BỘ CÔNG AN
CÔNG AN TỈNH BẮC KẠN

SỔ TAY PHÒNG, CHỐNG TỘI PHẠM LỪA ĐẢO TRÊN KHÔNG GIAN MẠNG

1 Lừa đảo gửi quà, tiền từ nước ngoài về Việt Nam

2 Giả danh cán bộ cơ quan Nhà nước gọi điện để lừa đảo

3 Lừa vay tiền online

4 Giả người thân nhờ chuyển tiền, vay tiền

5 Giả tuyển cộng tác viên bán hàng online, làm nhiệm vụ

6 Kinh doanh đa cấp trên các sàn giao dịch tiền ảo, sàn ngoại hối chưa được cấp phép

7 Cảnh báo ứng dụng VNeID giả mạo

8 Bẫy tình

9 Gọi video có hình ảnh của lãnh đạo, người quen để lừa đảo

10 Giả mạo trang thông tin điện tử cơ quan doanh nghiệp ngân hàng

11 Chiêu lừa "Gái gọi" qua mạng

12 Dịch vụ lấy lại tiền khi bị lừa

- Địa chỉ liên hệ:
+ https://www.facebook.com/congnghecaobackan
+ Đường dây nóng: 069.2549.005
- Quét QR Code bằng máy ảnh điện thoại thông minh có Internet để truy cập vào cẩm nang phòng, chống tội phạm

CẢNH BÁO THỦ ĐOẠN LỪA ĐẢO PHỔ BIẾN TRÊN KHÔNG GIAN MẠNG

1 Lừa đảo gửi quà, tiền từ nước ngoài về Việt Nam

THỦ ĐOẠN

- Đối tượng sử dụng mạng xã hội Facebook, Zalo… giả làm người nước ngoài, Việt kiều để kết bạn, trò chuyện với người dân để tạo sự tin tưởng, qua đó thể hiện sự mong muốn được gửi quà, tiền có giá trị lớn từ nước ngoài cho người dân.
- Một số đối tượng khác giả danh nhân viên sân bay, hải quan gọi điện yêu cầu nạn nhân nộp tiền để làm thủ tục thông quan, nhận hàng có giá trị lớn nhưng đang bị giữ ở sân bay, tàu, cảng.
- Sau khi chuyển tiền, đối tượng sẽ tiếp tục "chèo kéo" để lừa số tiền lớn hơn hoặc cắt đứt liên lạc.

KHUYẾN CÁO

- Chúng ta có thể kết bạn, tạo mối quan hệ với người khác trên Internet, nhưng tuyệt đối không chuyển tiền để nhận các loại quà, vì có nguy cơ cao là lừa đảo.

2 Giả danh cán bộ cơ quan Nhà nước gọi điện để lừa đảo

THỦ ĐOẠN

- Đối tượng giả danh cán bộ công an, viện kiểm sát, tòa án gọi điện, nhắn tin thông báo người dân có liên quan đến vụ án, vụ việc đang điều tra; đe dọa, yêu cầu người dân chuyển tiền vào tài khoản của đối tượng để "xác minh, kiểm tra nguồn gốc tiền" nếu không sẽ thực hiện lệnh bắt, giữ.
- Giả danh nhân viên ngân hàng thông báo tài khoản của người dân đang bị "treo", yêu cầu cung cấp thông tin đăng nhập, mã OTP để kiểm tra lỗi.
- Trong một số trường hợp, đối tượng đề nghị người dân cài đặt phần mềm giả mạo Bộ Công an, yêu cầu người dân điền thông tin cá nhân, tài khoản ngân hàng; sau đó, chúng sử dụng các thông tin này để chiếm đoạt số tiền trong tài khoản ngân hàng.

KHUYẾN CÁO

- Cơ quan Nhà nước không gọi điện, nhắn tin yêu cầu người dân chuyển tiền vào tài khoản với bất cứ lý do gì. Mọi trường hợp đều làm việc trực tiếp tại trụ sở cơ quan Nhà nước hoặc nơi người dân cư trú.
- Tuyệt đối không làm theo yêu cầu cung cấp thông tin cá nhân, tài khoản ngân hàng , mật khẩu, mã OTP cho các đối tượng lạ; cần thông báo lực lượng Công an nơi gần nhất để được giúp đỡ.

CẢNH BÁO THỦ ĐOẠN LỪA ĐẢO PHỔ BIẾN TRÊN KHÔNG GIAN MẠNG

3 Lừa vay tiền online

THỦ ĐOẠN

- Lợi dụng mạng xã hội Facebook, Zalo... đối tượng tạo các tài khoản giống nhân viên ngân hàng, công ty tài chính và đăng tải thông tin hỗ trợ vay tiền online, giải ngân nhanh với thủ tục nhanh gọn, không cần thế chấp tài sản.
- Chúng hướng dẫn người dân truy cập vào website hoặc tải ứng dụng điện thoại để vay tiền. Sau khi người dân điền thông tin, đến bước chuyển tiền về tài khoản thì website hoặc ứng dụng sẽ hiện thông báo người dân cần nộp phí bảo hiểm để nhận được tiền vay, hoặc người dân đặt sai lệnh nên hệ thống lỗi, không thể giải ngân.
- Đề nghị bị hại đóng các khoản phí để làm bảo hiểm khoản vay hoặc làm lại thủ tục vay rồi chiếm đoạt số tiền này.

KHUYẾN CÁO

- Không vay tiền online từ các ứng dụng, trang web trôi nổi trên không gian mạng, không rõ nguồn gốc, không được Nhà nước công nhận.
- Nếu có nhu cầu vay tiền thì liên hệ và trực tiếp đến ngân hàng, các tổ chức tín dụng gần nhất để được hỗ trợ.

4 Giả người thân nhờ chuyển tiền, vay tiền

THỦ ĐOẠN

- Đối tượng lập tài khoản mạng xã hội hoặc chiếm quyền sử dụng tài khoản mạng xã hội (hack) của người khác.
- Sử dụng tài khoản này, đối tượng nhắn tin cho người thân, bạn bè trong danh sách liên lạc để hỏi vay tiền, hoặc nhờ chuyển tiền.

KHUYẾN CÁO

- Sử dụng mật khẩu 2 lớp đối với các tài khoản mạng xã hội (có thể sử dụng Google tìm kiếm từ khóa "mật khẩu 2 lớp" và làm theo hướng dẫn).
- Khi thấy người thân nhắn tin, gọi điện nhờ chuyển tiền vào tài khoản ngân hàng lạ thì khả năng cao là lừa đảo.
- Xác minh trước khi chuyển tiền bằng cách gọi vào số điện thoại của người thân để nói chuyện (lưu ý: Gọi số điện thoại, không gọi qua ứng dụng mạng xã hội).

CẢNH BÁO THỦ ĐOẠN LỪA ĐẢO PHỔ BIẾN TRÊN KHÔNG GIAN MẠNG

5 Giả tuyển cộng tác viên bán hàng online, làm nhiệm vụ

THỦ ĐOẠN

- Đối tượng mạo danh nhân viên của các trang thương mại điện tử để lôi kéo cộng tác viên bán hàng online với hoa hồng hấp dẫn.
- Yêu cầu cộng tác viên phải thanh toán tiền đơn hàng trước mới nhận được tiền gốc và hoa hồng.
- Ban đầu, chúng thanh toán cho cộng tác viên từ 1-3 đơn hàng có giá trị thấp.
- Sau đó, chúng dụ dỗ cộng tác viên chuyển các khoản tiền lớn để mua các đơn hàng có giá trị cao rồi chiếm đoạt.

KHUYẾN CÁO

- Nên kiểm tra kỹ các thông tin trước khi nhận làm cộng tác viên hoặc trước khi chuyển tiền.
- Việc chuyển một khoản tiền nào đó thường khó phát sinh lợi nhuận cho người chuyển; do vậy, cần cảnh giác với đa số lời quảng cáo tuyển cộng tác viên làm việc online.

6 Kinh doanh đa cấp trên các sàn giao dịch tiền ảo, sàn ngoại hối chưa được cấp phép

THỦ ĐOẠN

- Đối tượng lập ra các website tài chính, ứng dụng có giao diện tương tự sàn đầu tư tài chính quốc tế rồi lôi kéo người tham gia.
- Chúng cam kết người chơi có thể rút vốn bất kỳ lúc nào, không cần đầu tư trí tuệ, thời gian, nếu kêu gọi được thêm người sẽ có hoa hồng.
- Sau một thời gian sàn giao dịch thông báo dừng hoạt động để bảo trì hoặc lỗi không truy cập được.
- Khách hàng không đăng nhập được để rút tiền hoặc mất hết tiền kỹ thuật số trong tài khoản.

KHUYẾN CÁO

- Không tham gia vào các sàn giao dịch tiền ảo, tiền ngoại hối không được Nhà nước cấp phép.

CẢNH BÁO THỦ ĐOẠN LỪA ĐẢO PHỔ BIẾN TRÊN KHÔNG GIAN MẠNG

7 Cảnh báo ứng dụng VNeID giả mạo

THỦ ĐOẠN

- Đối tượng giả danh Cơ quan Công an gọi điện cho người dân hướng dẫn kích hoạt định danh điện tử.
- Lừa người dân cài đặt ứng dụng VNeID giả mạo do đối tượng cung cấp.
- Đối tượng sử dụng ứng dụng VNeID giả mạo chiếm quyền điều khiển của điện thoại di động nạn nhân, sau đó tiến hành truy cập vào tài khoản ngân hàng nạn nhân và thực hiện chiếm đoạt toàn bộ số tiền có trong tài khoản.

KHUYẾN CÁO

- Chỉ cài đặt các ứng dụng VNeID từ nguồn chính thống trên App Store (đối với hệ điều hành IOS dành cho điện thoại Iphone) và CH Play (đối với điện thoại sử dụng hệ điều hành Android). Tuyệt đối không cài đặt ứng dụng VNeID không rõ nguồn gốc, từ các đường link do đối tượng cung cấp.
- Không bật chế độ cài đặt ứng dụng từ nguồn không xác định (trên điện thoại Android và xác thực độ tin cậy (đối với điện thoại Iphone) gây nguy cơ mất an toàn cho thiết bị và thận trọng khi cung cấp thông tin cá nhân qua điện thoại.
- Khi người dân nhận được các cuộc gọi của đối tượng nghi giả danh cán bộ Công an kích hoạt định danh điện tử cần liên hệ với Cơ quan Công an nơi gần nhất hoặc liên hệ đường dây nóng 1900.0368 để được hướng dẫn (Tổng đài duy nhất hướng dẫn VNeID).

8 Bẫy tình

THỦ ĐOẠN

- Kẻ lừa đảo xây dựng hồ sơ ảo, thông tin giả mạo sau đó tiến hành tìm hiểu và tiếp cận nạn nhân thông qua các kênh trực tuyến, mạng xã hội Facebook, app hẹn hò….
- Tạo một mối quan hệ tình cảm giả với nạn nhân, dùng lời nói thân mật để tán tỉnh, chia sẻ câu chuyện cảm động hoặc đưa ra lời hứa.
- Dẫn dụ nạn nhân gửi hình ảnh, video nhạy cảm, sau đó dúng lời lẽ ngon ngọt rủ rê nạn nhân tham gia đầu tư trực tuyến để lừa đảo. Khi không rủ rê được, kẻ lừa đảo sẽ dùng những hình ảnh nhạy cảm của nạn nhân để khống chế, tống tiền.

KHUYẾN CÁO

- Cần cảnh giác, không nên nhanh tin tưởng vào một người mà bạn mới gặp qua mạng xã hội hoặc các nền tảng trực tuyến khác vì các đối tượng lừa đảo tình cảm thường bắt đầu bằng việc tạo một mối quan hệ gần gũi, đồng cảm để lấy lòng và đánh lừa nạn nhân.
- Không gửi thông tin cá nhân nhạy cảm, hình ảnh riêng tư cho người khác trên mạng.
- Hãy cảnh giác với những yêu cầu gửi tiền, đầu tư vào các sản giao dịch, tiền ảo... Đối tượng lừa đảo thường sử dụng chiêu trò hứa hẹn lợi nhuận cao hoặc cơ hội đầu tư hấp dẫn để chiếm đoạt tài sản của nạn nhân.

CẢNH BÁO THỦ ĐOẠN LỪA ĐẢO PHỔ BIẾN TRÊN KHÔNG GIAN MẠNG

9 Gọi video có hình ảnh của lãnh đạo, người quen để lừa đảo

THỦ ĐOẠN

- Đối tượng sử dụng công nghệ trí tuệ nhân tạo (AI) để tạo ra những video hoặc hình ảnh giả, sao chép chân dung tạo ra đoạn video giả danh cán bộ cơ quan nhà nước để gọi điện yêu cầu nạn nhân chuyển tiền vào tài khoản hoặc cung cấp thông tin tài khoản ngân hàng; giả người thân nhờ chuyển tiền, vay tiền.

DẤU HIỆU NHẬN BIẾT

- Thời gian gọi thường rất ngắn chỉ vài giây.
- Khuôn mặt người gọi thiếu tính cảm xúc và khá "trơ" khi nói, hoặc tư thế trông lúng túng, không tự nhiên, hoặc hướng đầu và cơ thể của họ trong video không nhất quán với nhau...
- Màu da của nhân vật trong video bất thường, ánh sáng kỳ lạ và bóng đỏ không đúng vị trí, video trông rất giả tạo và không tự nhiên.
- Âm thanh sẽ không đồng nhất với hình ảnh, có nhiều tiếng ồn bị lạc vào clip hoặc clip không có âm thanh.
- Ngắt máy giữa chừng với lý do mất sóng, sóng yếu...

KHUYẾN CÁO

- Khi nhận thấy các yếu tố bất thường về thời gian cuộc gọi, khuôn mặt, màu da, âm thanh, kết nối kém đều là dấu hiệu của deepfake, người dân cần cảnh giác.
- Đối với các công việc có liên quan đến cán bộ Nhà nước, người dân có thể yêu cầu gặp mặt trực tiếp để làm việc; đối với người dân trong gia đình chúng ta có thể gọi vào số điện thoại trong danh bạ để xác minh.

CẢNH BÁO THỦ ĐOẠN LỪA ĐẢO PHỔ BIẾN TRÊN KHÔNG GIAN MẠNG

10 Giả mạo trang thông tin điện tử cơ quan doanh nghiệp ngân hàng

THỦ ĐOẠN

- Đối tượng xấu lập ra các website, trang thông tin điện tử có hình thức giao diện tương tự website, cơ quan nhà nước, doanh nghiệp, ngân hàng.
- Sau đó tìm kiếm lý do, phương pháp gửi đường link cho nạn nhân truy cập trang thông tin điện tử và yêu cầu cung cấp thông tin cá nhân, số tài khoản ngân hàng, mã OTP...

DẤU HIỆU NHẬN BIẾT

- Các website giả mạo thường có giao diện gần giống nhưng không giống hoàn toàn so với website chính thống.
- Tên miền truy cập website giả mạo thường có những ký tự lạ hoặc có đuôi tên miền không phổ biến như .biz.site.info...

KHUYẾN CÁO

- Tuyệt đối không truy cập các đường link lạ, không cung cấp thông tin cá nhân, số tài khoản, mã OTP... cho các website lừa đảo.
- Khi có công việc liên quan, người dân cần trực tiếp liên hệ với cơ quan, đơn vị, ngân hàng để xác minh thông tin.

CẢNH BÁO THỦ ĐOẠN LỪA ĐẢO PHỔ BIẾN TRÊN KHÔNG GIAN MẠNG

11 Chiêu lừa "Gái gọi" qua mạng

THỦ ĐOẠN

- Chúng dụ dỗ bằng các quảng cáo khêu gợi, "mát mẻ" trên MXH. Khi con mồi tương tác sẽ được gửi hình ảnh các cô gái đẹp, khêu gợi và yêu cầu mở thẻ VIP để "hẹn hò".
- Nạn nhân bị đưa vào các nhóm chat kín để "cò mồi" dụ dỗ nạp tiền bình chọn, đánh giá người đẹp. Ban đầu sẽ nhận được "hoa hồng" thật.
- Khi nạp đến một số tiền nhất định, chúng đưa ra các lý do để yêu cầu tiếp tục chuyển khoản, nếu không sẽ mất số tiền trước đó.
- Thậm chí chúng đe dọa tung nội dung nhắn tin nhạy cảm lên mạng xã hội để "tống tiền" nạn nhân.

KHUYẾN CÁO

- Không tham gia hoạt động mại dâm, đồi trụy trên KGM.

12 Dịch vụ lấy lại tiền khi bị lừa

THỦ ĐOẠN

- Lợi dụng sự hoang mang của nạn nhân sau khi bị lừa đảo, các đối tượng giả dạng luật sư, công an, cán bộ ngân hàng, tự xưng là các "chuyên gia" dụ dỗ nạn nhân tiếp tục chuyển tiền để có thể lấy lại số tiền đã mất trước đó.
- Trong giai đoạn đầu, các "chuyên gia" này luôn nhấn mạnh việc sẽ thu hồi được tiền lừa đảo giúp nạn nhân mà không cần mất một đồng tiền phí nào. Tuy nhiên, các đối tượng sử dụng các chiêu trò để bịa ra một lý do phù hợp, đẩy cho nạn nhân một lỗi nào đó và yêu cầu người này phải chuyển khoản tiền phí nhằm vắt kiệt nạn nhân đến đồng tiền cuối cùng.

KHUYẾN CÁO

- Sau khi trở thành nạn nhân của các vụ lừa đảo, người dân nên lập tức trình báo cho cơ quan chức năng tại địa phương. Thay vì đưa thông tin các nhân, vụ việc của mình lên mạng xã hội để rồi bị các đối tượng giả danh luật sư, chuyên gia kinh tế, nhân viên ngân hàng... lừa đảo lần thứ 2.

Chịu trách nhiệm xuất bản:
Thượng tá NGUYỄN VĂN TUẤN - Trưởng phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh Bắc Kạn

* Giấy phép xuất bản số /GP-STTTT do Sở Thông tin và Truyền thông Bắc Kạn cấp ngày .../6/2024.
* In 11.500 bản, khổ 14,5x20,5cm tại Công ty cổ phần In Bắc Kạn, địa chỉ: Số 463, tổ 11C, P. Đức Xuân, TP Bắc Kạn. In xong và nộp lưu chiểu tháng 6 năm 2024.

XUẤT BẢN PHẨM KHÔNG BÁN