

Dấu hiệu nhận diện tài khoản mạng xã hội bị đánh cắp, nhắn tin lừa đảo

15:29 19/07/2023

Thời gian qua, tình hình tội phạm và vi phạm pháp luật liên quan đến hoạt động lừa đảo chiếm đoạt tài sản vẫn diễn biến phức tạp, với thủ đoạn tinh vi, đặc biệt là lừa đảo chiếm đoạt tài sản trên không gian mạng có chiều hướng gia tăng. Nhóm tội phạm này sử dụng nhiều thủ đoạn khác nhau để chiếm quyền điều khiển tài khoản mạng xã hội (gửi các đường link giả mạo thông tin dịch bệnh COVID-19, quảng cáo tuyển dụng, làm việc tại nhà, các trò chơi giải trí trên mạng...).



Ảnh minh họa

Người dùng cần lưu ý những dấu hiệu sau để nhận diện tài khoản mạng xã hội bị đánh cắp, nhắn tin lừa đảo:

- Tin nhắn hoặc email đáng ngờ: Nếu bạn nhận được một tin nhắn hoặc email từ một người bạn trong danh sách bạn bè yêu cầu cung cấp thông tin cá nhân nhạy cảm, yêu cầu chuyển tiền hoặc thực hiện hành động khẩn cấp, hãy cảnh giác. Đặc biệt, nếu tin nhắn có chứa các lời khẩn cấp, đe dọa hoặc yêu cầu không phù hợp, hãy kiểm tra lại xem có phải tin nhắn thực sự từ bạn bè của bạn hay không.

- Sự thay đổi đột ngột trong ngôn ngữ hoặc phong cách viết: Nếu tin nhắn từ bạn bè có sự thay đổi đột ngột trong cách viết, từ ngữ không giống với phong cách thông thường hoặc có chứa các lời lẽ lạ lùng, cần thận hơn.

- Đường link đáng ngờ: Kiểm tra đường link được chia sẻ trong tin nhắn. Nếu đường link có dấu hiệu đáng ngờ như URL không phổ biến, thiếu ký tự an toàn (https://), hoặc điều hướng đến các trang web không rõ nguồn gốc hoặc đáng ngờ, hãy tránh nhấp chuột hoặc truy cập vào đường link đó.

- Yêu cầu cung cấp thông tin cá nhân hoặc thông tin đăng nhập: Lưu ý rằng bạn không nên cung cấp thông tin cá nhân nhạy cảm hoặc thông tin đăng nhập (tên đăng nhập, mật khẩu) thông qua tin nhắn hoặc email. Lừa đảo thường sử dụng chiêu này để chiếm quyền điều khiển tài khoản của bạn.

- Xác minh thông tin: Nếu bạn nhận được một tin nhắn hoặc email đáng ngờ từ một người bạn, hãy thử liên hệ trực tiếp với họ thông qua các phương tiện khác (điện thoại, tin nhắn, email) để xác minh xem tin nhắn đó có phải từ họ hay không. Đừng sử dụng thông tin liên hệ được cung cấp trong tin nhắn đáng ngờ để xác minh.

- Báo cáo và cảnh báo: Nếu bạn nhận thấy bất kỳ dấu hiệu lừa đảo nào, hãy báo cáo ngay lập tức cho người bạn bè bị ảnh hưởng và thông báo vụ việc cho nền tảng mạng xã hội hoặc dịch vụ email để họ có thể thực hiện biện pháp cần thiết.

Cần làm gì khi bị đánh cắp tài khoản mạng xã hội, nhận tin lừa đảo?

Nếu bạn hay người thân gặp phải bất kỳ dấu hiệu nào như trên, hãy thực hiện các biện pháp sau:

- Thay đổi mật khẩu ngay lập tức của tài khoản mạng xã hội và sử dụng một mật khẩu mạnh, bao gồm cả chữ hoa, chữ thường, số và ký tự đặc biệt.

- Báo cáo sự cố thông qua mạng xã hội hoặc các liên hệ khác như điện thoại, email.

- Thông báo cho bạn bè và người thân trong danh sách bạn bè của bạn về tình huống và cảnh báo họ không nên tin tưởng hoặc phản hồi vào những tin nhắn lừa đảo.

Ngoài ra, hãy luôn giữ cảnh giác và tuân thủ các biện pháp bảo mật cơ bản như không chia sẻ thông tin cá nhân và mật khẩu với bất kỳ ai, không bấm vào các liên kết không rõ nguồn gốc hoặc tin nhắn đáng ngờ, và cập nhật phần mềm

bảo mật định kỳ để tránh các lỗ hổng bảo mật.

Hà Trần