

Cảnh giác trước link phishing lừa đảo

11:08 24/07/2023

Để tránh bị lừa đảo, người dân cần hết sức cảnh giác trước các đường link lạ.



Ảnh minh họa

Theo Cục An toàn thông tin, Bộ Thông tin và Truyền thông, chiêu trò rải link phishing lừa đảo, seeding quảng cáo "bẩn" trên Facebook thường có một số dấu hiệu đáng chú ý như:

- Tạo trang web giả mạo: Kẻ lừa đảo tạo một trang web giả mạo có giao diện tương tự như một trang web đáng tin cậy như ngân hàng hoặc dịch vụ trực tuyến. Trang web này được thiết kế để thu thập thông tin cá nhân và đăng nhập của người dùng khi họ nhập vào.
- Tạo một đường link hấp dẫn: Kẻ lừa đảo tạo một đường link hấp dẫn sử dụng một tiêu đề hoặc mô tả mà người dùng có thể quan tâm, chẳng hạn như "Nhận ngay ưu đãi đặc biệt" hoặc "Kiểm tra tài khoản của bạn" hoặc "Bạn bị bóc phốt" hoặc các sự kiện đang hot trending xu hướng trên mạng xã hội. Đảm bảo đường link này giống như một đường link đáng tin cậy để gây thiện cảm và khó phát hiện.

- Rải link và seeding quảng cáo bẩn trên Facebook: Kẻ lừa đảo sử dụng các tài khoản giả mạo hoặc các tài khoản đã bị xâm nhập để rải link và seeding quảng cáo bẩn trên Facebook. Đăng bài viết, nhận xét, bình luận hoặc quảng cáo với đường link đã được tạo, hấp dẫn người dùng để nhấn vào.

- Lừa đảo và đánh cắp thông tin, tài sản: Khi người dùng nhấn vào đường link lừa đảo, họ sẽ được chuyển hướng đến trang web phishing mà kẻ lừa đảo đã tạo. Từ đó, kẻ lừa đảo có thể thu thập thông tin cá nhân, tài khoản hoặc đăng nhập của họ và sử dụng để lừa đảo hoặc đánh cắp tài sản.

Cục An toàn thông tin, Bộ Thông tin và Truyền thông khuyến cáo, để tránh bị lừa đảo, người dân cần hết sức cảnh giác.

- Cẩn thận với các đường link không rõ nguồn gốc: Khi bạn nhận được một đường link từ nguồn không rõ hoặc không quen thuộc, hãy cẩn thận và không nhấp vào ngay. Kiểm tra xem link có xuất phát từ một nguồn đáng tin cậy hay không. Các đường link rút gọn cũng cần được kiểm tra trước khi nhấp vào.

- Kiểm tra địa chỉ URL trước khi nhấp vào: Trước khi nhấp vào một đường link trên Facebook hoặc bất kỳ nền tảng nào, hãy kiểm tra địa chỉ URL trên thanh địa chỉ của trình duyệt. Đảm bảo rằng nó khớp với trang web bạn định truy cập và không có các ký tự hoặc chuỗi lạ.

- Đánh giá tính xác thực của quảng cáo, tin nhắn, bình luận: Khi bạn thấy một quảng cáo trên Facebook, hãy đánh giá tính xác thực của nó trước khi tương tác. Kiểm tra chính xác nguồn gốc của quảng cáo, tìm hiểu về công ty hoặc sản phẩm được quảng cáo và đảm bảo rằng nó không có dấu hiệu lừa đảo hoặc đánh cắp thông tin.

- Tăng cường bảo mật tài khoản: Đảm bảo rằng bạn sử dụng mật khẩu mạnh và kích hoạt các biện pháp bảo mật bổ sung như xác thực hai yếu tố cho tài khoản Facebook của bạn. Điều này giúp ngăn chặn kẻ xấu truy cập vào tài khoản và tránh việc rải link phishing từ tài khoản của bạn.

- Tìm hiểu về các hình thức lừa đảo và phishing: Để trở nên cảnh giác hơn, tìm hiểu về các hình thức lừa đảo và phishing phổ biến, cùng với các dấu hiệu nhận biết và kỹ thuật lừa đảo. Điều này giúp bạn nhận ra các quảng cáo hoặc đường link đáng ngờ và tránh nhấp vào chúng.

- Cài đặt phần mềm chống phishing và bảo mật: Sử dụng phần mềm chống malware và chống phishing để bảo vệ thiết bị của bạn

- Cẩn trọng với việc chia sẻ thông tin cá nhân: Hạn chế việc chia sẻ thông tin cá nhân trên Facebook và các nền tảng trực tuyến khác. Tránh việc cung cấp thông tin nhạy cảm như số thẻ tín dụng, số bảo hiểm xã hội hoặc bất kỳ thông tin cá nhân khác cho các đường link hoặc quảng cáo không rõ nguồn gốc.

- Kiểm tra đánh giá và phản hồi của người dùng khác: Trước khi tương tác với một đường link hoặc quảng cáo, hãy đọc các đánh giá và phản hồi từ người dùng khác. Nếu có những báo cáo về lừa đảo hoặc đánh cắp thông tin, hãy cân nhắc và tránh tương tác với nội dung đó.

- Luôn cập nhật và sử dụng phiên bản mới nhất của trình duyệt và phần mềm bảo mật: Đảm bảo rằng bạn luôn cập nhật phiên bản mới nhất của trình duyệt web và phần mềm bảo mật trên thiết bị của bạn. Các bản vá bảo mật thường cung cấp bảo vệ chống lại các lỗ hổng bảo mật và các cuộc tấn công phishing.

- Báo cáo các trường hợp đáng ngờ: Nếu bạn phát hiện một đường link phishing hoặc quảng cáo lừa đảo trên Facebook, hãy báo cáo cho Facebook bằng cách sử dụng tính năng báo cáo hoặc liên hệ trực tiếp với họ để thông báo về tình huống. Bằng cách báo cáo, bạn giúp ngăn chặn sự lan truyền của lừa đảo và bảo vệ cộng đồng trực tuyến.

- Giáo dục và nâng cao nhận thức: Nắm vững kiến thức về các hình thức lừa đảo và phishing trên mạng xã hội. Hãy chia sẻ thông tin và nhận thức này với gia đình, bạn bè và cộng đồng của bạn để giúp họ tránh trở thành nạn nhân và cùng nhau tạo một môi trường trực tuyến an toàn hơn. Theo dõi và cập nhật các thông tin, tình huống, dấu hiệu về lừa đảo trực tuyến tại Cổng không gian mạng quốc gia (khonggianmang.vn).

Hà Trần (t/h)