Phụ lục

Một số thông tin về tội phạm mạng trong nước sử dụng để lừa đảo trực tuyến và khuyến nghị người dân cách phòng tránh

1. Cảnh báo chiêu trò lừa đảo từ thiện, quyên góp ủng hộ đồng bào vùng lũ lụt.

Vừa qua, bão số 3 (bão Yagi) đã gây mưa lớn, lũ quét, ngập lụt, sạt lở đất trên diện rộng tại các tỉnh miền Bắc. Lợi dụng tình hình đó, nhiều đối tượng xấu đã mạo danh Hội Chữ thập đỏ, các tổ chức từ thiện uy tín kêu gọi quyên góp nhằm chiếm đoạt số tiền của người dân ủng hộ đồng bào gặp thiên tai.

Nhiều đối tượng giả mạo cơ quan nhà nước hoặc các tổ chức uy tín đưa ra các thông tin sai lệch về tình hình bão lũ tại các tỉnh miền Bắc, từ đó kêu gọi quyên góp, ủng hộ cho các gia đình bị ảnh hưởng bởi thiên tai. Các đối tượng lừa đảo sử dụng hình ảnh, thông tin giống các trang chính thống để kêu gọi những người hảo tâm quyên góp, chuyển tiền vào tài khoản cá nhân để chiếm đoạt. Thậm chí, các đối tượng đánh vào sự quan tâm của người dân đối với tin tức liên quan đến tình hình bão lũ, các đối tượng đã phát tán thôngtin giả mạo, tin tức sai sự thật trên các trang mạng xã hội về tình hình lũ lụt.

Trước thực trạng lừa đảo diễn ra,Cục An toàn thông tin (Bộ TT&TT) khuyến cáo người dân trước khi quyên góp,ủng hộ, cần tìm hiểu kỹ về tổ chức kêu gọi, xác minh tính xác thực của thông tin được cung cấp. Trong trường hợp người có tấm lòng hảo tâm, chia sẻ với những khó khăn của đồng bào trong vùng thiên tai thì nên quyên góp, ủng hộ tại các đơn vị có uy tín, minh bạch, đảm bảo sự đóng góp của mình thực sự có ý nghĩa.Nếu phát hiện hoặc nghi ngờ về ứng dụng hoặc dịch vụ đọc trộm tin nhắn, cầnbáo cáo ngay cho cơ quan chức năng để có biện pháp ngăn chặn kịp thời.

2. Cảnh báo mạo danh cắt ghép hình ảnh của các bệnh viện để lừa đảo chiếm đoạt tài sản.

Lợi dụng nhu cầu làm đẹp của người dân ngày càng cao, các đối tượng không ngừng mạo danh bác sĩ thẩm mỹ của Bệnh viện Chợ Rẫy để tạo lòng tin với khách hàng nhằm trục lợi bất chính.

Cụ thể, thời gian gầnđây, bệnh viện Chợ Rẫy tiếp tục phát hiện thêm 1 trang fanpage giả mạo tự xưng là bác sĩ Trưởng khoa, đang công tác tại khoa Tạo hình thẩm mỹ bệnh viện Chợ Rẫy, có tên "PGS,TS,Bác sĩ Văn Thanh -Chuyên Khoa Thẩm Mỹ Bệnh viện Chợ Rẫy". Đáng lưu ý, hình nền của trang giả mạo này còn sử dụng hình ảnh tập thể khoa Nội soi bệnh viện Chợ Rẫy để cắt ghép, đưa hình bác sĩ giả mạo vào nhằm mục đích tạo lòng tin với các khách hàng, gây nên sự bức xúc không nhỏ chocác bác sĩ có mặt trong ảnh gốc.

Đối với hình thức lừa đảo trên, các đối tượng lừa đảo lập các tài khoản mạng xã hội giả mạo tên và hình ảnh của bác sĩ có uy tín hoặc danh tiếng trong lĩnh vực

y tế. Các trang giả mạo này thường chia sẻ các bài viết liên quan đến sức khỏe, khám chữa bệnh để thu hút sự chú ý và tạo niềm tin cho người theo dõi. Ngoài ra, để tạo thêm uy tín, đối tượng sẽ cung cấp hình ảnh các chứng chỉ, bằng cấp giả mạo hoặc chỉnh sửa hình ảnh để làm giả danh tính bác sĩ. Sau khi xây dựng lòng tin với người theo dõi, kẻ lừa đảo sẽ mời chào dịch vụ khám chữa bệnh trực tuyến với mức giá thấp hoặc ưu đãi đặc biệt. Sau khi nhận được tiền cọc hoặc thanh toán dịch vụ, đối tượng sẽ biến mất hoặc cung cấp thông tin y tế không chính xác, gây nguy hại cho sức khỏe người bệnh.

Trước thực trạng lừa đảo diễn ra, Cục An toàn thông tin (Bộ TT&TT) khuyến cáo người dân tuyệt đối cẩn trọng trước các dịch vụ khám chữa bệnh, bán thuốc trên mạng xã hội. Trước khi sử dụng dịch vụ khám chữa bệnh, hãy kiểm tra kỹ thông tin về bác sĩ và cơ sởy tế, thực hiện xác minh qua website của các cơ quan y tế uy tín hoặc từ nguồn tin đáng tin cậy. Nếu có nhu cầu khám chữa bệnh, hãy đến các bệnh viện hoặc cơ sở y tế có uy tín, được cơ quan chức năng cấp phép để đảm bảo an toàn. Ngoài ra, chỉ nên sử dụng các nền tảng khám chữa bệnh online chính thống, được cấp phép và có hệ thống kiểm tra danh tính bác sĩ rõ ràng. Trong trường hợp nghi ngờ bản thân bị lừa đảo, người dân cần ngay lập tức báo cáo cho cơ quan chức năng hoặc tổ chức bảo vệ người tiêu dùng để được hỗ trợ, giải quyết và ngăn chặn kịp thời.

3. Cảnh báo chiêu trò lừa đảo đầu tư tài chính trên mạng xã hội.

Công an thành phố Hà Nội vừa tiếp nhận đơn trình báo từ chị V. (sinh năm1974, trú tại Nam Từ Liêm, Hà Nội) về việc bị lừa đảo 2,3 tỷ đồng sau khi tham gia nhóm "Tài chính thời đại" và đầu tư tiền ảo qua sàn Bitforex.com.

Đối với chiêu trò trên, các đối tượng thường lập ra các sàn chứng khoán, đầu tư tiền ảo giả mạo hoặc không được cấp phép hoạt động. Thậm chí, đối tượng còn giả danh là chuyên gia tài chính, chuyên viên chứng khoán hoặc đại diện của các công ty môi giới uy tín. Tiếp đó, đối tượng mời nạn nhân vào các nhóm đầu tư trên mạng xã hội (như Facebook, Telegram, Zalo...) và mời chào nạn nhân tham gia vào sàn mà đối tượngtạo ra. Ban đầu, đối tượng quảng cáo sàn giao dịch của mình với lời hứa lãi suất cao, thậm chí đưa ra các bằng chứng giả mạo về lợi nhuận từ các nhà đầu tư trước đó. Sau khi thu hút được số lượng lớn nhà đầu tư và nhận tiền, sàn giao dịch ảo sẽ đóng cửa hoặc biến mất, khiến nhà đầu tư mất sạch số tiền đã đầu tư.

Trước tình trạng trên, Cục An toàn thông tin (Bộ TT&TT) khuyến cáo người dân tuyệt đối không tham gia không tham gia đầu tư, mua bán trên các sàn giao dịch tiền ảo, tiền kỹ thuật số, website hay ứng dụng đầu tư tiền ảo. Trước khi tham gia bất kỳ sàn giao dịch nào, người dân cần kiểm tra giấy phép hoạt động và thông tin về sàn giao dịch;Chỉ nên giao dịch trên các sàn được cấp phép bởi cơ quan chức năng;Không chia sẻ thông tin cá nhân cho bất kỳ ai dưới mọi hình thức;Không tải về các ứng dụng không rõ nguồn gốc hoặc nhấp vào đường dẫn lạ. Trong trường

hợp nghi ngờ bản thân bị lừa đảo, người dân cần ngay lập tức báo cáo cho cơ quan chức năng hoặc tổ chức bảo vệ người tiêu dùng để được hỗ trợ, giải quyết và ngăn chặn kịp thời.

4. Cảnh giác trước những thông tin giảmạo liên quan đến việc xuất khẩu lao động tại Hàn Quốc.

Mới đây, Trung tâm Lao động ngoài nước (Bộ Lao động, Thương binh và Xã hội) vừa phát đi cảnh báo về thông tin giả mạo, lừa đảo người lao động đi Hàn Quốc làm việc theo chương trình EPS.

Đối với hình thức lừa đảo trên, các đối tượng thường mạo danh các công ty môi giới lao động hợp pháp bằng cách tạo website giả mạo hoặc cung cấp giấy tờ giả. Tinh vi hơn, các đối tượng còn tổ chức các buổi hội thảo, gặp gỡ tại các địa phương, hứa hẹn việc làm tại nước ngoài với mức thu nhập cao và điều kiện lao động tốt. Đối tượng đưa ra lời hứa hẹn về chi phí xuất khẩu lao động thấp hơn so với mức thông thường và thu nhập rất cao. Tiếp đó, đối tượng yêu cầu người lao động nộp một khoản tiền lớn để làm thủ tục hoặc chi phí đầu vào trước khi ký hợp đồng chính thức. Người lao động sau khi nộp tiền môi giới, chi phí hồ sơ sẽ không thể liên lạc lại với đối tượng lừa đảo hoặc được đưa sang nước ngoài với công việc, thu nhập khác xa so với lời hứa ban đầu.

Trước tình hình lừa đảo, Cục An toàn thông tin (Bộ TT&TT) khuyến cáo người lao động nên tìm hiểu kỹ về các chương trình xuất khẩu lao động qua các nguồn chính thống, như các cơ quan chính phủ, đại sứ quán, hoặc các tổ chức có uy tín. Tuyệt đối không tin vào các quảng cáo hay lời mời hứa hẹn hấp dẫn nhưng thiếu cơ sở pháp lý. Thực hiện kiểm tra danh tính của các tổ chức, xác minh thông qua các trang web chính thức của cơ quan chức năng. Chỉ nên tham gia các chương trình xuất khẩu lao động thông qua các công ty được Bộ Lao động -Thương binh và Xã hội cấp phép. Tuyệt đối không nộp bất kỳ khoản tiền nào trước khi ký kết hợp đồng lao động rõ ràng với các điều khoản về công việc, thu nhập, chi phí cụ thể.

Trong trường hợp nghi ngờ bản thân bị lừa đảo, người dân cần ngay lập tức báo cáo cho cơ quan chức năng hoặc tổ chức bảo vệ người tiêu dùng để được hỗ trợ, giải quyết và ngăn chặn kịp thời.

5. Cảnh báo lừa đảo thông qua hình thức tặng quà 20/10.

Công an thành phố Hà Nội cho biết, gần đây ở Hà Nội đã xuất hiện hình thức lừa đảo thông qua “tặng quà tri ân”.

Mới đây, bà C (sinh năm1964, trú tại quận Tây Hồ) thấy trên mạng xã hội Facebook quảng cáo nội dung "YODY Thời Trang Mọi Nhà" tặng quà 20/10 cho khách hàng. Đối tượng hướng dẫn bà thực hiện một số nhiệm vụ để có cơ hội nhận tiền và các phần quà. Do nhẹ dạ, cả tin bà C đã chuyểncho đối tượng khoảng 50 triệu đồng để làm nhiệm vụ. Tuy nhiên, đối tượng lừa đảo tiếp tục yêu cầu nạn nhân chuyển thêm tiền để nhận được phần quà lớn hơn. Chiều 24/9, bà C đến ngân

hàng VPbank (251 Thụy Khuê) để chuyển thêm 40 triệuđồng. Sau khi được cán bộ Công an phường và nhân viên nhân hàng thuyết phục, phân tích về thủ đoạn lừa đảo, bà C đã dừng chuyển tiền cho các đối tượng.

Thủ đoạn chung của các đối tượng này là thông báo cho nạn nhân qua tin nhắn, email, hoặc cuộc gọi đã trúng thưởng giải thưởng lớn dù không hề tham gia bất kỳ chương trình nào. Thêm vào đó, đối tượng sẽ lợi dụng tên tuổi của các tổ chức, công ty lớn để tạo lòng tin, như các nhãn hiệu điện thoại, xe hơi, hoặc các nhãn hàng nổi tiếng. Đối tượng lừa đảo sẽ yêu cầu nạn nhân cung cấp thông tin cá nhân như số chứng minh nhân dân, số tài khoản ngân hàng, mật khẩu. Ngoài ra, đối tượng còn yêu cầu bạn chuyển khoản một khoản tiền (phí vận chuyển, thuế) để nhận giải thưởng. Thậm chí, đối tượng còn thường tạo áp lực về thời gian, yêu cầu bạn phải hành động ngay lập tức nếu không sẽ mất phần thưởng.

Trước thông tin trên, Cục An toàn thông tin (Bộ TT&TT) khuyến cáongười dân nên thận trọng và cảnh giác trước những tin nhắn, cuộc gọi thông báo trúng thưởng hoặc mời tham gia chương trình tri ân khách hàng miễn phí. Người dân cần chủ động tìm hiểu và kiểm tra, xác minh danhtính đối tượng bằng cách liên hệ qua các trang thông tin chính thống. Tuyệt đối không làm theo hướng dẫn, không thực hiện giao dịch chuyển tiền cho các đối tượng lạ. Không cung cấp thông tin cá nhân nhạy cảm dưới bất kỳ hình thức nào. Không truy cập vào các đường dẫn lạ. Tuyệt đối không chia sẻ số tài khoản ngân hàng, mã OTP, mật khẩu, hoặc bất kỳ thông tin nhạy cảm nào.

Trong trường hợp nghi ngờ bản thân bị lừa đảo, người dân cần ngay lập tức báo cáo cho cơ quan chức năng hoặc tổ chức bảo vệ người tiêu dùng để được hỗ trợ, giải quyết và ngăn chặn kịp thời.

6. Cảnh giác chiêu trò giả danh cảnh sát giao thông gửi thông báo phạt nguội.

Thời gian qua, nhiều người dân bị một số đối tượng lừa đảo, giả danh Cảnh sát giao thôngthông báo kết quả phạt nguội. Không nắm rõ quy trình xử lý của lực lượng chức năng, đã có người sập bẫy.

Theo đó, anh L.H.P (sinh năm1995, ở quận Hai Bà Trưng, Hà Nội) bất ngờ nhận được tin nhắn từ một người tự xưng là cán bộ Đội Cảnh sát giao thôngthuộc Phòng Cảnh sát giao thôngCông an thành phốHà Nội. Nội dung tin nhắn thông báo về việc lực lượng chức năng ghi nhận anh P điều khiển xe gắn máy có hành vi lạng lách, đánh võng; nêu rõ số tiền xử phạt là từ 6-8 triệu đồng, tước giấy phép lái xe từ 2-4 tháng. Để tăng lòng tin, đối tượng còn trích dẫn các điều, khoản trong Nghị định 100/2019/NĐ-CP để làm căn cứ, đồng thời "đề nghị chủ xe cầm theo giấy tờ xe, đăng ký xe, căn cước công dân lên Đội Cảnh sát giao thôngđể xử phạt theo quy định của pháp luật". Đáng chú ý, nội dung cuối cùng của tin nhắn còn có lời răn đe, dọa nạt người dân để tạo tâm lý lo sợ. Nghi ngờ, anh P đến trực tiếp cơ quan Công an để xác minh và tránh được việc sập bẫy lừa đảo.

Thủ đoạn chung của các đối tượng này là tự xưng Cảnh sát giao thôngthông báo hành vi vi phạm giao thông. Tuy nhiên, do đã quá thời hạn xử lý, đề nghị người vi phạm cung cấp số biên bản. Nếu người vi phạm chưa nhận được biên bản, các đối tượng giả danh này yêu cầu người vi phạm cung cấp một loạt thông tin như: tên, tuổi, địa chỉ, số chứng minh nhân dân/căn cước công dân, số hộ chiếu, số tài khoản ngân hàng... để lực lượng chức năng cung cấp số biên bản, hành vi vi phạm, hình thức xử lý, số tiền xử phạt. Sau đó, đối tượng yêu cầu nạn nhân chuyển tiền vào tài khoản của đối tượng. Những người có tâm lý nhẹ dạ, không cảnh giác sẽ trở thành "con mồi" cho kẻ chiếm đoạt tài sản.

Trước thông tin trên, Cục An toàn thông tin (Bộ TT&TT) khuyến cáongười dân nên tỉnh táo khi nhận phải các cuộc gọi và tin nhắn từ những đối tượng không rõ danh tính. Người dân cần chủ động tìm hiểu và kiểm tra, xác minh danh tính đối tượng bằng cách liên hệ qua các trang thông tin chínhthống. Các trường hợp bị phạt nguội, Cảnh sát giao thôngđều gửi thông báo yêu cầu chủ phương tiện hoặc người liên quan đến trụ sở cơ quan công an (nơi xảy ra vi phạm) để làm việc nên không có chuyện gọi điện, nhắn tin qua điện thoại thông báo vi phạm. Tuyệt đối không làm theo hướng dẫn, không thực hiện giao dịch chuyển tiền cho các đối tượng lạ. Không cung cấp thông tin cá nhân nhạy cảm dưới bất kỳ hình thức nào. Không truy cập vào các đường dẫn lạ.

7. Cảnh giác trước các lời mời chào "làm nhiệm vụ online".

Ngày 19/9/2024, Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao Công an tỉnh Bình Phước đãtiếp nhận đơn của ông C.X.H, trúphường Minh Thành, thị xã Chơn Thành trình báo việc bịtội phạm công nghệcao lừa đảo chiếm đoạt hơn 1 tỷđồng.

Theo đó, nạn nhân bị một tài khoản mạng xã hội giả mạo dẫn dụ tải ứng dụng Telegram để tham gia xem phim online vàbình chọn được trảphí. Đối tượng gửi một đường dẫnvàhướng dẫn ông C.X.H đăng nhập tài khoản, truy cập vào một trang webđểxem phim và làm nhiệm vụ sau khi hoàn thành thìnhận được 170.000 đồng chuyển vào tài khoản. Sau nhiều lần nạp tiền vào mà vẫn không rút tiền ra được, ông C.X.H nhắn tin hỏi thìcác đối tượng đưa ra nhiều lýdo để thoái thác việc trả lại tiền đãnạp vào hệthống. Lúc này, nghi ngờbịtội phạm công nghệcao lừa sốtiền 1 tỷ 6 triệu 880 ngàn đồng nên ông C.X.H đã đến cơ quan công an trình báo.

Đối với hình thức lừa đảo trên, các đối tượng thường tạo lập các tài khoản mạng xã hội giả mạo, tự xưng là nhân viên hỗ trợ, mạo danh các công ty uy tín. Đối tượng thông qua các trang mạng xã hội như Facebook, Zalo hoặc Telegram để dẫn dụ và hướng dẫn nạn nhân tham gia vào các “dự án” hoặc nhiệm vụ nạp tiền nhận hoa hồng không có thật. Đôi khi đối tượng còn sử dụng chiến thuật gây áp lực, khẳng định rằng nếu không hành động ngay, người dùng sẽ mất một cơ hội lớn. Sau khi nạn nhân tin tưởng chuyển tiền, đến một số tiền lớn nhất định, đối

tượng sẽ đưa ra hàng loạt các lý do để nạn nhân không thể rút được tiền ra và chặn toàn bộ liên lạc.

Trước tình hình lừa đảo, Cục An toàn thông tin (Bộ TT&TT) khuyến cáo người dân cần đề cao cảnh giác trước các lời hứa hẹn về thu nhập cao, việc làm dễ dàng không cần bằng cấp. Thực hiện xác minh thông tin từ các nguồn chính thức, không tin tưởng vào những thông báohoặc kênh thông tin không rõ ràng. Không cung cấp thông tin cá nhân, thông tin tài khoản ngân hàng hoặc mật khẩu cho bất kỳ ai. Thiết lập xác thực hai yếu tố cho tài khoản trực tuyến và cập nhật mật khẩu thường xuyên. Trong trường hợp nghi ngờ bản thân bịlừa đảo, người dân cần ngay lập tức báo cáo cho cơ quan chức năng hoặc tổ chức bảo vệ người tiêu dùng để được hỗ trợ, giải quyết và ngăn chặn kịp thời.

8. Cảnh giác với các ứng dụng ngân hàng giả mạo nhằm chiếm quyền điều khiển thiết bị.

Lợi dụng công nghệ, các đối tượng lừa đảo đã dùng app ngân hàng giả, tạo hóa đơn chuyển tiền giả để chiếm đoạt tài sản.

Thủ đoạn chung của đối tượng lừa đảo chiêu trò trên thường là tạo lập các trang web, ứng dụng, trang mạng xã hội mạo danh tổ chức ngân hàng và các tổ chức tài chính, đơn vị trung gian thanh toán. Sau đó, tiếp cận nạn nhân bằng nhiều hình thức (chạy quảng cáo, phát tán tin nhắn mạo danh ngân hàng hoặc mạo danh nhân viên ngân hàng gọi điện thoại cho nạn nhân...) nhằm đánh cắp thông tin cá nhân của người dùng và thực hiện kịch bản lừa đảo. Kịch bản lừa đảo của đối tượng thường liên tục thay đổi để đối phó với việc cơ quan chức năng thường xuyên tuyên truyền cảnh báo người dân như: mời nâng cấp thẻ tín dụng; vay tiền trực tuyến với thủ tục dễ dàng, lãi suất thấp; thông báo tài khoản ngân hàng phát sinh giao dịch đáng ngờ; hướng dẫn cập nhật sinh trắc học, thông tin tài khoản... Sau đó các đối tượng thao túng và yêu cầu nạn nhân làm theo yêu cầu cung cấp thông tin đăng nhập, mật khẩu và đặc biệt là mã OTP xác thực.

Đáng chú ý là hiện tượng dẫn dụ nạn nhân cài đặt app giả mạo trên điện thoại. Các ứng dụng này có chứa mã độc và chiếm quyền điều khiển điện thoại để đánh cắp thông tin rồi thực hiện việc chuyển tiền trực tuyến để chiếm đoạt tài sản của nạn nhân.

Trước thông tin trên, Cục An toàn thông tin (Bộ TT&TT) khuyến cáo người dân nên thận trọng trước những bài đăng hoặc những thông tin không rõ nguồn gốc trên mạng xã hội. Người dân cần thực hiện kiểm tra tính xác thực của thông tin về nghệ sĩ. Tuyệt đối không làm theo hướng dẫn, không thực hiện giao dịch chuyển tiền cho các đối tượng lạ. Không cung cấp thông tin cá nhân nhạy cảm dưới bất kỳ hình thức nào. Không truy cập vào các đường dẫn lạ. Tuyệt đối không chia sẻ số tài khoản ngân hàng, mã OTP, mật khẩu, hoặc bất kỳ thông tin nhạy cảm nào. Trong trường hợp nghi ngờ bản thân bị lừa đảo, người dân cần ngay lập tức báo

cáo cho cơ quan chức năng hoặc tổ chức bảo vệ người tiêu dùng để được hỗ trợ, giải quyết và ngăn chặn kịp thời.

9. Cảnh giác với hình thức lừa đảo giả mạo công ty điện lực.

Mới đây, chính quyền Canada đã đưa ra cảnh báo về thủ đoạn lừa đảo giả mạo công ty điện lực Sask Power, gửi tin nhắn đến người dân yêu cầu thanh toán những khoản phí nợ thông qua hình thức chuyển khoản trực tuyến.

Các đối tượng tự nhận là nhân viên làm việc tại công ty điện lực, gửi hóa đơn thanh toán trễ hạn bao gồm thông tin và địa chỉ nhà của nạn nhân thông qua Email, yêu cầu truy cập vào đường dẫn để tiến hành các thủ tục thanh toán. Để tăng tính thuyết phục, các đối tượng đính kèm số điện thoại phía cuối tin nhắn, dụ dỗ nạn nhân gọi điện để xác thực và giải quyết những khúc mắc. Sau khi nạn nhân thực hiện cuộc gọi, các đối tượng sử dụng giọng điệu cấp bách, khẩn trương, nói rằng nguồn điện nơi nạn nhân sinh sốngsẽ bị ngắt trong vài giờ tới, yêu cầu nhanh chóng thanh toán khoản nợ. Để thanh toán một cách thuận tiện và nhanh chóng, các đối tượng yêu cầu nạn nhân cung cấp thông tin về nơi đăng ký tài khoản ngân hàng, sau đó gửi đường dẫn và khuyến khích nạn nhân truy cập bằng thiết bị điện thoại có cài sẵn ứng dụng ngân hàng trực tuyến. Sau khi truy cập, đường dẫn sẽ tự động chuyển hướng tới màn hình giao dịch, yêu cầu nạn nhân xác nhận để hoàn tất thành toán.

Qua thủ đoạn lừa đảo trên, Cục An toàn thông tin (Bộ TT&TT) khuyến cáo người dân cảnh giác khi nhận được tin nhắn, Email yêu cầu thanh toán các khoản phí. Cẩn thận xác minh kỹ thông tin, danh tính của người gửi Email, đơn vị công tác thông qua số điện thoại hoặc cổng thông tin chính thống. Tuyệt đối không truy cập vào đường dẫn lạ, không thực hiện các giao dịch chuyển tiền vào tài khoản đáng ngờ khi chưa xác thực được thông tin. Khi bắt gặp hành vi có dấu hiệu lừa đảo, người dân cần trình báo với lực lượng chức năng, cơ quan công an địa phương để kịp thời tiến hành điều tra và truy vết đối tượng, ngăn chặn hành vi lừa đảo.

10. Cảnh giác các hội nhóm "tư vấn sức khoẻ" trên mạng xã hội.

Hiện nay,tình trạng lừa đảo trên các trang mạng xã hội diễn ra ngày càng tinh vi và phức tạp dưới nhiều hình thức khác nhau, điển hình có thể kể đến là tình trạng lừa đảo từ các nhóm kín “tư vấn sức khỏe”, hành vi này không chỉ khiến người dân thiệt hại về tài sảnmà nguy hiểm hơn là ảnh hưởng đến sức khỏe vì có nguy cơ sử dụng phải thuốc giả hoặc không rõ nguồn gốc xuất xứ.

Theo đó, bà D.N.L ở (55 tuổi, TP.Hồ Chí Minh) bị bệnh xương khớp lâu năm nên có tham gia một số nhóm kín về tư vấn sức khỏe để giao lưu cũng như chia sẻ kinh nghiệm về căn bệnh của mình. Thời gian gần đây,trên nhóm có đăng một số bài quảng cáo sản phẩm thuốc đông y, cam kết 100% hiệu quả,thấy có khuyến mãi nên bà đã mua về sử dụng và được gửi ngay sau đó. Khi nhận sản phẩm, nhận thấy thuốc hơi khác, bà có đến phòng mạch để hỏi bác sĩ thì bác sĩ tư vấn là thuốc này hoàn toàn không có trị bệnh khớp.

Thủ đoạn chung của các đối tượng trên là tạo lập các Fanpage, hội nhóm trên mạng xã hội hoặc gọi điện nhằm lôi kéo nạn nhân tham gia. Ban đầu, các đối tượng mời tham gia vào các hội nhóm rồi gọi điện tư vấn mua thuốc đông y để chữa bệnh cùng chương trình khuyến mãi hấp dẫn, như được dùng thuốc miễn phí trong 5 năm và được bảo hiểm hoàn trả 80% tiền thuốc đã điều trị. Tại đây, các đối tượng sẽ chia sẻ trao đổi những thông tin, video clip có sử dụng hình ảnh bác sĩ, nhân viên y tế để mô tả tư vấn và hướng dẫn sử dụng các thực phẩm hoặc mô tả công dụng thực phẩm giống như một kinh nghiệm thực tế hay nhân chứng sống của người đã từng bị bệnh để tăng thêm sức thuyết phục. Với tình trạng bệnh đã chữa trị lâu năm nhưng không khỏi và những lời mời có cánh trên mạng, các nạn nhân này đã bị đối tượng lừa đảo hàng triệu đồng. Sau khi nhận được tiền, kẻ lừa đảo liền mất liên lạc.

Trước thủ đoạn lừa đảo nói trên, Cục An toàn thông tin (Bộ TT&TT) khuyến cáo người dân cần tuyệt đối cẩn trọng trước các dịch vụ khám chữa bệnh, bán thuốc trên mạng xã hội. Trước khi sử dụng dịch vụ khám chữa bệnh, hãy kiểm tra kỹ thông tin về bác sĩ và cơ sở y tế, thực hiện xác minh qua website của các cơ quan y tế uy tín hoặc từ nguồn tin đáng tin cậy. Nếu có nhu cầu khám chữa bệnh, hãy đến các bệnh viện hoặc cơ sở y tế có uy tín, được cơ quan chức năng cấp phép để đảm bảo an toàn. Ngoài ra, người dân chỉnên sử dụng các nền tảng khám chữa bệnh online chính thống, được cấp phép và có hệ thống kiểm tra danh tính bác sĩ rõ ràng./