Trong thời gian qua, các sự cố lộ lọt thông tin, dữ liệu cá nhân, lừa đảo trực tuyến diễn biến ngày càng phức tạp với nhiều thủ đoạn tinh vi. Một trong những nguyên nhân chính gây ra mất an toàn thông tin được xác định đến từ nhận thức của người sử dụng. Các cuộc tấn công mạng có xu hướng tập trung chủ yếu vào con người thay vì máy móc, thiết bị. Việc trang bị cho mỗi cá nhân những kiến thức và kỹ năng cơ bản để bảo đảm an toàn thông tin trên không gian mạng là yếu tố then chốt giúp tạo dựng một không gian mạng Việt Nam an toàn, góp phần thúc đẩy nhanh quá trình chuyển đổi số, phát triển hạ tầng kinh tế - xã hội số một cách bền vững.



**ốn bước nhận diện, phòng tránh và xử lý khi bị lừa đảo trực tuyến.**

**Cách nhận diện các chiêu trò lừa đảo trực tuyến**

Các kỹ năng phòng tránh lừa đảo trực tuyến cơ bản: Việc nâng cao nhận thức, luôn cảnh giác trước những bất thường khi tham gia không gian mạng là những kỹ năng cơ bản giúp hạn chế tối đa rủi ro không đáng có.

Để phòng tránh lừa đảo trực tuyến, việc đầu tiên người dùng cần làm là kiểm tra nguồn gốc thông tin. Xác định xem thông tin đến từ nguồn đáng tin cậy hay không. Kiểm tra tên miền và đường dẫn URL của trang web. Hãy chú ý đến các tên miền khác thường, có lỗi chính tả hoặc không có các chứng chỉ tín nhiệm mạng.

Thứ hai là cảnh giác với người lạ kết bạn qua mạng xã hội Zalo, Facebook, Telegram… Khi có dấu hiệu khả nghi ngay lập tức không kết bạn và không trả lời. Ngoài ra ẩn đi danh sách bạn bè của mình trên các tài khoản mạng xã hội để tránh bị đối tượng lừa đảo biết đến các mối quan hệ xung quanh của mình.

Thứ ba là cảnh giác với email và tin nhắn lạ. Các email hoặc tin nhắn lừa đảo thường giả mạo các tổ chức uy tín (như ngân hàng, đơn vị nhà nước hoặc công ty công nghệ).

Kiểm tra kỹ địa chỉ email người gửi, so sánh đối chiếu với địa chỉ email được ghi trên các cổng thông tin chính thống. Thông thường, các địa chỉ Email giả mạo sẽ bao gồm các ký tự thừa, tên miền không chính xác.

Thứ tư là cẩn thận với các yêu cầu cung cấp thông tin cá nhân, tài chính. Không chia sẻ thông tin cá nhân hoặc tài chính qua email hoặc tin nhắn cho các đối tượng lạ. Ngoài các đơn vị ngân hàng, các tổ chức hoặc doanh nghiệp uy tín sẽ không yêu cầu cung cấp dữ liệu cá nhân.

Thứ năm là cảnh giác với những yêu cầu đặt cọc hoặc chuyển khoản. Tuyệt đối không chuyển tiền cho các đối tượng lạ trong mọi trường hợp. Đối với các giao dịch trực tiếp, người dân được khuyến cáo nên thực hiện trực tiếp hoặc thông qua cá nhân hoặc tổ chức trung gian uy tín.

Kỹ năng cuối cùng là tìm hiểu thêm về các hình thức lừa đảo phổ biến.Các loại hình lừa đảo qua mạng như lừa đảo qua email, tin nhắn, mạo danh và lừa đảo chiếm đoạt tài sản đã được phổ biến rất nhiều trên mạng. Hiểu biết về các phương thức này sẽ giúp dễ dàng nhận diện và phòng tránh hậu quả không đáng có.

**Các kỹ năng phòng tránh lừa đảo trực tuyến nâng cao**

Bên cạnh việc nâng cao nhận thức, người dùng cũng cần những kỹ năng nâng cao giúp phòng tránh lừa đảo trực tuyến một cách hiệu quả nhất, bao gồm:

Một là, bảo vệ thông tin cá nhân. Tránh chia sẻ quá nhiều thông tin, hình ảnh cá nhân trên các nền tảng mạng xã hội. Ẩn hết các thông tin cá nhân như địa chỉ, ngày tháng năm sinh, số điện thoại…). Khi đăng gì lên mạng xã hội nên cân nhắc kỹ và nên chia sẻ ở chế độ bạn bè.

Hai là, sử dụng mật khẩu dài và phức tạp. Đảm bảo mỗi tài khoản trực tuyến sở hữu mật khẩu mạnh, bao gồm chữ hoa, chữ thường, số và ký tự đặc biệt. Tránh sử dụng cùng một mật khẩu cho nhiều tài khoản

Ba là, thiết lập xác thực đa yếu tố (2FA). Kích hoạt xác thực đa yếu tố đối với các tài khoản trực tuyến. Điều này đồng nghĩa với việc bổ sung một lớp xác thực (thông qua tin nhắn, email hoặc cuộc gọi) ngoài mật khẩu nhằm gia tăng mức độ bảo mật cho tài khoản.

Bốn là, cập nhật phần mềm bảo mật. Cài đặt và thường xuyên cập nhật các phần mềm diệt virus, tường lửa, và các công cụ bảo mật khác để bảo vệ thiết bị khỏi các phần mềm có chứa mã độc và các mối đe dọa khác.

Năm là, kiểm tra và giám sát tài khoản tài chính. Theo dõi kỹ các giao dịch trên tài khoản ngân hàng và thẻ tín dụng để phát hiện bất kỳ giao dịch nào không hợp lệ.

Sáu là, sao lưu dữ liệu định kỳ. Sao lưu dữ liệu quan trọng thường xuyên để tránh mất dữ liệu trong trường hợp bị tấn công hoặc bị lừa đảo.

**Các cách thức của đối tượng lừa đảo trực tuyến**

Cách thức các đối tượng lừa đảo trực tuyến nhận tiền lừa đảo từ nạn nhân được Cẩm nang khuyến cáo bao gồm:

Chuyển khoản vào các tài khoản ngân hàng rác, các tài khoản không chính chủ được mua lại từ các đối tượng như sinh viên, hoặc các số tài khoản ngân hàng ảo;

Chuyển tiền qua các cổng thanh toán trực tuyến (Ví dụ như thanh toán mua thẻ điện thoại: cổng Ngân lượng, Bảo kim…);

Chuyển tiền qua các ví điện tử như Momo, ViettelPay, VNPay…; Chuyển tiền thông qua tiền ảo trên các sàn giao dịch.

**Cách xử lý khi bị lừa chuyển tiền qua mạng**

Theo Cẩm nang kỹ năng nhận diện và phòng chống lừa đảo trực tuyến của Cục An toàn thông tin xây dựng thuộc Bộ TT&TT thì không ít trường hợp nạn nhân nhẹ dạ cả tin, làm theo lời dẫn dụ của đối tượng lừa đảo và tự chuyển tiền vào tài khoản của các đối tượng này.

Trong trường hợp gặp phải tình huống tương tự, nạn nhân cần phải:

Dừng chuyển tiền: Tuyệt đối không tiếp tục làm theo lời dẫn dụ của đối tượng lừa đảo.

Liên hệ ngay lập tức với ngân hàng: Để báo cáo lừa đảo và yêu cầu họ dừng mọi giao dịch.

Sao lưu lịch sử giao tiếp, giao dịch: Nhanh chóng lưu lại các đoạn hội thoại với đối tượng lừa đảo, lịch sử giao dịch chuyển khoản nhằm phục vụ cho quá trình điều tra và truy vết đối tượng.

Trình báo: Trình báo vụ việc lừa đảo trực tuyến với các cơ quan chức năng như lực lượng công an địa phương.

Cảnh báo cho gia đình và bạn bè: Về trường hợp lừa đảo này để họ có thể đề phòng những chiêu trò tiếp theo có thể xảy ra.

*Xuân Nghĩa*