùng đã ngây

thor làm theo, họ cần nhanh chóng gỡ bỏ các plug-in, ứng dụng mới được cài trên trình duyệt cũng như máy tính, thiết bị di động.

Bên cạnh đó, người dùng cần trang bị cho máy tính hay smartphone của họ một phần mềm diệt virus để giúp ngăn chặn các nguy cơ cũng như giúp nhanh chóng gỡ bỏ được các phần mềm độc hại.

Một cách để lấy lại Facebook là gỡ bỏ các tiện ích mà trang web lừa đảo cài đặt

Với trường hợp đã điền thông tin tài khoản và mật khẩu vào trang có giao diện giống Facebook, điều này có nghĩa mật khẩu của người dùng đã bị rơi vào tay kẻ xấu. Do đó, người dùng cần ngay lập tức thay đổi mật khẩu Facebook cũng như của các tài khoản (Gmail, Yahoo...) có dùng chung password đó, tránh trường hợp tài khoản bị lợi dụng phát tán tiếp thậm chí là có thể mất vĩnh viễn tài khoản nếu như hacker đổi mật khẩu của người dùng.

Người dùng cũng nên thiết lập ngay cơ chế xác thực hai yếu tố cho các tài khoản Facebook, Gmail... Có nghĩa là để đăng nhập được, ngoài mật khẩu chính, còn phải thêm một mật khẩu OTP (One Time Password) mà người dùng nhận qua SMS hoặc một ứng dụng cài trên điện thoại. Nếu hacker đánh cắp được mật khẩu, chúng cũng không thể truy cập vào được tài khoản.