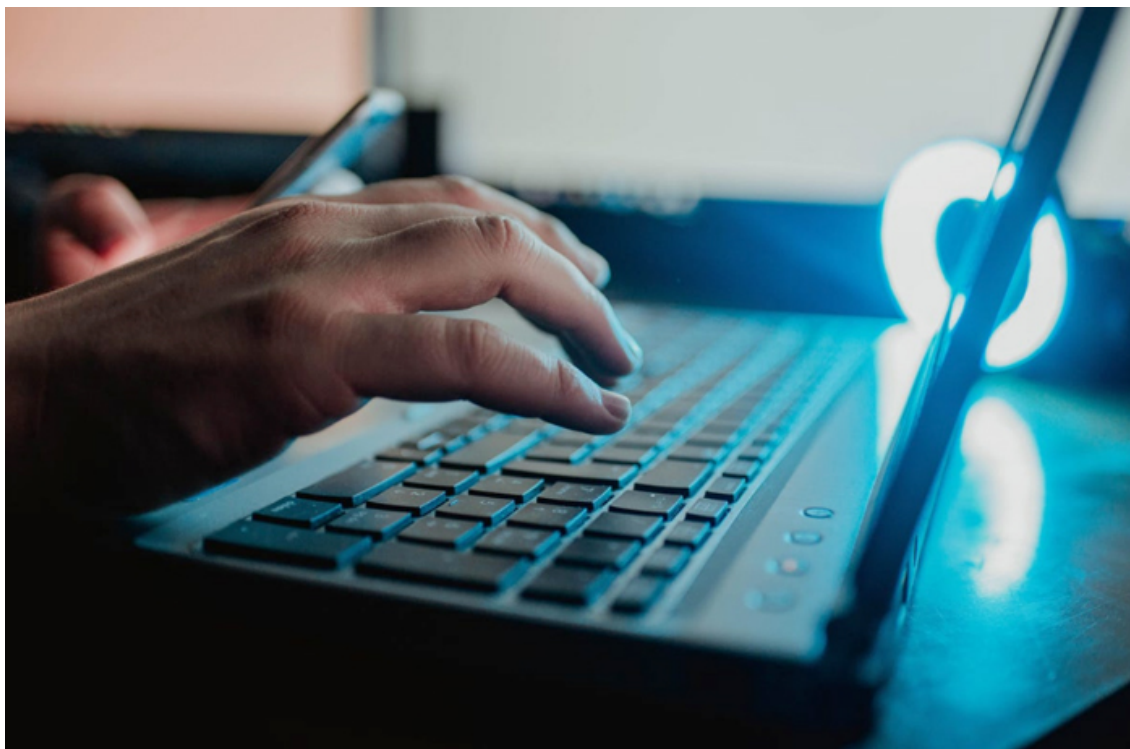


Năm chiêu trò lừa đảo trực tuyến dịp Tết Giáp Thìn 2024 cần chú ý

12:39 31/01/2024

Thời gian vừa qua, các vụ việc liên quan đến lừa đảo, chiếm đoạt tài sản trên không gian mạng đang diễn ra hết sức phức tạp, có xu hướng gia tăng, với các phương thức, thủ đoạn mới, tinh vi, khó lường và gây nhiều khó khăn cho các cơ quan chức năng trong việc phát hiện, điều tra, xử lý vi phạm.

Theo đó, Cục An toàn Thông tin, Bộ Thông tin và Truyền thông đã điểm ra 05 chiêu trò lừa đảo phổ biến trên Internet nhằm bảo vệ người dân khỏi những rủi ro không đáng có. Đồng thời, nội dung cũng sẽ cung cấp thêm kiến thức về lừa đảo không gian mạng: dấu hiệu nhận biết, hình thức thực hiện và biện pháp phòng tránh để giúp người dân nâng cao cảnh giác khi đối mặt với các tình huống lừa đảo không gian mạng.



Ảnh minh họa

Lừa đảo mua vé máy bay, du lịch giá rẻ dịp lễ, Tết

Nhu cầu đi du lịch dịp nghỉ Tết Nguyên đán của người dân tăng mạnh khiến cho các chuyến bay có thể hết chỗ sớm hơn dự kiến. Lợi dụng tình trạng này, các đối tượng đã lừa đảo, chiếm đoạt tài sản của người dân.

Cục An toàn Thông tin khuyến cáo người dân cảnh giác khi thực hiện giao dịch trên mạng xã hội, nhất là với các quảng cáo giá siêu rẻ và ưu đãi lớn. Khi có nhu cầu mua vé máy bay, người dân nên trực tiếp đặt vé qua website chính của hãng hàng không hoặc gọi trực tiếp lên tổng đài.

Trước khi thực hiện giao dịch, cần tìm hiểu kỹ, xác nhận thông tin mã vé và kiểm tra có hiệu lực, đồng thời yêu cầu nhân viên của hãng soát lại thông tin hành trình bay, hành khách bay. Đặc biệt, người dân không nên giao dịch qua bên trung gian thứ ba hay các đại lý khi không rõ về chất lượng, độ uy tín.

Lừa đảo việc làm thêm trên mạng xã hội

Lợi dụng tâm lý của nhiều người muốn kiếm thêm thu nhập để có chi phí trang trải dịp Tết, một số đối tượng áp dụng chiêu lừa đảo tuyển dụng lao động thời vụ, làm việc tại nhà với mức lương hấp dẫn. Do thiếu thông tin và nôn nóng muốn kiếm tiền, nhiều người đã “sập bẫy” để rồi không chỉ mất tiền và thời gian mà còn chịu gánh nặng về tâm lý. Các đối tượng thường nhắm đến nạn nhân là các ‘mẹ bỉm sữa’, học sinh, sinh viên, người lao động có thu nhập trung bình - thấp... có nhu cầu tìm việc làm thêm.

Khuyến cáo của Cục An toàn Thông tin là người dân nên cẩn trọng với các lời giới thiệu việc làm trên mạng xã hội; cần tìm hiểu kỹ về người giới thiệu và chính sách của công ty mà đối tượng nhắc tới; không nên quá tin tưởng vào những đề nghị quá hấp dẫn và những công việc dễ dàng, không quan trọng trình độ hay kỹ năng. Tuyệt đối không đặt cọc cho các đối tượng dưới bất cứ hình thức nào khi chưa nắm bắt rõ ràng thông tin và mức độ uy tín.

Có nhu cầu tìm việc, người dân nên tìm đến các văn phòng, công ty có uy tín hoặc các trang web chính thống của họ. Người dân cũng cần đặc biệt lưu ý không cung cấp thông tin cá nhân, số tài khoản ngân hàng hay mã OTP cho bất kỳ ai và dưới bất kỳ hình thức nào.

Giả danh công an, luật sư hỗ trợ nạn nhân lấy lại tiền đã mất

Gần đây, trên Facebook xuất hiện nhiều tài khoản mạo danh các lãnh đạo, cán bộ thuộc cơ quan chức năng, văn phòng luật cung cấp dịch vụ hỗ trợ các nạn nhân bị lừa đảo qua mạng.

Đánh vào tâm lý muốn lấy lại tiền đã mất của những người từng bị lừa đảo, các đối tượng đã giả danh cán bộ làm an ninh mạng để hỗ trợ thu hồi tiền lừa đảo.

Một số đối tượng giới thiệu sẽ hỗ trợ thu hồi tiền bị lừa, cam kết lấy lại được tiền với thủ tục nhanh chóng hiệu quả thủ tục đơn giản hơn nhiều so với việc đến cơ quan công an trình báo.

Sau đó, các đối tượng hướng dẫn và yêu cầu nạn nhân đóng phí để hỗ trợ hoặc làm nhiệm vụ để rút tiền treo trên hệ thống khi có người chuyển tiền, các đối tượng thông báo tài khoản ngân hàng bị lỗi và không cho rút tiền về.

Cục An toàn Thông tin đề nghị người dân, đặc biệt là những người dân đã trở thành nạn nhân của các đối tượng lừa đảo, phải nâng cao cảnh giác. Trường hợp nhận được cuộc gọi nghi ngờ mạo danh, người dân có thể ghi âm cuộc gọi, lưu lại số điện thoại và thông báo kịp thời cho cơ quan công an nơi gần nhất để trình báo vụ việc.

Người dân cũng cần thường xuyên cập nhật và nắm bắt thông tin về vấn đề an toàn không gian mạng; luôn cảnh giác với những lời mời chào trên mạng xã hội; tuyệt đối không cung cấp các thông tin cá nhân để tránh bị đánh cắp thông tin sử dụng cho mục đích phi pháp.

Lừa đảo vay tiền qua ứng dụng "tín dụng đen"

Lợi dụng ưu điểm nhanh gọn, thuận tiện của hình thức vay trực tuyến, các đối tượng lừa đảo vay tiêu dùng ngày càng có nhiều thủ đoạn tinh vi đánh vào tâm lý nhẹ dạ cả tin, thiếu thông tin của người dân.

Các app "tín dụng đen" đa phần đều được quảng cáo là lãi suất thấp, giải ngân nhanh, thậm chí có nơi còn cho vay ưu đãi 0% hoặc thủ tục vay không cần tài sản thế chấp.

Tuy nhiên, thực tế đây là hình thức vay nhanh thanh toán ngắn trong vòng 7 đến 10 ngày với lãi suất rất cao.

Các đối tượng thường dùng mạng xã hội Zalo hoặc Facebook nhắn tin điều hành giao dịch việc cho vay và thu hồi nợ; thẩm duyệt hồ sơ khách hàng bằng cách yêu cầu cung cấp thông tin cá nhân.

Để thuận tiện cho việc đòi nợ, các ứng dụng yêu cầu người vay nợ cho phép truy cập vào danh bạ điện thoại, tài khoản mạng xã hội, chụp ảnh nhận diện, ảnh chứng minh nhân dân hoặc căn cước công dân.

Đến hạn thanh toán mà người dân không trả hoặc chậm trả lãi, đối tượng sẽ truy cập vào điện thoại hoặc quay sang đòi nợ những người trong danh bạ; gửi tin nhắn đe dọa, xúc phạm... nhằm gây áp lực ép người vay phải trả tiền.

Trước tình trạng trên, Cục An toàn Thông tin khuyến nghị người dân nên tìm đến các tổ chức cho vay uy tín như ngân hàng hoặc các công ty tài chính hợp pháp; không cung cấp thông tin cá nhân hoặc tài khoản ngân hàng trên các website hoặc ứng dụng không đáng tin cậy; đặc biệt là không để bên cho vay truy cập tài khoản và danh bạ điện thoại cá nhân.

Khi cài đặt ứng dụng, nhất là ứng dụng tài chính, người dân nên xem xét cẩn thận các quyền mà ứng dụng yêu cầu cũng như đọc kỹ các điều khoản, chính sách của ứng dụng này. Trường hợp phát hiện điểm đáng nghi, cần ngay lập tức hủy cài đặt ứng dụng.

Chiêu lừa đảo "nhận quà trúng thưởng"

Lừa đảo chiếm đoạt thông qua hình thức "nhận quà trúng thưởng" là một chiêu trò không còn mới. Các đối tượng thường liên hệ với nạn nhân thông qua hình thức gọi điện thông báo trúng thưởng và thường sẽ thiên biến theo nhiều cách thức khác nhau như: Gọi điện thông báo trúng thưởng, mua hàng để nhận mã trúng thưởng, nhắn tin trúng thưởng qua Facebook.

Cùng với việc chỉ rõ các bước lừa đảo người dùng của từng cách thức nêu trên, Cục An toàn Thông tin khuyến cáo người dân không làm theo hướng dẫn của đối tượng khi chưa xác minh được danh tính; không truy cập vào các đường link lạ hoặc tải các ứng dụng lạ; không cung cấp thông tin cá nhân cho bất kỳ đối tượng nào qua mọi hình thức.

Người dân cũng cần tìm hiểu kỹ về đối tượng gọi đến, yêu cầu họ cung cấp đầy đủ thông tin về họ tên, chức vụ, đơn vị công tác, địa chỉ, số điện thoại (nếu bên tặng thưởng là cá nhân); tên công ty, địa chỉ cụ thể, số điện thoại, mã số thuế, giấy phép đăng ký kinh doanh (nếu bên tặng thưởng là doanh nghiệp) để tìm hiểu, tra cứu và xác minh.

Ngoài ra, người dân cần liên hệ với các cơ quan có thẩm quyền để được giải đáp và hỗ trợ kịp thời về chương trình khuyến mãi, trao thưởng.

Cục An toàn Thông tin cũng khuyến nghị người dân theo dõi và cập nhật các thông tin, tình huống thông tin, tình huống, dấu hiệu về lừa đảo trực tuyến tại **Cổng không gian mạng quốc gia (<https://khonggianmang.vn>)**

Nếu phát hiện dấu hiệu lừa đảo, người dân hãy gửi phản ánh về địa chỉ của trang ***Cảnh báo an toàn thông tin Việt Nam*** (<https://canhbao.khonggianmang.vn>).

Minh Đức