TẠP CHÍ ĐIỆN TỬ
THƯƠNG HIỆU & CÔNG LUẬN

Cảnh báo hàng loạt chiêu trò lừa đảo du lịch nhân dịp nghỉ lễ

10:17 28/04/2024

Lợi dụng kỳ nghỉ lễ 30/4 và 1/5 năm nay kéo dài, các đối tượng thực hiện hàng loạt các chiêu trò lừa đảo du lịch khác nhau nhằm chiếm đoạt tài sản người dùng. Bộ Thông tin và Truyền thông đã chỉ ra 5 dấu hiệu để nhận biết lừa đảo du lịch, đồng thời cảnh báo các nhà hàng cũng bị lừa đảo bằng chiêu trò đặt tiệc, nhờ mua rượu, thực phẩm cho khách sử dụng...

Cùng nhìn lại cảnh báo lừa đảo trực tuyến trong tuần qua (22 đến 28/4) của Cục An toàn thông tin, Bộ Thông tin và Truyền thông.

CẢNH BÁO CHIÊU TRÒ LỪA ĐẢO DU LỊCH DỊP LỄ 30/4 - 1/5

Cảnh báo hàng loạt chiêu trò lừa đảo du lịch nhân dịp nghỉ lễ ảnh 1

Vào dịp lễ 30/4 và 1/5, nhu cầu sử dụng các dịch vụ của người dân tăng cao, lợi dụng thời điểm này, tội phạm lừa đảo có thể sẽ xuất hiện với nhiều "chiêu lừa" mới.

Theo Cục An toàn thông tin (Bộ Thông tin và Truyền thông), kỳ nghỉ lễ năm nay kéo dài hơn mọi năm nên người dân có nhiều kế hoạch, dự định đi du lịch, nghỉ dưỡng. Lợi dụng thời điểm này, các đối tượng thực hiện hàng loạt các chiêu trò lừa đảo du lịch khác nhau nhằm chiếm đoạt tài sản người dùng.

Một, đối tượng làm giả ảnh chụp biên lai, hóa đơn thanh toán cùng con dấu của công ty. Sau khi khách hàng chuyển khoản để thanh toán dịch vụ du lịch, các đối tượng sẽ chặn liên lạc và xóa mọi dấu vết.

Hai, đối tượng chạy quảng cáo những bài đăng với nội dung bán tour du lịch, phòng khách sạn giá rẻ, nhiều ưu đãi kèm theo. Khi có nạn nhân tiếp cận, đối tượng mời chào và đề nghị nạn nhân chuyển tiền đặt cọc (30-50% giá trị). Sau khi đặt cọc, các đối tượng sẽ yêu cầu nạn nhân tự khai thông tin, hoàn thiện hồ sơ... nhằm đánh cắp thông tin cá nhân của người dùng và chiếm đoạt tài sản.

Ba, đối tượng dẫn dụ nạn nhân bằng chiêu trò đăng bài viết quảng cáo dịch vụ làm visa (thị thực) du lịch nước ngoài, cam kết tỷ lệ thành công cao, hoàn trả 100% số tiền nếu không xin được visa. Sau khi nạn nhân chuyển khoản thanh toán chi phí hoặc một phần chi phí, các đối tượng sẽ để nạn nhân tự khai thông tin tờ khai, hoàn thiện hồ sơ... Sau đó, đối tượng lấy lý do nạn nhân khai thông tin bị thiếu và không trả lại tiền.

Bốn, mạo danh đại lý bán vé máy bay, tạo lập những website/fanpage của các công ty du lịch uy tín, mạo danh đại lý vé máy bay, tạo các website, trang mạng xã hội, địa chỉ đường dẫn, thiết kế tương tự website thật của hãng.

Năm, nhiều người dân có thói quen đặt vé online phục vụ nhu cầu đi du lịch, về quê,... dẫn đến tình trạng nhiều trường hợp bị lừa đảo chiếm đoạt. Một số khách hàng mua vé nhận được thẻ lên tàu bị cạo sửa thông tin như giá vé, đối tượng khuyến mãi, ngày đi tàu, ga đi ga đến... nên không có giá trị đi tàu.

Trước tình trạng trên, Cục An toàn thông tin (Bộ Thông tin và Truyền thông) khuyến cáo người dân cần nâng cao cảnh giác khi gặp các trường hợp trên. Người dân cần tìm hiểu kỹ thông tin khi lựa chọn các gói du lịch; nên lựa chọn dịch vụ đặt tour, phòng khách sạn, vé máy bay của những công ty hoặc ứng dụng du lịch uy tín; lựa chọn các trang mạng xã hội có dấu tích xanh (tài khoản đã đăng ký).

Người dân có thể đề nghị phía đối tác cho xem giấy phép hoạt động kinh doanh, giấy tờ, chứng chỉ hành nghề... của công ty lữ hành, du lịch. Cảnh giác với các gói du lịch, phòng khách sạn, vé máy bay có mức giá quá rẻ.

Chú ý các dấu hiệu nhận biết website giả mạo thông qua tên miền. Thông thường tên miền các website giả sẽ gần giống với tên các website thật nhưng sẽ có thêm một số ký tự. Sau khi đặt phòng khách sạn hoặc vé máy bay, cần xác nhận lại thông tin đặt phòng (từ khách sạn đã đặt), thông tin vé máy bay (từ hãng).

Đồng thời, các doanh nghiệp thuộc lĩnh vực cần cảnh giác phát hiện các trang web, tài khoản giả mạo doanh nghiệp, kịp thời tố cáo đến cơ quan chức năng để ngăn chặn xử lý.

Khi phát hiện các hành vi có dấu hiệu lừa đảo, người dân nhanh chóng trình báo cơ quan công an gần nhất để xử lý theo đúng pháp luật.

CẢNH BÁO HÌNH THỨC LỪA ĐẢO ĐẶT TIỆC, ĐẶT NHÀ HÀNG DỊP NGHỈ LỄ ĐỂ CHIẾM ĐOẠT TIỀN ĐẶT CỌC

Cảnh báo hàng loạt chiêu trò lừa đảo du lịch nhân dịp nghỉ lễ ảnh 2

Thời gian gần đây, một số nhà hàng và dịch vụ nấu ăn trên địa bàn thành phố Đà Nẵng bị các đối tượng lừa đảo, chiếm đoạt hàng trăm triệu đồng bằng chiêu trò đặt tiệc, nhờ mua rượu, thực phẩm cho khách sử dụng...

Hàng loạt các đối tượng sử dụng tài khoản mạng xã hội liên hệ nhà hàng A.L.B trên địa bàn quận Ngũ Hành Sơn đặt tiệc tiếp khách. Sau khi thống nhất các món ăn, "khách hàng" yêu cầu nhà hàng chuẩn bị rượu vang để sử dụng và đặt số lượng lớn loại nước uống hồng sâm của Hàn Quốc làm quà tặng cho khách dự tiệc.

Sau khi được nhân viên nhà hàng liên hệ, nhận báo giá của cửa hàng rồi thông báo lại cho "khách hàng". Đồng thời bảo "khách hàng", chốt đặt đơn hàng, nhân viên nhà hàng đề nghị đối tượng chuyển tiền để nhà hàng mua rượu và hồng sâm, tuy nhiên, đến gần thời gian đặt tiệc, đối tượng lại gửi biên lai hóa đơn giả.

Dù chưa nhận được tiền nhưng do tin tưởng, nhà hàng chuyển số tiền đặt hàng cho phía cửa hàng bán rượu và hồng sâm. Tuy nhiên sau đó, chẳng có khách nào đến nhà hàng dự tiệc, rượu và hồng sâm đặt giúp cũng không ai mang đến. Trong khi đó, qua kiểm tra, phát hiện "khách vip" cũng như đại diện cửa hàng hồng sâm đã chặn tin nhắn của nhà hàng và xóa kết bạn.

Để phòng ngừa, ngăn chặn loại tội phạm với phương thức, thủ đoạn nêu trên, Cục An toàn thông tin (Bộ Thông tin và Truyền thông) khuyến cáo người dân và các nhà hàng, cơ sở dịch vụ ăn uống, cơ sở lưu trú cần nâng cao ý thức cảnh giác, kiểm tra kỹ để tránh bị lừa đảo; đồng thời chia sẻ, cảnh báo với người thân, bạn bè về thủ đoạn phạm tội trên.

Các cơ sở kinh doanh ăn uống, nhà hàng biết phương thức, thủ đoạn tội phạm nhằm nêu cao tinh thần cảnh giác tội phạm khi thực hiện yêu cầu của khách đặt tiệc qua mạng viễn thông, mạng xã hội.

Người dân tuyệt đối không nhận chuyển khoản hay thanh toán hộ cho những đối tượng không rõ danh tính; kiểm tra kỹ nội dung biên lai và chỉ nên thực hiện khi chắc chắn tài khoản của mình nhận được tiền của đối tượng.

Khi phát hiện các hành vi có dấu hiệu lừa đảo, người dân nhanh chóng trình báo cơ quan công an gần nhất để xử lý theo đúng pháp luật.

CẢNH BÁO LỪA ĐẢO BẰNG CÔNG NGHỆ DEEPFAKE

Cảnh báo hàng loạt chiêu trò lừa đảo du lịch nhân dịp nghỉ lễ ảnh 3

Deepfake đã trở thành mối đe dọa đối với không gian mạng tại Việt Nam, nơi tội phạm mạng thường sử dụng các cuộc gọi video deepfake để mạo danh một cá nhân và vay mượn người thân, bạn bè của họ những khoản tiền lớn cho những trường hợp cấp bách.

Đối tượng làm giả/chiếm đoạt tài khoản của người dùng mạng xã hội, liên lạc với người thân trong danh sách bạn bè cho biết đang bị mắc kẹt khi du lịch tại nước ngoài và cần một khoản tiền ngay lập tức.

Sử dụng công nghệ deepfake (công nghệ ứng dụng trí tuệ nhân tạo để tạo ra các đoạn video với hình ảnh, khuôn mặt nhân vật giống hệt như hình ảnh của người mà các đối tượng muốn giả mạo) và thực hiện cuộc gọi video (hình ảnh) để nạn nhân tưởng rằng đang nói chuyện với người thân của mình và nhu cầu vay tiền là có thật, từ đó chuyển tiền cho các đối tượng.

Trước tình trạng trên, Cục An toàn thông tin (Bộ Thông tin và Truyền thông) khuyến cáo người dùng có thể dùng chính các công cụ AI để nhận diện deepfake nhằm giảm thiểu xác suất thành công của các vụ lừa đảo như Intel FakeCatcher, Microsoft Video Authenticator…

Đối với video deepfake, một số công cụ giúp nhận diện sự chuyển động không khớp giữa khuôn miệng và lời thoại. Một số công cụ phát hiện lưu lượng máu bất thường dưới da bằng cách phân tích độ phân giải của video vì khi tim bơm máu, tĩnh mạch của con người sẽ đổi màu. Người dùng có thể phát hiện deepfake nhờ vào hình mờ đánh dấu tác giả.

Người dùng cần đặc biệt nâng cao cảnh giác, không cung cấp thông tin cá nhân như căn cước công dân, tài khoản ngân hàng, mã OTP và không chuyển tiền cho người lạ qua điện thoại, mạng xã hội, các trang web có dấu hiệu lừa đảo. Khi có yêu cầu vay/chuyển tiền vào tài khoản qua mạng xã hội, nên thực hiện các phương thức xác thực khác như gọi điện thoại truyền thống hay sử dụng các kênh liên lạc khác để xác nhận lại.

CẢNH BÁO THỦ ĐOẠN LỪA ĐẢO VỀ CHÍNH SÁCH BẢO HIỂM XÃ HỘI

Lợi dụng lòng tin của người dân vào chính sách Bảo hiểm xã hội, Bảo hiểm Y tế (BHXH, BHYT), một số đối tượng đã giả danh là người của cơ quan BHXH Việt Nam nhằm lừa đảo, chiếm đoạt tài sản của người dân khi làm các thủ tục liên quan đến BHXH, BHYT.

Một trong những trường hợp bị lừa đảo hình thức trên, anh NTT - trú tại phường Hiệp Thành (quận 12, Thành phố Hồ Chí Minh) về việc truy cập mạng xã hội và bị đối tượng mạo danh là nhân viên BHXH lừa đảo chuyển tiền để được giảm trùng BHXH, cắt giảm quá trình đóng trùng và hủy bỏ sổ BHXH.

Theo phản ánh của anh T, anh đã cho em trai mượn hồ sơ nhân thân của mình để đóng BHXH. Sau đó, anh T truy cập mạng xã hội Facebook và nhắn tin thông qua Messenger tài khoản có tên Phạm Ngọc Anh (hiện đối tượng này đã khóa tài khoản) – đối tượng này mạo danh là nhân viên BHXH hỗ trợ tạo nộp và giải quyết các loại hồ sơ bảo hiểm.

Qua trao đổi, tài khoản Facebook Phạm Ngọc Anh nhận giải quyết được cho anh T. và yêu cầu phí là 900.000 đồng. Cả tin, anh T đã cung cấp thông tin cá nhân, ảnh chụp CCCD và sổ BHXH.

Đối tượng lừa đảo đã gửi cho anh T hình ảnh tiếp nhận hồ sơ, có đóng dấu đỏ, chữ ký xác nhận của người có tên "Nguyễn Vinh Quang - Phó Giám đốc BHXH Việt Nam (đây là tên mạo danh, BHXH Việt Nam không có chức danh này). Tin tưởng, anh T đã chuyển tiền 2 lần vào tài khoản của đối tượng và sau đó, anh T nhắn tin hỏi kết quả, thì đối tượng đã khóa tài khoản, lúc này anh T mới tìm đến Fanpage BHXH Việt Nam nhắn tin trao đổi thì biết mình bị lừa.

Theo Cục An toàn thông tin (Bộ Thông tin và Truyền thông), tất cả các dịch vụ mà BHXH Việt Nam đang triển khai, người dân đều không phải trả phí.

Đây không phải lần đầu xuất hiện các đối tượng lừa đảo hình thức trên. Cục An toàn thông tin (Bộ Thông tin và Truyền thông) khuyến cáo người dân khi thực hiện các thủ tục hành chính về BHXH, BHYT cần nâng cao cảnh giác hơn nữa để phòng tránh bị đối tượng xấu lợi dụng, lừa đảo.

Bên cạnh đó, người dân cũng cần tăng cường trau dồi kiến thức về pháp luật, chính sách BHXH, BHTN, BHYT; thường xuyên theo dõi các thông báo của cơ quan chức năng về phương thức thủ đoạn phạm tội, lừa đảo trên các phương tiện thông tin đại chúng.

Trường hợp khi thực hiện các thủ tục hành chính của ngành BHXH Việt Nam, nếu có vướng mắc thì liên hệ trực tiếp với cơ quan công an gần nhất để được hỗ trợ. Đồng thời, liên hệ Trung tâm Dịch vụ hỗ trợ, chăm sóc khách hàng qua số hotline: 1900.9068 hoặc số 0243.7899999 (trong giờ hành chính) để được hỗ trợ.

Hiện nay, BHXH Việt Nam chỉ có 1 trang Fanpage đã được cấp tích xanh của Facebook tại địa chỉ: https://www.facebook.com/baohiemxahoi.gov.vn, người

dùng cần lưu ý để tránh các trang giả mạo.

MƯỢN DANH QUYÊN GÓP TỪ THIỆN, CHIẾM ĐOẠT HÀNG CHỤC TỶ ĐỒNG

Cảnh báo hàng loạt chiêu trò lừa đảo du lịch nhân dịp nghỉ lễ ảnh 6

Chiều 24/4, Cơ quan Cảnh sát điều tra Công an thành phố Đà Nẵng tống đạt Quyết định khởi tố vụ án, khởi tố bị can và ra Lệnh bắt bị can để tạm giam đối với Lê Đình Hải (26 tuổi, trú phường Bình Trị Đông, quận Bình Tân, thành phố Hồ Chí Minh) về tội Lừa đảo chiếm đoạt tài sản.

Trước đó, qua công tác nắm tình hình trên không gian mạng, Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (gọi tắt là Phòng An ninh mạng), Công an thành phố Đà Nẵng phát hiện trên mạng xã hội Facebook xuất hiện các tài khoản như: "Một Lòng Hướng Phật - Ni Sư Chức Từ", "Phật Pháp Nhiệm Màu - Ni Sư Nhân Độ", "Ni sư Tâm Phúc", "Phật Pháp Nhiệm Mầu - Ni Sư Tâm Hạ"... thường xuyên đăng tải hình ảnh những hoàn cảnh đáng thương (tai nạn, bệnh hiểm nghèo, người già neo đơn, trẻ em mồ côi cha, mẹ...), kèm theo là các bài viết kêu gọi quyên góp từ thiện vào nhiều tài khoản ngân hàng cá nhân.

Tại cơ quan công an, cùng với các tài liệu, dữ liệu điện tử thu thập được, Lê Đình Hải thừa nhận hành vi lừa đảo chiếm đoạt tiền từ thiện của mình. Tiến hành khám xét nơi ở của đối tượng, lực lượng công an thu giữ nhiều tài liệu chứng minh hành vi phạm tội.

Trước hiện trang trên, Cục An toàn thông tin (Bộ Thông tin và Truyền thông) khuyến cáo người dân nên tìm hiểu kỹ về các hoạt động từ thiện và hỗ trợ trên mạng xã hội. Đây là một hiện trạng đáng lên án khi lợi dụng lòng tốt của những nhà hảo tâm để chuộc lợi, gây mất niềm tin của người dân đối với các hoạt động thiện nguyện thật.

Do đó, để lòng tốt được trao gửi đúng chỗ, những người có tấm lòng thiện nguyện nên lựa chọn các quỹ, chương trình từ thiện do Nhà nước, đoàn thể, quỹ xã hội, quỹ từ thiện được cơ quan có thẩm quyền cấp phép đứng ra tổ chức. Trường hợp có nghi ngờ về hoạt động lừa đảo, chiếm đoạt tài sản, cần báo cho cơ quan Công an gần nhất để kịp thời xử lý.

Cảnh báo hàng loạt chiêu trò lừa đảo du lịch nhân dịp nghỉ lễ ảnh 7

Chương trình Phát triển Liên hợp quốc (UNDP) đang điều tra một cuộc tấn công mạng sau khi các tác nhân đe dọa vi phạm hệ thống CNTT của mình để đánh

cắp dữ liệu nguồn nhân lực.

UNDP, mạng lưới phát triển toàn cầu của Liên hợp quốc, hoạt động tại hơn 170 quốc gia và vùng lãnh thổ và dựa vào sự đóng góp từ các quốc gia thành viên Liên hợp quốc và các tổ chức khu vực tư nhân/đa phương để giúp xóa đói giảm nghèo và chống lại sự bất bình đẳng và loại trừ.

Vào ngày 27/3, UNDP đã nhận được thông báo tình báo đe dọa rằng một tác nhân tống tiền dữ liệu đã đánh cắp dữ liệu bao gồm một số thông tin nhân sự và mua sắm nhất định. Các hành động ngay lập tức được thực hiện để xác định nguồn tiềm năng và chứa máy chủ bị ảnh hưởng cũng như xác định chi tiết cụ thể của dữ liệu bị lộ và ai bị ảnh hưởng.

Trong khi cơ quan Liên hợp quốc vẫn chưa liên kết cuộc tấn công với một nhóm đe dọa cụ thể, băng đảng ransomware 8Base đã thêm một mục nhập UNDP mới vào trang web rò rỉ dữ liệu web đen của mình vào ngày 27/3.

Những kẻ tấn công nói rằng các tài liệu mà các nhà khai thác của họ quản lý để lọc ra trong quá trình vi phạm có chứa một lượng lớn thông tin nhạy cảm. Các tệp mà họ tạm thời rò rỉ thông qua một liên kết hiện đã hết hạn được cho là bao gồm "một lượng lớn thông tin bí mật", dữ liệu cá nhân, dữ liệu kế toán, chứng chỉ, hợp đồng lao động, thỏa thuận bảo mật, hóa đơn, biên lai,...

8Base xuất hiện vào tháng 3/2022 và vào tháng 5/2023 băng đảng đã ra mắt trang web rò rỉ dữ liệu cùng với tuyên bố rằng những người thử nghiệm bút "trung thực và đơn giản" nhắm mục tiêu "các công ty đã bỏ qua quyền riêng tư và tầm quan trọng của dữ liệu của nhân viên và khách hàng của họ."

Cho đến nay, nhóm ransomware này đã liệt kê hơn 350 nạn nhân trên trang web của mình, công bố tối đa sáu nạn nhân cùng một lúc trong một số ngày.

Trước thông tin trên, Cục An toàn thông tin (Bộ Thông tin và Truyền thông) khuyến cáo người dân cần có những biện pháp bảo vệ thông tin cá nhân của bản thân trên không gian mạng. Đồng thời, khi đọc chính sách quyền riêng tư của ứng dụng, điều quan trọng, nên kiểm tra xem ứng dụng có tôn trọng quyền của người dùng hay không và liệu ứng dụng chỉ thu thập dữ liệu mà họ được cấp quyền hay không. Ngoài ra, hãy đảm bảo rằng người dùng có thể liên hệ với bộ phận dịch vụ khách hàng và yêu cầu họ xóa thông tin cá nhân.

Bên cạnh đó, người dùng nên hạn chế cấp quyền truy cập dữ liệu của ứng dụng; cân nhắc việc giới hạn quyền truy cập vào nguồn dữ liệu cá nhân như hình ảnh, danh bạ, vị trí, bộ phận thu âm thanh đối với những ứng dụng có thể hoạt động mà không cần đến nguồn thông tin này. Sử dụng các giải pháp bảo mật để chặn

các ứng dụng truy cập thông tin cá nhân, cảnh báo người dùng nếu số điện thoại và dữ liệu của họ bị rò rỉ cũng như cảnh báo họ nếu tệp độc hại đã được tải xuống trên các thiết bị.

CISCO CẢNH BÁO VỀ CÁC CUỘC TẤN CÔNG QUY MÔ LỚN NHẰM VÀO DỊCH VỤ VPN

Cảnh báo hàng loạt chiêu trò lừa đảo du lịch nhân dịp nghỉ lễ ảnh 9

Cisco cảnh báo về một chiến dịch ép buộc thông tin xác thực quy mô lớn nhắm vào các dịch vụ VPN và SSH trên các thiết bị Cisco, CheckPoint, Fortinet, SonicWall và Ubiquiti trên toàn thế giới.

Cuộc tấn công là quá trình cố gắng đăng nhập vào tài khoản hoặc thiết bị bằng nhiều tên người dùng và mật khẩu cho đến khi tìm thấy sự kết hợp chính xác. Khi họ có quyền truy cập vào thông tin đăng nhập chính xác, các tác nhân đe dọa sau đó có thể sử dụng chúng để chiếm quyền điều khiển thiết bị hoặc truy cập vào mạng nội bộ.

Theo Cisco Talos, chiến dịch brute force mới này sử dụng kết hợp tên người dùng nhân viên hợp lệ và chung chung liên quan đến các tổ chức cụ thể. Các nhà nghiên cứu cho biết các cuộc tấn công bắt đầu vào ngày 18/3/2024, trong khi tất cả các cuộc tấn công đều bắt nguồn từ các nút thoát TOR và nhiều công cụ và proxy ẩn danh khác, mà các tác nhân đe dọa sử dụng để trốn tránh các khối.

Tùy thuộc vào môi trường mục tiêu, các cuộc tấn công thành công thuộc loại này có thể dẫn đến truy cập mạng trái phép, khóa tài khoản hoặc các điều kiện từ chối dịch vụ.

Một số dịch vụ được sử dụng để thực hiện các cuộc tấn công bao gồm TOR, VPN Gate, IPIDEA Proxy, BigMama Proxy, Space Proxy, Nexus Proxy và Proxy Rack. Hoạt động độc hại thiếu sự tập trung cụ thể vào các ngành hoặc khu vực cụ thể, cho thấy một chiến lược rộng lớn hơn về các cuộc tấn công ngẫu nhiên, cơ hội.

Nhóm Talos đã chia sẻ một danh sách đầy đủ các chỉ số thỏa hiệp (IoC) cho hoạt động này trên GitHub, bao gồm địa chỉ IP của kẻ tấn công để đưa vào danh sách chặn và danh sách tên người dùng và mật khẩu được sử dụng trong các cuộc tấn công bạo lực.

Trước thông tin trên, Cục An toàn thông tin (Bộ Thông tin và Truyền thông) khuyến cáo người dân nên bật tính năng Firewall Posture (HostScan). Người dùng cần nâng cao kiến thức về các hình thức tấn công mạng, nhận biết dấu

hiệu như số lượng yêu cầu xác thực bất thường được ghi lại bởi nhật ký hệ thống.

Theo Báo Nhân Dân