Phụ lục 01
Một số phương thức tội phạm mạng sử dụng để lừa đảo trực tuyến và khuyến nghị phòng tránh

1. Cảnh báo hình thức lừa đảo tổ chức cá độ bóng đá qua không gian mạng, chiếm đoạt hàng trăm tỷ đồng

Ngày 02/01/2024, Công an tỉnh Thừa Thiên - Huế tiến hành tạm giữ 9 đối tượng trong đường dây tổ chức đánh bạc dưới hình thức cá độ bóng đá qua mạng với số tiền giao dịch trong một tháng là 3,5 triệu USD, tương đương hơn 176 tỷ đồng. Trong đó, Hoàng Anh Luân, 31 tuổi, trú tại thị xã Hương Trà được xác định là người cầm đầu.

Tại cơ quan công an, các đối tượng khai nhận hành vi lừa đảo chiếm đoạt tài sản. Đối tượng cầm đầu khai nhận đã quản lý một tài khoản cá độ bóng đá cấp cao, hạn mức lên tới 1,4 triệu USD; theo đó, đối tượng chia tài khoản theo các cấp nhỏ hơn và đưa cho đồng phạm nhằm tổ chức cá độ bóng đá qua không gian mạng.

Trước thực trạng trên, Bộ TT&TT khuyến cáo người dân cần nâng cao ý thức chấp hành quy định pháp luật liên quan đến tội phạm và tệ nạn cờ bạc, đặc biệt là cá độ bóng đá. Người dân cần ý thức được hậu quả và tác hại của tệ nạn cá độ bóng đá đối với bản thân, gia đình và xã hội. Tuyệt đối không tham gia cá độ bóng đá dưới mọi hình thức.

Trường hợp phát hiện các đối tượng có biểu hiện nghi vấn liên quan đến cá độ bóng đá cần kịp thời báo tin tố giác với cơ quan Công an gần nhất hoặc qua đường dây nóng của Cục Cảnh sát hình sự Bộ Công an (069.2348569) để có biện pháp điều tra xử lý, góp phần làm lành mạnh môi trường xã hội.

2. Cảnh báo chiêu trò sử dụng các ứng dụng cho vay nặng lãi, thu lợi bất chính

Phòng Cảnh sát hình sự, Công an tỉnh Nghệ An vừa bắt giữ 3 đối tượng về hành vi cho vay lãi nặng trong giao dịch dân sự. Từ đầu 2023 đến nay, các đối tượng đã cho 20 người vay số tiền trên 2 tỷ đồng, thu lợi bất chính hơn 500 triệu đồng.

Với chiêu trò này, các đối tượng không viết giấy vay nợ, hay bất kỳ một loại giấy thể hiện lãi suất vay mà sử dụng các phần mềm ứng dụng (app) trên mạng xã hội để quản lý. Các đối tượng đã lợi dụng sự khó khăn về kinh tế của người dân trên địa bàn để cho vay tiền với lãi suất cao từ 3.000 - 5.000 đồng/1 triệu đồng/ngày (tương đương 108% đến 182,5%/1 năm). Khi đến hạn thanh

toán tiền lãi nếu người vay không trả kịp, các đối tượng sẽ trực tiếp đến nhà đe dọa người vay nhằm gây sức ép.

Qua quá trình điều tra cho thấy, các đối tượng lừa đảo trên có nhiều mối quan hệ xã hội phức tạp, đã từng có tiền án, và hoạt động rất tinh vi.

Trước thực trạng trên, Bộ TT&TT khuyến cáo người dân nên tìm đến các tổ chức cho vay uy tín như ngân hàng hoặc các công ty tài chính hợp pháp; tuyệt đối không cung cấp bất kỳ thông tin cá nhân hoặc tài khoản ngân hàng trên các trang web hoặc ứng dụng không đáng tin cậy. Khi cài đặt bất kỳ ứng dụng nào, đặc biệt liên quan đến 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. Nếu phát hiện có điểm đáng ngờ, hãy hủy cài đặt ứng dụng ngay lập tức.

3. Cảnh báo chiêu trò giả danh cán bộ làm việc tại Bộ Công an hỗ trợ nạn nhân lấy lại tiền bị mất để tiếp tục chiếm đoạt tài sản

Công an tỉnh Thái Nguyên vừa khởi tố vụ án, bắt tạm giam Lê Nguyên Giáp, sinh năm 1993, ở phường Đại Kim, quận Hoàng Mai, TP Hà Nội về hành vi "Lừa đảo chiếm đoạt tài sản".

Trước đó, ngày 20/12/2023, Phòng An ninh mạng và Phòng chống tội phạm sử dụng công nghệ cao, Công an tỉnh Thái Nguyên tiếp nhận đơn trình báo của một người sinh năm 1984, ở huyện Phú Bình, tỉnh Thái Nguyên về hành vi lừa đảo của Lê Nguyên Giáp.

Theo đó, đối tượng giả danh quen biết cán bộ làm việc tại Bộ Công an có khả năng giải quyết, lấy lại được tiền ảo đã thua lỗ của nạn nhân để lừa đảo chiếm đoạt tiền. Nạn nhân cho biết có tham gia đầu tư tiền ảo trên mạng và đã bị lừa đảo chiếm đoạt tài sản, nhưng sau đó vì tâm lý muốn lấy lại tiền, nạn nhân lại tìm và tham gia vào một số nhóm trên mạng xã hội để tìm cơ hội lấy lại tiền. Nắm bắt tâm lý trên của nạn nhân, đối tượng chủ động nhắn tin và cho biết mình cũng từng bị lừa đảo; đồng thời tự giới thiệu có quen biết với một cán bộ làm ở Bộ Công an có thể giúp lấy lại số tiền bị lừa đảo. Để tạo lòng tin, đối tượng còn gửi số điện thoại của bản thân, giả làm cán bộ công an gọi điện và trao đổi với nạn nhân. Trong quá trình trao đổi, nạn nhân đã tin tưởng và chuyển tiền cho đối tượng lừa đảo trên 3 lần với tổng số tiền là 100 triệu đồng. Tuy nhiên, nạn nhân lại tiếp tục rơi vào bẫy và bị lừa chiếm đoạt số tiền trên.

Trước thực trạng lừa đảo trên, Bộ TT&TT đưa ra khuyến cáo người dân, đặc biệt là những người đã trở thành nạn nhân của các đối tượng lừa đảo, cần phải 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 những thông tin cá nhân như Căn cước công dân, Chứng minh nhân dân, số tài khoản ngân hàng, mã OTP, … để tránh bị đánh cắp thông tin sử dụng cho mục đích phi pháp. Không thực hiện bất kỳ giao dịch nào trên mạng xã hội nếu chưa xác minh được chính xác người nhận tiền là ai.

Nếu đã bị lừa thì lập tức báo ngay cho cơ quan Công an gần nhất, tuyệt đối không nghe theo hướng dẫn của bất cứ đối tượng nào mạo danh có thể lấy lại tiền giúp nạn nhân mà phải chuyển phí trước.

4. Cảnh bảo hình thức lừa đảo sử dụng kịch bản "thanh lý đồ điện tử giá rẻ" nhằm chiếm đoạt tài sản của người dùng mạng xã hội

Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh Bắc Kạn vừa xử lý thành công chuyên án đấu tranh với đối tượng sử dụng mạng xã hội Facebook để thực hiện hành vi lừa đảo, chiếm đoạt tài sản của nhiều người dân.

Theo đó, đối tượng Lê Thanh Tuấn sinh năm 1989, ở Hoài Đức, Hà Nội bị bắt giữ vì hành vi lập nick ảo để lừa đảo, chiếm đoạt tài sản. Với thủ đoạn lập các tài khoản Facebook giả mạo rồi dùng kịch bản thanh lý đồ điện tử giá rẻ, đối tượng đã lừa tiền của nhiều người dùng mạng xã hội.

Đối tượng đã tạo lập các tài khoản Facebook giả mạo với tên tương tự những tài khoản ngân hàng chính chủ đã mua. Những tài khoản này được đối tượng sử dụng để đăng tải các bài viết có nội dung thanh lý các món đồ điện gia dụng như tủ lạnh, tủ đông, tủ hải sản,... tại các hội nhóm trên mạng xã hội. Đối tượng thường tự giới thiệu là người ở huyện Chợ Mới, tỉnh Bắc Kạn, hiện làm nghề mua bán hải sản, cần thanh lý đồ đạc trong cửa hàng để chuyển đổi mục đích kinh doanh. Để thu hút người mua, đối tượng này rao bán đồ điện tử với mức giá thấp hơn nhiều so với giá thị trường. Bằng thủ đoạn này, nhiều người đã tin tưởng mua hàng, đồng thời chuyển tiền đặt cọc trước vào tài khoản ngân hàng do Lê Thanh Tuấn cung cấp. Sau khi nhận tiền, đối tượng liền ngay lập tức chặn tương tác với nạn nhân. Để tránh bị phát hiện, đối tượng này liên tục thay đổi tên và hình đại diện các tài khoản Facebook giả mạo, thậm chí đổi cả số điện thoại liên hệ.

Trước tình trạng người dân liên tục bị lừa đảo bằng hình thức bán xe giá rẻ, Bộ TT&TT khuyến cáo người dân nên lựa chọn những địa chỉ uy tín và chính thống để tránh sập bẫy lừa đảo. Người dân không mua những sản phẩm không rõ nguồn gốc xuất xứ cũng như giá rẻ hơn nhiều lần so với thị trường để tránh mua phải những mặt hàng kém chất lượng hoặc bị chiếm đoạt tài sản.

5. Lừa bán phần mềm đọc trộm tin nhắn, chiếm đoạt tài sản hàng trăm triệu đồng

Phòng Cảnh sát hình sự Công an tỉnh Thanh Hóa vừa khởi tố vụ án, khởi tố bị can và bắt tạm giam đối tượng Nguyễn Trung Hiếu sinh năm 1984 ở thành phố Vĩnh Yên, tỉnh Vĩnh Phúc về hành vi "Lừa đảo chiếm đoạt tài sản".

Theo kết quả điều tra, để có tiền trang trải nợ nần, đầu tháng 9/2023, đối tượng đã nảy sinh ý định lừa đảo chiếm đoạt tài sản bằng cách tạo lập một trang web với giao diện có các nội dung thể hiện là phần mềm đọc trộm tin nhắn Zalo, Facebook, định vị số điện thoại nhưng bản chất phần mềm không thể thực hiện được các tính năng này.

Tiếp đó, Hiếu mua tài khoản Facebook ảo có nhiều người theo dõi và sửa tên tài khoản Facebook thành "Shop Công Nghệ Gia Đình" đăng kèm số điện thoại cá nhân và chạy quảng cáo với nội dung dịch vụ cho thuê phần mềm đọc trộm tin nhắn Zalo, Facebook, định vị số điện thoại để tìm khách hàng có nhu cầu sử dụng dịch vụ để lừa đảo. Khi khách hàng liên hệ đến số điện thoại hoặc nhắn tin qua Facebook hỏi thuê dịch vụ phần mềm, đối tượng sẽ gửi tin nhắn liệt kê các tính năng và hình ảnh của phần mềm cho khách hàng. Say khi lấy được lòng tin của nạn nhân, đối tượng yêu cầu nộp các loại phí như: phí tạo link, thuê Server, mua bộ nhớ, phí vượt qua lớp bảo mật... Mỗi loại phí có giá trị từ 2 triệu đến 3 triệu đồng, tùy theo dịch vụ và tăng theo cấp độ khó của từng dịch vụ. Sau khi khách hàng đã nộp đầy đủ các khoản phí theo yêu cầu, ngay lập tức, đối tượng chặn liên lạc để chiếm đoạt số tiền.

Theo Bộ TT&TT, người dân nên tìm hiểu và theo dõi các chuyển biến của các hình thức, thủ đoạn lừa đảo tinh vi trên không gian mạng, để có thể chủ động đối phó trước mọi tình huống. Tuyệt đối không vì hiếu kỳ mà tìm mua những sản phẩm, thiết bị nêu trên; không mua các sản phẩm, thiết bị trôi nổi, giá rẻ, nhập lậu giá rẻ để tránh bị các đối tượng xấu theo dõi, đánh cắp thông tin, dữ liệu cá nhân và xâm phạm đời sống riêng tư.

Ngoài ra, việc tự ý mua, bán và sử dụng những phần mềm, thiết bị ngụy trang đọc trộm, ghi âm, ghi hình khi không được cơ quan có thẩm quyền cấp phép là hành vi vi phạm pháp luật; có thể bị xử phạt hành chính hoặc nghiêm trọng hơn là truy tố hình sự. Việc xử phạt không chỉ áp dụng với các đối tượng kinh doanh, cung cấp thiết bị trái phép mà còn là người mua và sử dụng thiết bị.

6. Cảnh báo chiêu trò mạo danh cán bộ thuế để lừa đảo chiếm đoạt tài sản

Chiêu trò lừa đảo giả danh cán bộ thuế hay công an để lừa đảo đã không còn quá xa lạ trên môi trường không gian mạng, tuy nhiên, các đối tượng giả danh này lại luôn thay đổi hình thức, thao túng tâm lý người dùng một cách tinh vi.

Đại diện Chi cục Thuế quận Hai Bà Trưng, thành phố Hà Nội cho biết, các đối tượng lừa đảo làm giả giấy mời của Chi cục Thuế để gửi cho các hộ kinh doanh trên địa bàn. Trong giấy mời thì có nội dung cần liên lạc qua Zalo với một số điện thoại lạ, nhằm mục đích tư vấn hoàn thuế, nhưng thực chất là khi người dân liên hệ sẽ đòi chi phí để thực hiện các thủ tục.

Trước thông tin trên, Bộ TT&TT khuyến cáo người dân cần nâng cao cảnh giác, đồng thời tìm hiểu và trang bị cho bản thân những kiến thức để bảo vệ mình trên mạng xã hội. Tuyệt đối không cung cấp thông tin cá nhân cho bất cứ ai thông qua bất kể hình thức nào; việc lộ lọt thông tin sẽ dẫn đến nhiều hậu quả đáng lo ngại. Khi có cuộc gọi lạ hoặc tiếp xúc với hội nhóm cung cấp dịch vụ trên mạng xã hội, tuyệt đối không thực hiện giao dịch chuyển tiền cho đối tượng khi chưa tìm hiểu và xác minh danh tính của đối tượng đó.

7. Giả danh công an gọi điện hù dọa, lừa đảo chiếm đoạt của một người phụ nữ hơn 15 tỷ đồng

Công an quận Hà Đông, thành phố Hà Nội điều tra, xác minh vụ giả danh cán bộ Công an, lừa đảo chiếm đoạt tài sản với số tiền 15 tỷ đồng.

Công an TP Hà Nội cho biết, ngày 5/4/2024, bà P sinh năm 1956, trú tại quận Hà Đông, Hà Nội nhận được điện thoại của một đối tượng tự xưng là cán bộ Công an. Đối tượng nói Căn cước công dân của bà P có liên quan đến đường dây buôn bán ma túy, rửa tiền. Nếu bà P không chứng minh được mình không liên quan thì vài ngày tới sẽ bắt bà. Do lo sợ nên bà P đã chuyển tiền vào tài khoản của các đối tượng để xác minh. Bà P đã thực hiện 32 lần chuyển khoản với tổng số tiền là 15 tỷ đồng. Sau đó, bà P biết mình bị lừa nên đã cơ quan Công an trình báo.

Trước thông tin trên, Bộ TT&TT khuyến cáo người dân cần cảnh giác, tuyên truyền đến người thân, bạn bè về thủ đoạn trên, tránh mắc bẫy của đối tượng xấu. Để làm việc với người dân, cơ quan công an sẽ trực tiếp gửi giấy mời, giấy triệu tập hoặc gửi qua công an địa phương, không yêu cầu người dân chuyển tiền vào tài khoản ngân hàng. Khi phát hiện các trường hợp có dấu hiệu lừa đảo như trên, người dân cần báo ngay cho cơ quan công an nơi gần nhất.

Điều đáng nói, đối tượng lừa đảo thường nhắm vào sự thiếu hiểu biết, không minh mẫn của người cao tuổi để ra tay lừa đảo. Vì thế, để đối phó với các đối tượng lừa đảo qua điện thoại thì những người trong gia đình phải tuyên truyền cho người cao tuổi để họ nhận biết và có ý thức cảnh giác, phòng tránh hiệu quả.

Nếu phát hiện các trường hợp có dấu hiệu bị lừa đảo, người dân cần trình báo cơ quan Công an để giải quyết vụ việc theo quy định của pháp luật; không nên tìm đến các trang mạng xã hội giới thiệu có thể lấy lại tiền bị lừa, tránh để bị mắc bẫy của các đối tượng lừa đảo.

8. Cảnh báo nhóm đối tượng mạo danh phóng viên, cộng tác viên báo chí để chiếm đoạt tài sản

Ngày 9/5/2024, Công an tỉnh Thái Nguyên cho biết, Cơ quan Cảnh sát điều tra Công an tỉnh vừa khởi tố đối với 8 đối tượng về tội "Cưỡng đoạt tài sản", với thủ đoạn mượn danh, mạo danh cộng tác viên, phóng viên của một số báo, tạp chí để đe dọa người khác chiếm đoạt tài sản.

Đối tượng làm giả bằng cấp rồi sử dụng để nộp hồ sơ làm cộng tác viên, phóng viên của một số báo, tạp chí. Sau đó, các đối tượng đến cơ quan, doanh nghiệp, tổ chức, hộ kinh doanh… với danh nghĩa phóng viên, cộng tác viên của báo, tạp chí để thu thập thông tin liên quan đến hoạt động điều hành, kinh doanh, sản xuất của các cơ sở đó. Khi tìm ra các sơ hở, thiếu sót của các cơ sở, các đối tượng gây sức ép, gợi ý để các cơ sở biết rõ hoặc ngầm hiểu nếu không đưa tiền cho các đối tượng thì sẽ bị báo đến chính quyền địa phương và viết bài phản ánh trên báo chí. Do lo sợ việc bị đưa thông tin trên báo chí sẽ ảnh hưởng đến hoạt động điều hành sản xuất kinh doanh nên các cơ sở đã phải đưa tiền cho các đối tượng.

Các đối tượng tổ chức hoạt động theo từng nhóm liên huyện, liên tỉnh, trao đổi thông tin về các cơ sở cho nhau. Khi một đối tượng lấy được tiền ở một cơ sở bất kỳ thì sẽ thông tin lại cho các đối tượng khác biết để tiếp tục đến cơ sở đó, gây sức ép là phóng viên, cộng tác viên của báo, tạp chí khác nhằm cưỡng đoạt tài sản.

Trước thông tin trên, Bộ TT&TT khuyến cáo người dân cần nâng cao kiến thức để bảo vệ bản thân trước các đối tượng lừa đảo mạo danh để tránh bị chiếm đoạt tài sản. Các cơ quan, doanh nghiệp cần nhận biết và tìm hiểu rõ danh tính của đối tượng trước khi thực hiện bất kì một thỏa thuận nào. Hiện nay, tình trạng làm giả giấy tờ, chứng chỉ, hồ sơ đang tràn lan trên mạng xã hội và được sử dụng vào những mục đích phi pháp. Người dân cần nâng cao cảnh giác, nếu gặp trường hợp lừa đảo tương tự cần báo ngay cho cơ quan chức năng, cơ quan Công an gần nhất để được hỗ trợ và giải quyết kịp thời.

9. Thủ đoạn lừa đảo chiếm đoạt tài sản bằng hình thức kêu gọi từ thiện trên mạng xã hội

Hiện nay, tình trạng lừa đảo bằng hình thức kêu gọi từ thiện diễn ra ngày càng nhiều khiến cho số lượng nạn nhân ngày một tăng lên. Đối tượng lợi dụng lòng tốt của những nhà hảo tâm để trục lợi về phía mình.

Ngày 14/5/2024, Văn phòng Cơ quan Cảnh sát Điều tra Công an tỉnh Đắk Nông cho biết, đơn vị vừa ra quyết định khởi tố vụ án, bị can và ra lệnh tạm

giam đối với Vy Bảo Châu. Lực lượng Công an cho biết, Châu đã lập nhiều tài khoản giả mạo, để hình đại diện là những tổ chức từ thiện uy tín. Bằng những tài khoản này, đối tượng đăng tải các bài viết có nội dung về những người có số phận bất hạnh, sau đó đính kèm số tài khoản chính thống của các tổ chức từ thiện. Tiếp theo, đối tượng vào phần bình luận, nói là số tài khoản trên bài bị lỗi và để số tài khoản của mình để người truy cập ủng hộ. Vì lòng trắc ẩn và thiếu cảnh giác, nhiều người đã không ngần ngại chuyển tiền vào số tài khoản của Châu.

Với thủ đoạn trên, trong khoảng thời gian từ tháng 6/2023 tới tháng 5/2024 thời điểm bị bắt giữ, Vy Bảo Châu đã chiếm đoạt tổng cộng hơn 400 triệu đồng từ gần 700 người, chủ yếu nạn nhân là những nhà hảo tâm trên khắp các địa bàn cả nước.

Cũng vào ngày 15/5/2024, Phòng an ninh mạng và Phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh Đồng Tháp đã bàn giao đối tượng Huỳnh Phương Thủy cho Cơ quan cảnh sát điều tra, Công an thành phố Cao Lãnh, tỉnh Đồng Tháp để điều tra về hành vi lừa đảo chiếm đoạt tài sản qua mạng.

Được biết, Thủy cũng có hành vi lừa đảo bằng hình thức kêu gọi hỗ trợ từ thiện. Đối tượng lập ra các tài khoản Facebook với nhiều cái tên khác nhau như "Thu Nguyễn", "Thúy Phương", "Loan Nguyễn", "Ngọc Trâm", "Thu Thuy", sau đó đăng tải các bài viết kêu gọi ủng hộ trong các hội nhóm sở hữu nhiều thành viên. Sau khi thành công chiếm đoạt tài sản, Thủy rút tiền và tiêu xài vào mục đích cá nhân. Trong quá trình điều tra, Cơ quan Công an nhận thấy tài khoản ngân hàng của Thủy có nhiều giao dịch quyên góp ủng hộ với tổng số tiền lên tới 140 triệu đồng.

Tình hình lừa đảo chiếm đoạt tài sản trên không gian mạng ngày càng phức tạp, khó lường với nhiều thủ đoạn mới, hết sức tinh vi. Để đấu tranh với các loại hình lừa đảo này, Bộ TT&TT 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.

10. Cảnh giác với hình thức giả mạo quỹ đầu tư PYN Elite để lừa đảo

Hiện nay, trên mạng xã hội lần lượt xuất hiện nhiều fanpage, nhóm chat giả danh các công ty chứng khoán, quỹ đầu tư nhằm dụ dỗ các nạn nhân tham gia gửi tiền.

Theo lực lượng Công an, một số đối tượng lừa đảo đã mạo danh quỹ PYN Elite để kêu gọi người dân đầu tư nhằm chiếm đoạt tài sản. Ban đầu, dưới danh nghĩa là các chuyên gia, cố vấn cấp cao của PYN Elite, kẻ lừa đảo tiếp cận và giới thiệu với nạn nhân về các khóa học đầu tư. Sau đó, các nạn nhân được add vào các nhóm chat Zalo , Telegram với số thành viên lên tới hàng chục nghìn người. Các đối tượng lừa đảo sử dụng phương pháp hết sức tinh vi như tạo ra ứng dụng giả mạo Pyn Smart, tạo ra website theo đường dẫn pynelitevn.pro với giao diện y nguyên từ website gốc, lập các tài khoản ngân hàng dưới danh nghĩa các công ty PYN Elite giả mạo để tạo dựng độ uy tín nhằm lợi dụng sự bất cẩn của người dân.

Ông Petri Deryng, nhà sáng lập quỹ PYN Elite cho biết: "Quỹ PYN Elite thu hút vốn đầu tư 100% từ các nhà đầu tư Phần Lan vào tài khoản ngân hàng tại Phần Lan. Các tài khoản ngân hàng tại Việt Nam được đặt dưới tên của quỹ đều là lừa đảo. Hãy lưu ý không chuyển tiền vào các tài khoản lừa đảo này tại Việt Nam. PYN Elite chỉ đầu tư vào thị trường chứng khoán Việt Nam, và không thực hiện bất kỳ hình thức kinh doanh hay tiếp thị nào ở Việt Nam. Tất cả các group chat và website bằng tiếng Việt lấy tên của quỹ đều là giả mạo"

Để phòng tránh những hành vi lừa đảo kể trên, Bộ TT&TT khuyến cáo người dân cảnh giác trước những lời mời gọi đầu tư từ người lạ. Cần phải tìm hiểu thật kỹ danh tính đối tượng, mức độ chính thống của các dự án đầu tư. Tuyệt đối không truy cập, tải các ứng dụng từ đường link lạ, chỉ truy cập vào các đường link xuất hiện trên các trang điện tử, website chính thống. Nếu gặp những trường hợp tương tự, người dân cần chủ động liên hệ ngay với các cơ quan chức năng để kịp thời điều tra và ngăn chặn hành vi chiếm đoạt tài sản.

11. Cảnh báo lừa đảo thông qua hành vi mạo danh Tổng Công ty Cảng hàng không Việt Nam (ACV)

Ngày 13/5/2024, đại diện ACV cho biết gần đây trên các nền tảng xã hội thường xuyên xuất hiện các bài đăng, fanpage mạo danh ACV với mục đích chiếm đoạt tài sản, trục lợi từ dự án sân bay Long Thành.

Theo đó, ACV nhận được nhiều thông tin, phản ánh về các bài đăng trên nền tảng Facebook với nội dung như: "Kêu gọi góp vốn đầu tư", "Đóng góp tiền với cơ hội trúng các gói thầu",... Đính kèm là những văn bản giả mạo chữ ký Chủ tịch Hội đồng quản trị ACV nhằm gia tăng mức độ uy tín, khiến cho việc dụ dỗ nạn nhân trở nên dễ dàng hơn.

Trước hành vi lừa đảo kể trên, đại diện ACV cho biết : "Chúng tôi đã có văn bản gửi Cục An ninh Kinh tế, Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao và Công an tỉnh Đồng Nai. Sáng 13/5/2024, chúng tôi vừa cung cấp thêm các thông tin cho phía cơ quan công an. Công an tỉnh Đồng Nai thông báo đang tích cực vào cuộc điều tra, làm rõ những hành vi giả mạo này".

Phía ACV cũng khẳng định Tổng Công ty hiện tại không có bất kỳ chủ trương, chính sách nào về việc huy động vốn đầu tư. Đại diện ACV cũng khuyến cáo người dân đề cao cảnh giác trước bất kỳ sự tiếp cận nào có liên quan tới hành vi kêu gọi đầu tư vào các dự án nói chung và dự án sân bay Long Thành nói riêng.

Trước thực trạng trên, Bộ TT&TT khuyến cáo người dân khi thấy các bài đăng có nội dung kêu gọi đầu tư trên mạng xã hội, phải kiểm tra bằng cách tìm kiếm thông tin trên các trang web chính thống của doanh nghiệp. Xác định kĩ danh tính đối tượng trước khi chuyển tiền. Khi bắt gặp những hành vi lừa đảo, người dân cần chủ động liên hệ ngay với các cơ quan chức năng để kịp thời ngăn chặn.

12. Cảnh báo các hình thức lừa đảo liên quan tới ứng dụng VssID giả mạo

Cơ quan Bảo hiểm xã hội Việt Nam cảnh báo các hình thức lừa đảo thông qua những dịch vụ liên quan tới ứng dụng VssID - Bảo hiểm xã hội số. Người dân được khuyến cáo đề cao cảnh giác khi bắt gặp những dịch vụ này trong quá trình sử dụng các nền tảng mạng xã hội.

Thời gian gần đây, mạng xã hội xuất hiện một kênh Tik Tok mang tên "VssID - Hỗ trợ Bảo hiểm Xã hội". Kênh Tik Tok này thường xuyên đăng tải các video về cách thức lấy lại mật khẩu đăng nhập vào ứng dụng trong trường hợp người dùng không nhớ hoặc bị mất. Bên cạnh đó, kênh này cũng quảng bá dịch vụ thay đổi thông tin cá nhân như số điện thoại, email, địa chỉ ,... đi kèm một khoản phí nhất định với những ưu đãi hấp dẫn. Theo như phản ánh của người dùng, sau khi đưa thông tin cần thiết để sử dụng dịch vụ, họ không nhận được hồi âm nên đã không chuyển tiền cho đối tượng.

Sau khi tiếp nhận những lời phản ánh, Bảo hiểm Xã hội thành phố Hà Nội khẳng định dịch vụ mà kênh Tik Tok cung cấp là trái với pháp luật. Theo như quy định, người dân sẽ không mất bất kỳ một khoản phí nào khi sử dụng dịch vụ cấp lại mật khẩu hoặc thay đổi thông tin cá nhân của tài khoản VssID.

Bên cạnh đó, các đối tượng lừa đảo cũng chủ động liên hệ với nạn nhân thông qua hình thức liên lạc điện thoại. Vào ngày 9/5/2024, anh T.H.T trú tại

phường Bửu Long, thành phố Biên Hòa, tỉnh Đồng Nai đã nhận được một cuộc gọi điện thoại đầu số là 0924635… Người gọi tự xưng là cán bộ làm việc tại cơ quan Bảo hiểm xã hội Đồng Nai, thông báo và yêu cầu anh T đồng bộ dữ liệu Căn cước công dân. Người gọi cũng nói rằng anh T có thể đồng bộ trực tuyến thông qua ứng dụng VssID mà không cần phải tới cơ quan trực tiếp. Nghi ngờ lừa đảo nên anh T đã chủ động liên hệ với cơ quan Bảo hiểm Xã hội Đồng Nai để xác minh thông tin. Sau khi kiểm tra, cơ quan cho biết không có cán bộ nào có đầu số như trên.

Trước tình hình lừa đảo diễn biến phức tạp, Bộ TT&TT khuyến cáo người dân nâng cao cảnh giác, đề phòng khi bắt gặp những dịch vụ liên quan tới ứng dụng VssID trên các nền tảng mạng xã hội. Người dân chỉ sử dụng dịch vụ từ các trang web chính thống hoặc trực tiếp đến với các cơ quan Bảo hiểm xã hội địa phương. Người dân chỉ nên tải ứng dụng VssID thông qua hệ thống cửa hàng trực tuyến như CH Play (đối với hệ điều hành Android) và App Store (đối với hệ điều hành IOS), tuyệt đối không cài đặt ứng dụng VssID từ các nguồn không xác định, những nguồn link lạ, không cung cấp thông tin cá nhân cho đối tượng lạ, khuyến khích tắt chế độ "cài đặt ứng dụng từ nguồn không xác định" trong điện thoại thông minh.

Phụ lục 02

Một số biện pháp để phòng tránh lừa đảo trên không gian mạng phổ biến hiện nay

Thứ nhất, **bảo vệ thông tin cá nhân**: Không công khai các thông tin như ngày tháng năm sinh, số Chứng minh nhân dân, Căn cước công dân, số điện thoại, số tài khoản ngân hàng… trên mạng xã hội để tránh bị các đối tượng lợi dụng khai thác, sử dụng vào mục đích lừa đảo, cần chọn lọc thông tin trước khi chia sẻ công khai trên mạng xã hội.

Thứ hai, **kiểm tra và cập nhật**: Thường xuyên kiểm tra và cập nhật các tính năng bảo mật, quyền riêng tư trên các tài khoản ngân hàng, tài khoản mạng xã hội và cần bảo mật tuyệt đối thông tin các tài khoản trên, bao gồm: tên đăng nhập, mật khẩu, mã xác thực (OTP) hoặc số thẻ tín dụng… không cung cấp cho bất kỳ cá nhân, tổ chức nào khi chưa xác định được danh tính.

Thứ ba, **cẩn trọng xác minh**: Đối với các tin nhắn qua mạng xã hội vay tiền cần trực tiếp gọi điện thoại để xác nhận kỹ thông tin trước khi chuyển tiền.

Thứ tư, **tìm hiểu kỹ thông tin khi kết bạn**: Tìm hiểu kỹ thông tin khi kết bạn với những người lạ trên mạng xã hội, đặc biệt là những người hứa hẹn cho, tặng số tiền, tài sản lớn hoặc quà có giá trị lớn.

Thứ năm, **trình báo tại cơ quan Công an nơi gần nhất**: Khi nhận được cuộc gọi tự xưng là cán bộ các cơ quan nhà nước, đặc biệt là lực lượng Công an để thông báo, đe dọa mình có liên quan đến vụ án, vụ việc, cần liên lạc ngay với cơ quan Công an nơi gần nhất để trình bảo

Thứ sáu, **cẩn trọng khi thực hiện các giao dịch**: Không truy cập các đường link trong tin nhắn hay Email lạ không rõ nguồn gốc, không thực hiện giao dịch theo yêu cầu của các đối tượng lạ khi nhận được điện thoại, tin nhắn có nội dung liên quan đến giao dịch ngân hàng. Không cung cấp thông tin cá nhân, mã OTP, số tài khoản ngân hàng…

Thứ bảy, **cẩn trọng trước lời mời chào hấp dẫn**: Không nên nghe và làm theo những lời hướng dẫn, giới thiệu, dụ dỗ làm theo các cách thức làm việc nhẹ nhàng, kiếm tiền dễ dàng… Đặc biệt không nghe theo lời các đối tượng chuyển tiền vào tài khoản chỉ định. Cảnh giác trước các thông tin thông báo nhận thưởng qua mạng, yêu cầu cung cấp thông tin cá nhân hoặc chuyển tiền để nhận thưởng.

Thứ tám, **cẩn trọng khi cài ứng dụng, phần mềm**: Không cài đặt trên điện thoại, máy tính các ứng dụng chưa được xác thực. Khi phát hiện SIM điện

thoại bị vô hiệu hóa, cần liên hệ ngay nhà mạng để yêu cầu hỗ trợ, xác mình. Nếu bị mất điện thoại, cần nhanh chóng báo cho nhà mạng để khóa SIM kịp thời.

Thứ chín, **quản lý đăng ký tài khoản ngân hàng**: Không mở, cho thuê, bán tài khoản ngân hàng cho người khác. Khi phát hiện đối tượng có hành vi mua bán, cho thuê tài khoản ngân hàng cần báo ngay cho cơ quan Công an nơi gần nhất.

Thứ mười, **cẩn trọng đối với các Website, ứng dụng giả mạo**: Tuyệt đối không truy cập website, ứng dụng trong tin nhắn nhận được, trang web có nội dung không rõ ràng, giả mạo dịch vụ chuyển tiền quốc tế, trang web ngân hàng./.