UỶ BAN NHÂN DÂN XÃ YÊN ĐỊNH

CHUYÊN ĐỀ
NHẬN DIỆN VÀ PHÒNG CHỐNG LỪA ĐẢO TRỰC TUYẾN

TÌNH HÌNH CHUNG

Hoạt động lợi dụng không gian mạng để tiến hành phạm tội, nổi bật là lừa đảo trực tuyến (chiếm 57% tổng số tội phạm mạng) gia tăng cả về phạm vi, quy mô với thủ đoạn tinh vi; triệt để lợi dụng công nghệ mới, nhất là trí tuệ nhân tạo (AI), gây thiệt hại hàng nghìn tỷ USD mỗi năm.

Các đối tượng tội phạm mạng trong và ngoài nước liên tục thay đổi phương thức, thủ đoạn, triệt để lợi dụng công nghệ mới để tấn công, xâm nhập, lừa đảo quy mô lớn, gây thiệt hại lớn về kinh tế và ảnh hưởng xấu đến trật tự an toàn xã hội, đe dọa cuộc sống bình yên, hạnh phúc của người dân.

Năm 2023, thiệt hại là 1.026 tỷ USD, tương đương 1,05% GDP toàn cầu (Tại Việt Nam, Theo thống kê, trên cổng cảnh báo an toàn thông tin ghi nhận gần 16.000 phản ánh lừa đảo trực tuyến, gây thiệt hại hơn 390.000 tỷ đồng, tương đương 3,6% GDP; trong đó 91% liên quan lĩnh vực tài chính, tăng 64,78% so với năm 2022. Tỷ lệ người dùng nhận tin nhắn, cuộc gọi lừa đảo trực tuyến là 73%).

CÁC HÀNH VI LỪA ĐẢO THƯỜNG ĐƯỢC CÁC ĐỐI TƯỢNG SỬ DỤNG HIỆN NAY

1. Lừa đảo “combo du lịch giá rẻ”.
2. Giả danh nhân viên của các đơn vị chuyển phát (shipper) để lừa đảo
3. Lừa đảo cuộc gọi video Deepfake, Deepvoice.
4. Lừa đảo “khóa SIM” vì chưa chuẩn hóa thuê bao.
5. Giả mạo biên lai chuyển tiền thành công.
6. Giả danh giáo viên/nhân viên y tế báo người thân đang cấp cứu.
7. Chiêu trò lừa đảo tuyển người mẫu nhí.
8. Thủ đoạn giả danh các công ty tài chính, ngân hàng.
9. Cài cắm ứng dụng, link quảng cáo cờ bạc, cá độ, tín dụng đen,…
10. Giả mạo trang thông tin điện tử, cơ quan, doanh nghiệp (BHXH, ngân hàng…)
11. Lừa đảo SMS Brandname, phát tán tin nhắn giả mạo.
12. Lừa đảo đầu tư chứng khoán, tiền ảo, đa cấp.

13. Lừa đảo tuyển CTV online.
14. Đánh cắp tài khoản MXH, nhắn tin lừa đảo.
15. Giả danh cơ quan công an, viện kiểm sát, tòa án gọi điện lừa đảo.
16. Rao bán hàng giả hàng nhái trên sàn thương mại điện tử.
17. Đánh cắp thông tin CCCD đi vay nợ tín dụng.
18. Lừa đảo chuyển nhầm tiền vào tài khoản ngân hàng.
19. Lừa đảo dịch vụ lấy lại tiền khi đã bị lừa.
20. Lừa đảo lấy cắp Telegram OTP.
21. Lừa đảo tung tin giả về cuộc gọi mất tiền như FlashAI.
22. Lừa đảo dịch vụ lấy lại Facebook.
23. Lừa đảo tình cảm, dẫn dụ đầu tư tài chính, gửi bưu kiện, trúng thưởng,…
24. Rải link phishing lừa đảo, seeding quảng cáo bẩn trên Facebook.
25. Lừa đảo cho số đánh đề.

KỸ NĂNG NHẬN BIẾT

1. Cách các đối tượng tiếp cận để lừa đảo

Các đối tượng lừa đảo thường áp dụng các thủ đoạn tác động tâm lý để tiếp cận nạn nhân như: Tự nhận/giả mạo là cơ quan công quyền (công an, viện kiểm sát, cán bộ đang làm việc tại các Bộ, Sở/Ngành, Địa phương...), đơn vị cung cấp dịch vụ, các tổ chức tài chính ngân hàng, gia đình bạn bè,... để đánh vào nỗi sợ hãi, lòng tham, tình cảm, chủ quan...

Các kênh thường được đối tượng lừa đảo sử dụng để tiếp cận gồm:

1/ Cuộc gọi qua SIM

2/ Tin nhắn (SMS)/ Thư điện tử (Email)

3/ Mạng xã hội

4/ Nền tảng chat OTT (Ví dụ: Zalo, WhatsApp, Viber, Telegram...). Đôi khi các đối tượng còn sử dụng trực tiếp các kênh OTT này để tiếp cận nạn nhân.

5/Website giả mạo

6/Các ứng dụng giả mạo (ứng dụng ngân hàng, chính phủ, phát trực tuyến, tiện ích…)

STT	Website lừa đảo	Ghi chú
1	https://vietgcv[.]cc	Website giả mạo Bộ Thông tin và Truyền thông
2	https://hdtinchap[.]com	Website giả mạo Công ty Tài chính TNHH HD SAISON
3	https://dichvucong[.]dancuso[.]com	Website giả mạo Dịch vụ công Quốc Gia
4	http://dichvucong[.]hhlpa[.]com	Website giả mạo Dịch vụ công Quốc Gia
5	https://lotttemart[.]store	Website giả mạo LOTTE
6	https://clzl[.]pro	Website giả mạo MoMo
7	https://vdbank[.]com[.]vn	Website giả mạo Ngân hàng Phát triển Việt Nam
8	https://sotuyenvcb[.]vietcombanker[.]com	Website giả mạo Ngân Hàng TMCP Ngoại thương Việt Nam
9	https://nganhangsaison[.]org/	Website giả mạo Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh
10	https://nang-han-muc-vcs1-khcn-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
11	http://vipcard-vib[.]com/	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
12	https://tpbank[.]chamsocthekhachang-truc-tuyen[.]com/	Website giả mạo Ngân hàng TMCP Tiên Phong
13	https://shinhan[.]chamsoccanhankhachhangthe-tructuyen[.]online	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
14	https://canhanshinhan[.]com	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
15	https://www[.]vnambzuon36sc[.]vip/	Website giả mạo sàn TMĐT Amazon
16	http://sp6788[.]com	Website giả mạo sàn TMĐT Shopee
17	https://vn68822s[.]com/	Website giả mạo sàn TMĐT Shopee
18	https://sp77888[.]com/	Website giả mạo sàn TMĐT Shopee
19	https://tdkd07[.]com	Website giả mạo sàn TMĐT Tiki
20	https://vn147258p[.]com	Website giả mạo sàn TMĐTAmazon



hai ứng dụng có chứa mã độc Anatsa xuất hiện trên cửa hàng Google Play với tên gọi PDF Reader & File Manager và QR Reader & File Manager.



2. Phương thức lừa đảo

Các phương thức chính được các đối tượng lừa đảo trực tuyến sử dụng bao gồm:

1/ Dẫn dụ Quét mã QR hoặc vào các website lừa đảo để lấy cắp thông tin cá nhân (để hack vào các loại tài khoản) từ đây tiếp tục lừa đảo để lấy các mã OTP, mã xác thực,...hoặc hack vào các tài khoản mạng xã hội để làm bàn đạp tiếp tục lừa đảo bạn bè, người thân.

2/ Hướng kết nối vào các ứng dụng chat OTT để thao túng tâm lý (thường như Zalo sau đó dẫn dụ vào các OTT không được kiểm soát khác như Telegram, Viber, WhatsApp… để từ đây áp dụng các kịch bản lừa đảo khác nhau ...)

3/ Lừa nạn nhân cài các ứng dụng giả mạo hoặc kích hoạt tệp tin có chèn mã độc hại (có đuôi như .pdf, .doc, .xlsx, .bat, .zip, .rar, .html, exe...) để chiếm quyền thiết bị từ đó đánh cắp thông tin cá nhân, lấy tiền trong tài khoản, bôi nhọ danh dự hoặc tống tiền…

4/ Tác động tâm lý trực tiếp (qua điện thoại) để chiếm đoạt tiền trực tiếp (qua chuyển khoản hoặc ra ngân hàng gửi tiền cho đối tượng lừa đảo) hoặc dẫn dụ nạn nhân nhập cú pháp chuyển sang eSIM để chiếm đoạt số điện thoại của nạn nhân..

3. Cách thức thực hiện

Đối tượng lừa đảo thường dẫn dụ nạn nhân bằng những cách sau đây (8 cách):

1/ Tạo dựng lòng tin: Giả danh tổ chức uy tín như ngân hàng, cơ quan chính phủ, hoặc công ty nổi tiếng. Đối tượng sử dụng email, tin nhắn, hoặc cuộc gọi để tạo dựng lòng tin và yêu cầu thông tin nhạy cảm từ nạn nhân.

2/ Kịch bản lừa đảo: Được biên soạn sẵn một cách chi tiết, và khéo léo để thao túng tâm lý nhằm mục đích dẫn dụ tạo niềm tin và sự đồng cảm từ nạn nhân. Đóng nhiều vai nhân vật khác nhau để tạo ra một câu chuyện hoàn hảo đánh động vào tâm lý của nạn nhân một cách sâu sắc.

3/ Sử dụng biểu mẫu và giao diện giả mạo: Các trang web lừa đảo thường sao chép giao diện của các trang web chính thức, sử dụng biểu mẫu đăng nhập hoặc thanh toán giống như thật để đánh lừa người dùng.

4/ Kích thích tâm lý: Các đối tượng lừa đảo đa phần đánh vào tâm lý: lòng tham, sự sợ hãi, tính hiếu kỳ, tính tò mò và đặc biệt là tình thương, sự thương hại của con người. Đối tượng thường tạo ra cảm giác khẩn cấp để thúc đẩy nạn nhân hành động ngay lập tức mà không suy nghĩ kỹ lưỡng. Ví dụ, họ có thể thông báo rằng tài khoản của bạn sẽ bị khóa nếu không xác nhận thông tin ngay lập tức.

5/ Đưa ra phần thưởng hoặc cơ hội hiếm có: Hứa hẹn giải thưởng lớn, cơ hội đầu tư sinh lời cao, hoặc cơ hội việc làm hấp dẫn để thu hút sự chú ý của nạn nhân.

6/ Yêu cầu hành động gấp: Đối tượng lừa đảo gửi liên kết đến các trang web giả mạo hoặc mã QR, nơi nạn nhân được yêu cầu nhập thông tin cá nhân hoặc tài khoản. Các liên kết này thường được ngụy trang dưới dạng liên kết hợp pháp hoặc phần thưởng.

7/ Làm giả thông báo khẩn cấp: Sử dụng thông báo giả mạo về sự cố bảo mật, viện cớ lý do nguồn tiền đang bị treo vì phải đóng thuế, cơ quan công an điều tra, lỗi tài khoản, hoặc sự kiện khẩn cấp để yêu cầu nạn nhân cung cấp thông tin ngay lập tức.

8/ Kích thích sự tò mò: Gửi email hoặc tin nhắn về sự kiện, báo cáo, hoặc tài liệu: Đối tượng lừa đảo gửi thông tin về sự kiện nóng hổi, báo cáo quan trọng, hoặc tài liệu hấp dẫn, yêu cầu nạn nhân tải xuống hoặc mở file đính kèm chứa mã độc.

4. Mục đích của đối tượng lừa đảo

Mục tiêu cuối cùng của đối tượng đều là **lừa đảo chiếm đoạt tài sản**. Các đối tượng lừa đảo có thể tìm cách đánh cắp tiền từ tài khoản ngân hàng, ví điện tử, hoặc thẻ tín dụng của nạn nhân thông qua các kỹ thuật như phishing (lừa đảo qua email và tin nhắn), smishing (lừa đảo qua tin nhắn SMS), hoặc vishing (lừa đảo qua điện thoại).

Các yếu tố mà đối tượng tập trung hướng đến để lợi dụng thực hiện các hành vi lừa đảo là tâm lý nhẹ dạ cả tin, thiếu sự tiếp cận thông tin, thiếu việc làm hoặc thu nhập thấp, đánh vào lòng tham ẩn sâu trong mỗi con người.

Cách thức các đối tượng lừa đảo trực tuyến nhận tiền lừa đảo từ nạn nhân bao gồm (04 cách):

1/ 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.

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

3/ Chuyển tiền qua các ví điện tử như Momo, ViettelPay, VNPay…

4/ Chuyển tiền thông qua tiền ảo trên các sàn giao dịch.

KỸ NĂNG PHÁT HIỆN

1. Đối với hình thức lừa đảo Gọi điện trực tiếp

Người dùng có thể phát hiện các cuộc gọi lừa đảo thông qua những dấu hiệu sau đây (4 dấu hiệu):

1/ Cung cấp thông tin không rõ ràng hoặc không chính xác: Đối tượng lừa đảo thường cung cấp thông tin không rõ ràng hoặc mập mờ về mục đích của cuộc gọi, danh tính của mình hoặc tổ chức họ đại diện.

2/ Gây áp lực hoặc tạo cảm giác khẩn cấp: Cuộc gọi lừa đảo thường cố gắng tạo cảm giác khẩn cấp và sự thiếu cảnh giác của nạn nhân, yêu cầu người nhận thực hiện hành động ngay lập tức, thường là chuyển tiền hoặc cung cấp thông tin cá nhân.

3/ Yêu cầu cung cấp thông tin quan trọng và nhạy cảm cá nhân hoặc tài chính: Các đối tượng lừa đảo thường yêu cầu người nhận cung cấp thông tin như số thẻ tín dụng, số tài khoản ngân hàng, số chứng minh nhân dân hoặc các thông tin nhạy cảm khác.

4/ Hứa hẹn lợi ích bất ngờ: Đối tượng lừa đảo có thể hứa hẹn những lợi ích không thực tế, như trúng thưởng, quà tặng hoặc khoản tiền lớn, nhưng yêu cầu người nhận phải trả phí hoặc cung cấp thông tin trước.

2. Đối với hình thức lừa đảo qua Tin nhắn (SMS)/ Email

Để phát hiện hình thức lừa đảo thông qua tin nhắn (SMS)/email, người dùng cần lưu ý những dấu hiệu này (7 dấu hiệu):

1/ Địa chỉ gửi email không chính xác: Kiểm tra địa chỉ email của người gửi. Thông thường, địa chỉ email của các tổ chức uy tín sẽ có tên miền chính thức, còn email giả mạo thường có tên miền không rõ nguồn gốc hoặc không chính xác.

2/ Phần chữ ký và thông tin liên hệ của email không đúng chuẩn format, hoặc đôi khi không có chữ ký và thông tin liên hệ cụ thể như số điện thoại, địa chỉ…

3/ Lỗi chính tả và ngữ pháp: Email lừa đảo thường có lỗi chính tả, ngữ pháp, và cấu trúc câu không chuẩn.

4/ Yêu cầu thông tin cá nhân: Email yêu cầu bạn cung cấp thông tin cá nhân hoặc tài khoản ngân hàng một cách khẩn cấp.

5/ Liên kết, tệp tin đáng ngờ: Các liên kết trong email có thể dẫn đến trang web giả mạo. Di chuột qua liên kết để xem địa chỉ URL thực tế trước khi nhấp vào.

6/ Tệp tin đính kèm đáng ngờ: tệp tin có thể chèn mã độc hại (có đuôi như .pdf, .doc, .xlsx, .bat, .zip, .rar, .html, .exe...), đôi khi là tệp tin đính kèm là file nén có mật khẩu bảo vệ, hoặc tệp tin có kích thước lớn khi được giải nén nhằm vượt mặt sự phát hiện của các bộ máy rà quét mã độc trực tuyến (như Virustotal.com).

7/ Lời hứa về phần thưởng hoặc khuyến mãi bất ngờ: Tin nhắn hứa hẹn bạn thắng giải thưởng lớn hoặc yêu cầu bạn cung cấp thông tin cá nhân để nhận quà.

3. Đối với hình thức lừa đảo qua Mạng xã hội

Sử dụng các nền tảng mạng xã hội để lừa đảo giúp các đối tượng dễ dàng ẩn danh tính và đây là một số dấu hiệu cần lưu ý (5 dấu hiệu):

1/ Lời mời kết bạn, làm quen bất ngờ từ người lạ: Để tạo lòng tin, các đối tượng lừa đảo thường sử dụng hình ảnh chỉn chu, ngoại hình bắt mắt tiếp cận nạn nhân, làm quen một cách bất ngờ.

2/ Dụ dỗ tham gia các hội nhóm đầu tư, làm nhiệm vụ: Gắn mác đầu tư ít, lợi nhuận cao, các đối tượng đánh vào tâm lý muốn kiếm tiền của nạn nhân.

3/ Quảng cáo tuyển dụng hay các dịch vụ hấp dẫn: Các đối tượng lừa đảo thường đăng tải bài viết quảng cáo dịch vụ với nhiều ưu đãi hấp dẫn, mức giá không tưởng như tour du lịch, vé máy bay giá rẻ,… hay tuyển dụng "việc nhẹ lương cao", dịch vụ lấy lại tiền bị lừa,… để chào mời khách hàng nhẹ dạ cả tin trên mạng xã hội.

4/ Lừa đảo video Deepfake: Các đối tượng sử dụng công nghệ trí tuệ nhân tạo (AI) tạo ra những video hoặc hình ảnh giả, sao chép chân dung giả người thân, bạn bè để thực hiện các cuộc gọi lừa đảo trực tuyến.

5/ Yêu cầu đóng cọc trước, chuyển tiền khẩn: Các đối tượng lừa đảo có thể nghĩ ra nhiều lý do để yêu cầu nạn nhân phải chuyển tiền, hoặc giả danh bạn bè, người thân cần vay tiền gấp.

4. Đối với hình thức lừa đảo thông qua Website

Các đối tượng lừa đảo thường sử dụng những website giả mạo để đánh lừa người dùng, dưới đây là các dấu hiệu cần lưu ý để phát hiện kịp thời (9 dấu hiệu):

1/ Địa chỉ trình duyệt (URL) không chính xác: Kiểm tra kỹ địa chỉ URL để đảm bảo nó chính xác và thuộc về trang web chính thức. Các trang web lừa đảo thường có địa chỉ URL tương tự như trang web chính thức nhưng có những thay đổi nhỏ (như thay đổi ký tự, thêm số).

2/ Các đường dẫn có dấu hiệu hoặc ký tự bất thường như lỗi chính tả (Sai khác, thiếu hoặc thừa một vài ký tự, hoặc thay thế một vài ký tự với ký tự); Tên miền có tiền tố hoặc hậu tố sử dụng ký tự lạ; Tên miền phụ cố bắt chước tên miền của một trang hợp pháp…

3/ Độ tin cậy của domain: Các đuôi trang .com, .org, .gov (chính phủ), .edu (giáo dục đào tạo)… thường là những top-level domain có thể tin cậy được, tuy nhiên cũng cần phải cẩn trọng khi truy cập nếu thấy có dấu hiệu khả nghi về việc lấy cắp hay thu thập thông tin dữ liệu cá nhân; Các đuôi top-level domain ít phổ biến như .info, .asia, .vip, .tk, .xyz… thường có độ tin cậy khá thấp; Một số đường dẫn sử dụng tên miền quốc tế (IDN) để đánh lừa nạn nhân hoặc sử dụng dịch vụ rút gọn tên miền; Sử dụng tên miền dài khiến người dùng nhầm lẫn; Đường dẫn open redirector nhằm đánh lừa nạn nhân sau đấy điều hướng nạn nhân sang một trang khác để lừa đảo…

4/ Thiếu chứng chỉ SSL: Trang web chính thức thường có chứng chỉ SSL, biểu thị bằng khóa an toàn và “https” thay vì “http” trong địa chỉ URL.

5/ Thiết kế kém chất lượng: Trang web lừa đảo thường có thiết kế kém, hình ảnh không đúng quy chuẩn thương hiệu, lỗi chính tả, và thiếu chuyên nghiệp. Nguyên nhân là do các trang web giả mạo thường không kiểm duyệt kỹ nội dung. Hoặc các trang này được tạo bởi đối tượng ở nước ngoài không thành thạo ngôn ngữ được sử dụng để lừa đảo.

6/ Cảnh báo, đe dọa, quảng cáo: Website lừa đảo khi truy cập thường xuất hiện cảnh báo, đe dọa hoặc các chương trình trúng thưởng với phần quà hấp dẫn mục đích dẫn dụ người dùng truy cập các liên kết không an toàn.

7/ Chứng nhận Tín nhiệm mạng: Tín nhiệm mạng chứng nhận độ tin cậy về ATTT cho các đối tượng trên không gian mạng. Các website của cơ quan nhà nước đều sẽ được cấp chứng nhận tín nhiệm mạng. Người dùng cần đối chiếu kỹ càng với tín nhiệm mạng để đảm bảo website truy cập đủ tin cậy.

8/ Chứng nhận của Bộ Công Thương: Doanh nghiệp bắt buộc phải khai báo tên miền và trang web với Bộ Công Thương. Nếu không có chứng nhận này thì trang web chưa đủ độ tin cậy.

9/ Yêu cầu thông tin cá nhân ngay lập tức: Trang web yêu cầu bạn nhập thông tin cá nhân hoặc tài khoản ngân hàng ngay lập tức mà không có bất kỳ lý do hợp lý nào.

5. Đối với hình thức lừa đảo thông qua Phần mềm, ứng dụng giả mạo

Sử dụng các phần mềm, ứng dụng giả mạo là một trong những phương thức lừa đảo của các đối tượng, bởi vậy người dùng cần xây dựng kỹ năng phát hiện kịp thời và chú ý các dấu hiệu sau (5 dấu hiệu):

1/ Tải từ nguồn không chính thức: Nếu ứng dụng không được tải từ các cửa hàng ứng dụng chính thức như Google Play, CH Play hoặc App Store, đó có thể là dấu hiệu của ứng dụng giả mạo. Nếu ứng dụng được tải về dưới dạng đuôi file .apk (Dichvucong.apk) hoặc .mobileconfig thì tuyệt đối không nên cài đặt.

2/ Yêu cầu quyền truy cập không cần thiết: Nếu ứng dụng yêu cầu quyền truy cập vào các thông tin hoặc chức năng không liên quan đến mục đích chính của nó (như quyền truy cập danh bạ, tin nhắn, vị trí), đây có thể là dấu hiệu của phần mềm độc hại.

3/ Giao diện kém chất lượng: Ứng dụng giả mạo thường có giao diện kém chất lượng hoặc không chuyên nghiệp, nội dung chứa lỗi chính tả.

4/ Tính năng không rõ ràng: Nếu tính năng của ứng dụng không rõ ràng hoặc không giống như quảng cáo, có thể là dấu hiệu của phần mềm giả mạo.

5/ Thông tin nhà phát triển không được xác minh: Nhà phát triển ứng dụng không có trang web chính thức hoặc thông tin liên hệ rõ ràng.

KỸ NĂNG XỬ LÝ

1. Xử lý khi gặp lừa đảo trực tuyến

1/ Chủ động chặn các tin nhắn cuộc gọi: Khi được tiếp cận bởi các tin nhắn, cuộc gọi có dấu hiệu lừa đảo, người dân nên chủ động ngắt liên lạc, chặn tin nhắn.

2/ Báo cáo các tin nhắn, cuộc gọi: Chặn và báo cáo các tin nhắn có dấu hiệu lừa đảo trên các nền tảng mạng xã hội. Đối với các cuộc gọi điện, lưu lại số điện thoại của các đối tượng và trình báo với cơ quan công an nhằm kiểm tra và bắt giữ.

3/ Tìm kiếm thông tin trên mạng: Tìm kiếm các phương thức, thông tin liên quan tới hành vi lừa đảo, rất có thể hành vi đó đã được báo cáo và đăng tải bởi các cơ quan truyền thông hoặc nạn nhân khác.

4/ Gửi cảnh báo về Trang cảnh báo an toàn thông tin Việt Nam tại địa chỉ canhbao.khonggianmang.vn

2. Xử lý sau khi bị lừa đảo trực tuyến

2.1 Trường hợp bị dẫn dụ chuyển tiền cho các đối tượng lừa đảo:

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:

1/ Dừng chuyển tiền, tuyệt đối không tiếp tục làm theo lời dẫn dụ của đối tượng lừa đảo.

3/ Liên hệ ngay lập tức với ngân hàng và tổ chức tài chính để báo cáo lừa đảo và yêu cầu họ dừng mọi giao dịch.

4/ 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.

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

6/ 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.

2.2 Trường hợp bị mất các thông tin đăng nhập, chiếm quyền điều khiển thiết bị:

Trong trường hợp các đối tượng lừa đảo có thông tin đăng nhập tài khoản hay chiếm được quyền điều khiển thiết bị và thực hiện hành vi chiếm đoạt tài sản, người dùng cần:

1/ Liên hệ với ngân hàng hoặc các đơn vị tài chính: Trong trường hợp thông tin tài chính bị đối tượng lừa đảo chiếm đoạt, liên hệ ngay với ngân hàng hoặc các đơn vị tài chính để thông báo về sự cố và khóa tài khoản. Điều này sẽ giúp ngăn chặn các đối tượng thực hiện giao dịch trái phép.

2/ Thay đổi toàn bộ mật khẩu có độ khó cao, trên 12 ký tự (bao gồm chữ số chữ hoa, chữ thường và các ký tự đặc biệt) đồng thời bật tính năng bảo mật hai bước trên các nền tảng trực tuyến đang sử dụng.

3/ Kiểm tra thiết bị và hệ thống: Sử dụng phần mềm diệt virus và các công cụ bảo mật khác để quét thiết bị nhằm phát hiện và loại bỏ phần mềm độc hại.

4/ Cài đặt lại hệ thống thiết bị: Trong trường hợp nhận thấy thiết bị có dấu hiệu bị xâm nhập, người dân nên đặt lại dữ liệu, đưa thiết bị về trạng thái nguyên bản nhằm loại bỏ các phần mềm độc hại, ngăn không cho đối tượng thực hiện hành truy cập vào các tài khoản trực tuyến.

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

6/ Giám sát tài khoản và tín dụng: Theo dõi tài khoản ngân hàng và báo cáo tín dụng để phát hiện các hoạt động bất thường hoặc trái phép.

7/ Gửi cảnh báo về Trang cảnh báo an toàn thông tin Việt Nam tại địa chỉ canhbao.khonggianmang.vn

8/ Học hỏi từ kinh nghiệm: Xem xét lại cách thức lừa đảo nhằm phòng tránh các tình huống tương tự trong tương lai. Theo dõi kênh thông tin Cổng không gian mạng quốc gia trên Facebook, TikTok để cập nhật các tin tức an toàn thông tin, đặc biệt là lừa đảo trực tuyến.

KỸ NĂNG PHÒNG TRÁNH

1. Kỹ năng phòng tránh 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, người dùng cần:

1/ 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.

2/ Cảnh giác với người lạ kết bạn qua mạng xã hội, qua Zalo, 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.

3/ 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.

4/ 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.

5/ Cảnh giác với những yêu cầu đặt cọc hoặc chuyển khoản trước: 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.

6/ 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. **Theo dõi và cập nhật tại kênh thông tin Cổng không gian mạng quốc gia (Facebook/TikTok) hoặc website Khonggianmang.vn**

2. Kỹ năng phòng tránh 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:

1/ 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.

2/ 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.

3/ 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.

4/ 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.

5/ 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.

6/ 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.

KỸ NĂNG BẢO VỆ

1. “Nguyên tắc vàng” bảo vệ bản thân khỏi lừa đảo trực tuyến

Nguyên tắc 1: *Hãy chậm lại*

Những đối tượng lừa đảo thường tạo ra cảm giác cấp bách để chúng có thể vượt qua khả năng nhận định của bạn. Những cuộc gọi, tin nhắn... thúc giục phải hành động nhanh như: thời gian khuyến mãi đã hết; nếu không chuyển tiền bây giờ bạn và người thân phải thực hiện các thủ tục tố tụng...

Trong tình huống này, bạn hãy dành thời gian suy nghĩ kỹ và đặt câu hỏi tìm hiểu kỹ nội dung, thông tin để tránh bị dồn vào tình huống xấu.

Nguyên tắc 2*: Kiểm tra tại chỗ*

Tìm hiểu thêm để xác thực thông tin bạn đang nhận được. Nếu bạn nhận được một cuộc gọi không mong muốn, hãy tra cứu số ngân hàng, cơ quan, hoặc tổ chức đang gọi đến và liên hệ lại trực tiếp.

Nguyên tắc 3*: Dừng lại! Không gửi*

Không một cá nhân hoặc cơ quan nào yêu cầu thanh toán ngay tại chỗ. Vì vậy, nếu bạn cảm thấy giao dịch không đáng tin, hãy dừng lại vì có thể đây là dấu hiệu lừa đảo.

2. Quy tắc “6 KHÔNG”

1/ KHÔNG cung cấp thông tin cá nhân, địa chỉ, số điện thoại, số tài khoản ngân hàng của mình cho đối tượng không quen biết; thận trọng rà soát và kiểm tra kỹ thông tin trước khi thực hiện các giao dịch chuyển tiền.

2/ KHÔNG kết bạn và nói chuyện với người lạ, đặc biệt là những tài khoản có hình ảnh ngoại hình đẹp và bắt mắt. Tuyệt đối không nhận lời mời tham gia các hội nhóm mà không rõ mục đích đối tượng.

3/ KHÔNG truy cập, đăng nhập vào các đường dẫn, liên kết, website, ứng dụng hoặc mở tệp đính kèm đến từ người gửi không xác định, không rõ nguồn gốc.

4/ KHÔNG cán bộ cơ quan nhà nước, bộ công an, viện kiểm sát, tòa án hay đơn vị tài chính… nào gọi điện để điều tra qua điện thoại, yêu cầu phải cung cấp thông tin cá nhân hay đóng tiền.

5/ KHÔNG thực hiện chuyển khoản trước, tuyệt đối không đặt cọc, chuyển khoản tiền cho các đối tượng lạ trong bất cứ trường hợp nào.

6/ KHÔNG tham lam những tài sản, món quà không rõ nguồn gốc có thể nhận được một cách dễ dàng, những lợi nhuận "phi thực tế" mà không tốn sức lao động, những lời mời chào, dụ dỗ "việc nhẹ lương cao"...

Trân trọng cảm ơn!