ĐỀ CƯƠNG TUYÊN TRUYỀN
Một số phương thức, thủ đoạn của tội phạm sử dụng công nghệ cao lừa đảo, chiếm đoạt tài sản và biện pháp phòng tránh

I. MỘT SỐ PHƯƠNG THỨC, THỦ ĐOẠN CỦA TỘI PHẠM SỬ DỤNG CÔNG NGHỆ CAO LỪA ĐẢO, CHIẾM ĐOẠT TÀI SẢN

1. Làm giả tài khoản mạng xã hội của nạn nhân bằng cách lập tài khoản với ảnh đại diện là ảnh của nạn nhân, sau đó kết bạn với những người trong danh sách bạn bè của nạn nhân và nhắn tin vay mượn tiền, nhờ chuyển tiền. Để tạo lòng tin, đối tượng lợi dụng công nghệ Deepfake làm giả cuộc gọi video để lừa đảo nạn nhân (Deepfake là công nghệ trí tuệ nhân tạo dựa trên tệp tin hình ảnh khuôn mặt, giọng nói của một người ngoài đời thực, sử dụng thuật toán để tái tạo lại khuôn mặt và giọng nói phù hợp với nét mặt, biểu cảm của một người khác; sau đó tại ra video giả mạo hoàn toàn người đó ngoài đời thực).

2. Chiếm quyền điều khiển tài khoản mạng xã hội của người dùng, sau đó nhắn tin lừa đảo, mượn tiền mọi người trong danh sách bạn bè của nạn nhân.

3. Mạo danh nhân viên nhà mạng để yêu cầu cung cấp thông tin cá nhân, mã OTP

Đối tượng mạo danh nhân viên nhà mạng thực hiện các cuộc gọi lừa đảo đến người dân với các nội dung như: "Phải phối hợp để đối soát thông tin nếu không sẽ bị khóa sim 2 chiều", "nếu không hợp tác thì sẽ bị mời lên làm việc tại cơ quan Công an"… Sau đó yêu cầu người dân cung cấp thông tin cá nhân, mã otp để chiếm quyền sử dụng sim điện thoại, từ đó đăng nhập các ví điện tử hoặc tài khoản ngân hàng của người dân để chiếm đoạt tài sản.

4. Giả danh cán bộ ngành Công an, Viện kiểm sát, Tòa án nhắn tin, gọi điện báo đang điều tra vụ án có liên quan đến tài khoản ngân hàng của nạn nhân và yêu cầu nạn nhân chuyển tiền đến số tài khoản của đối tượng để điều tra làm rõ, sau khi điều tra làm rõ sẽ được trả lại tiền.

5. Giả danh người nước ngoài nhắn tin làm quen và gửi quà tặng về Việt Nam, sau đó giả danh nhân viên sân bay, hải quan, nhân viên thuế... để yêu cầu nạn nhân chuyển tiền nộp phí, nộp phạt để chiếm đoạt tài sản.

6. Bẫy tình: Đối tượng tiếp cận, làm quen nạn nhân qua mạng xã hội, bày tỏ tình cảm, sau đó dùng nhiều lý do yêu cầu nạn nhân chuyển tiền hoặc rủ rê tham gia đầu tư tài chính, tiền ảo để lừa đảo, chiếm đoạt tài sản.

7. Giả danh hải quan, cơ quan công an đăng tin thanh lý xe "trốn thuế", yêu cầu người mua đặt cọc tiền trước khi giao dịch, sau đó chặn liên lạc để chiếm đoạt tài sản.

8. Đăng tin tuyển mẫu ảnh nhí, công việc đơn giản, thu nhập cao

Lợi dụng tâm lý của các bà mẹ muốn con được làm mẫu ảnh và có thêm thu nhập, đối tượng đăng tin tuyển mẫu ảnh nhí với yêu cầu đơn giản và hứa hẹn mức thu nhập. Sau khi nạn nhân liên hệ, đối tượng yêu cầu nạn nhân tham gia nhóm chat và yêu cầu nộp phí làm hồ sơ hoặc làm nhiệm vụ theo yêu cầu (thường là chuyển khoản mua các sản phẩm theo yêu cầu và hứa hẹn sẽ được hoàn lại tiền cùng hoa hồng).

9. Chiếm đoạt tài khoản ngân hàng của nạn nhân bằng một số hình thức như giả danh ngân hàng gửi liên kết yêu cầu cập nhật tài khoản, xác nhận chuyển tiền quốc tế, sau đó truy cập trái phép vào tài khoản ngân hàng để thực hiện giao dịch chuyển tiền, chiếm đoạt tiền trong tài khoản.

10. Cố ý chuyển nhầm tiền vào tài khoản của người dân, sau khi người nhận nhận được tiền, đối tượng sẽ giả danh là người thu hồi nợ của một công ty tài chính để liên hệ, dọa nạt và yêu cầu họ trả lại số tiền đã nhận như một khoản vay cùng với số lãi cắt cổ.

11. Mạo danh giáo viên, nhân viên y tế, nhân viên bệnh viện báo tin học sinh bị tai nạn đang ở bệnh viện, lợi dụng tình trạng hoang mang, lo lắng, thiếu tỉnh táo của phụ huynh học sinh, yêu cầu chuyển tiền gấp để cấp cứu, làm phẫu thuật,… (Thủ đoạn này thời gian qua xảy ra nhiều ở khu vực TP Hồ Chí Minh và các tỉnh phía Nam).

12. Lừa đảo đầu tư tài chính, tiền ảo

Các cá nhân hoặc tổ chức lập các trang web đầu tư tài chính, ứng dụng có giao diện tương tự đầu tư tài chính quôc tế rồi dán nhãn đầu tư làm giàu nhanh, đầu tư 4.0 hoặc đầu tư thông minh, đầu tư thụ động lãi suất cao... trên các thị trường tài chính như chứng khoán, tiền tệ (forex), tiền ảo (crypto) để thu hút nhà đầu tư, thường là những cá nhân nhỏ lẻ, bỏ tiền vào nhằm kiếm lợi nhuận với cam kết người chơi sẽ được hưởng mức lãi suất cao nhưng an toàn, có thể rút vốn bất kỳ lúc nào, không cần đầu tư trí tuệ, thời gian. Thời gian đầu, các đối tượng cho nạn nhân rút tiền để tạo lòng tin và tiếp tục đầu tư số tiền lớn hơn. Sau một thời gian, sàn giao dịch thông báo ngừng hoạt động để bảo trì hoặc lỗi không truy cập được, khách hàng không đăng nhập được để rút tiền trong tài khoản mới biết mình bị lừa.

13. Lừa vay vốn qua mạng

13.1. Lợi dụng nhu cầu vay vốn của người dân, đối tượng sử dụng tài khoản mạng xã hội Facebook đăng tải bài viết vào nhiều Nhóm, Fanpage với nội dung "Cho vay tiền, chỉ cần cung cấp CMND, không cần tiền đặt cọc, không gọi điện

làm phiền…" Khi nạn nhân liên hệ, đối tượng yêu cầu cung cấp thông tin về tài khoản ngân hàng, chụp ảnh CMND/CCCD, số điện thoại liên hệ. Sau đó đối tượng sử dụng số điện thoại của nạn nhân để đăng nhập ví điện tử của nạn nhân, yêu cầu nạn nhân cung cấp mã OTP và chiếm đoạt quyền sử dụng ví điện tử của nạn nhân. Trường hợp ví điện tử đã liên kết tài khoản ngân hàng, đối tượng sẽ thực hiện rút tiền về ví điện tử sau đó chuyển về tài khoản của mình để chiếm đoạt. Trường hợp ví điện tử chưa liên kết tài khoản ngân hàng, đối tượng sẽ thao tác liên kết tài khoản ngân hàng của nạn nhân với ví điện tử rồi thực hiện hành vi chiếm đoạt tài sản.

13.2. Các đối tượng mời chào vay vốn với nhiều ưu đãi như: Hỗ trợ cho vay ngay cả trường hợp đang có nợ xấu, thủ tục đơn giản không cần nhiều giấy tờ, giải ngân chỉ trong 01 giờ, hạn mức cho vay lớn, lãi suất thấp… để thu hút khách hàng. Sau đó, yêu cầu khách hàng cài đặt ứng dụng cho vay online để đăng ký hồ sơ khoản vay và gửi thông báo phê duyệt khoản vay (sử dụng con dấu giả của các ngân hàng). Tuy nhiên, sau khi khách hàng đăng ký khoản vay, các đối tượng này sẽ thông báo lỗi giải ngân và yêu cầu nộp tiền để xử lý khoản vay. Hoặc các đối tượng lừa đảo sẽ yêu cầu khách hàng chuyển trước một khoản tiền để nộp phí hồ sơ hoặc bảo hiểm của khoản vay. Nhưng sau khi đã đóng tiền thì khách hàng không nhận được giải ngân khoản vay còn các đối tượng lừa đảo sẽ chiếm đoạt số tiền này và chặn mọi liên lạc.

13.3. Các đối tượng lừa đảo lấy thông tin của khách hàng sau đó liên hệ để giới thiệu về những app vay tiền khác với nhiều lời mời hấp dẫn: Được miễn lãi suất trong lần đầu vay; vay tiền không cần chứng minh thu nhập, không cần thế chấp...Tuy nhiên, sau khi giải ngân, khách hàng sẽ không nhận được toàn bộ số tiền vay mà chỉ nhận được một phần hoặc không nhận được đồng nào. Khi khách hàng đã không thể chi trả thì chúng sẽ gửi link tải app khác để tiếp tục vay tiền trả nợ. Cứ thế, khách hàng vướng vào vòng luẩn quẩn và ôm một khoản nợ lớn hơn ban đầu rất nhiều...

14. Mạo danh các trang mạng xã hội của thương hiệu, nhãn hàng, cửa hàng nhắn tin hoặc đăng tin tổ chức minigame dễ chơi dễ trúng thưởng hoặc tặng quà tri ân kỷ niệm ngày thành lập,… yêu cầu gửi tiền phí tham gia, vận chuyển, làm hồ sơ. Sau đó chặn liên lạc để chiếm đoạt tài sản.

15. Lừa đảo mua online "trả tiền trước qua Western Union"

Đối tượng sử dụng là đóng giả là người nước ngoài hoặc người Việt Nam tại nước ngoài mua hàng online với số lượng hàng hóa lớn, giá trị tài sản cao từ những người kinh doanh trong nước; đồng thời gợi ý chuyển tiền trả trước cho người bán hàng online thông qua dịch vụ chuyển tiền quốc tế Western Union. Để

tạo dựng niềm tin, các đối tượng sẽ giả lập một hóa đơn, chứng từ tiếp nhận tiền của dịch vụ chuyển tiền quốc tế Western Union; chụp ảnh hóa đơn, chứng từ này rồi gửi tin nhắn hình ảnh cho nạn nhân, khiến nạn nhân tưởng rằng phía bên mua hàng đã thực hiện lệnh chuyển tiền. Thông qua điện thoại di động hoặc các nền tảng mạng xã hội như Zalo, Facebook, các đối tượng sẽ gửi một tin nhắn đường link giả mạo website của dịch vụ chuyển tiền quốc tế Western Union; dẫn dắt các nạn nhân tiến hành các bước đăng nhập vào đường link này để rút số tiền mà các nạn nhân tin rằng các đối tượng đã trả để thanh toán mua hàng. Khi các nạn nhân nhấp vào đường link trong tin nhắn, họ sẽ được chuyển đến một trang web giả mạo có hiển thị giống như website chính thức của Western Union. Các nạn nhân sẽ phải khai báo các thông tin như tên, tuổi, địa chỉ, mã số thẻ ngân hàng... trên website giả mạo để làm thủ tục rút tiền. Sau khi có được thông tin tài khoản, các đối tượng lừa đảo sẽ thực hiện giao dịch chuyển tiền từ tài khoản của nạn nhân vào tài khoản của mình. Để lấy mã OTP chuyển tiền, chúng sẽ giả mạo tin nhắn của Western Union với nội dung: "Quý khách đang thực hiện giao dịch nạp tiền điện tử trên hệ thống iBanking với số tiền nhận là xxx triệu đồng. Mã OTP sẽ được xác nhận để hoàn tất giao dịch". Đồng thời, trên trang web giả mạo cũng hiện lên dòng chữ "Thủ tục nhận tiền: Quý khách vui lòng xác thực mã OTP cá nhân để nhận tiền". Cùng lúc đó, do các đối tượng đang thực hiện thao tác rút tiền trong tài khoản của nạn nhân nên các ngân hàng trong nước sẽ gửi mã OTP vào điện thoại của nạn nhân. Khi nạn nhân điền mã OTP này để hoàn tất thủ tục nhận tiền trên website giả mạo, đối tượng sử dụng mã OTP để chuyển toàn bộ tiền trong tài khoản nạn nhân sang tài khoản đã chuẩn bị trước để chiếm đoạt.

16. Lừa đảo cho số đánh lô, đề

Các đối tượng đăng bài quảng cáo trên mạng xã hội hoặc chủ động liên hệ với nạn nhân, giới thiệu mình là nhân viên của công ty xổ số hoặc có người nhà làm trong công ty xổ số, có thể biết trước được kết quả xổ số. Để tạo lòng tin cho nạn nhân, các đối tượng còn làm giả con dấu của những công ty xổ số kiến thiết và chữ ký của lãnh đạo công ty, bảng số lô đề được đóng dấu mật, dấu cam kết từ nhà quay thưởng để gửi cho nạn nhân hoặc đưa lên mạng xã hội. Với cam kết " trúng 100 % ", các đối tượng mời chào nạn nhân mua số, chuyển tiền qua tài khoản ngân hàng hoặc gửi thẻ điện thoại để có số đề, nếu không trúng sẽ hoàn tiền. Khi nhận được tiền do người mua số chuyển, các đối tượng chặn liên lạc để chiếm đoạt tiền.

17. Kêu gọi quyên góp tiền, hiện vật ủng hộ từ thiện

Thông qua các trang mạng xã hội, chủ yếu là Facebook, các đối tượng kêu gọi quyên góp, ủng hộ tiền để làm tự thiện, ủng hộ các gia đình, cá nhân có hoàn cảnh khó khăn. Từ đó lợi dụng chiếm đoạt tiền của các nhà hảo tâm.

18. Gửi mã QR giả kèm tin nhắn kết bạn zalo hoặc nhờ bình chọn cuộc thi,… Khi nạn nhân quét mã bằng Zalo đồng nghĩa với việc đăng nhập vào Zalo của mình trên máy tính của đối tượng, từ đó các đối tượng ăn cắp thông tin cá nhân hoặc nhắn tin vay mượn tiền người quen, bạn bè của nạn nhân.

19. Giả danh tập đoàn, công ty lớn huy động vốn đầu tư với cam kết lợi nhuận "khủng" để kêu gọi người dân góp vốn, thời gian đầu, các đối tượng trả tiền lãi đúng hẹn để nạn nhân tin tưởng và tiếp tục đầu tư nhiều tiền hơn. Khi nạn nhân đã đầu tư số tiền đủ lớn, các đối tượng báo làm ăn thua lỗ hoặc phá sản, sau đó chặn liên lạc để chiếm đoạt tài sản.

20. Lừa đảo "cộng tác viên online", hứa hẹn: kiếm tiền đơn giản, làm việc tại nhà, không cần ôm hàng…" với yêu cầu tuyển dụng: Có điện thoại/máy tính và tài khoản ngân hàng. Mua hàng online nhưng không nhận hàng (các đối tượng gọi là làm tăng tỷ lệ tương tác mua hàng đối với sản phẩm), việc mua hàng sẽ được thực hiện chuyển khoản qua tài khoản ngân hàng do các đối tượng cung cấp. Mỗi lượt mua hàng thành công sẽ được hưởng hoa hồng từ 10 - 20% số tiền gốc của mỗi đơn hàng, tiền sẽ được chuyển khoản ngược về sau 5 – 10 phút khi đặt hàng thành công (bao gồm cả tiền gốc và hoa hồng). Ban đầu, để tạo lòng tin và kích thích lòng tham của nạn nhân, các đối tượng sẽ cung cấp đường link trên hệ thống Shopee, Lazada, Tiki … của một sản phẩm giá trị không cao (thường khoảng vài trăm nghìn đồng) và tài khoản Ngân hàng cá nhân do đối tượng cung cấp để nạn nhân chuyển khoản với số tiền tương ứng với giá trị trên hệ thống; ngay sau đó các đối tượng sẽ chuyển khoản ngược lại cho nạn nhân như đã thỏa thuận. Khi nạn nhân chuyển số tiền đến vài triệu, vài chục triệu thì các đối tượng không chuyển khoản ngược lại nữa và đưa ra nhiều lý do khác nhau để nạn nhân tiếp tục "say mồi" như: Nhiệm vụ hoàn thành được 95/100 điểm tín nhiệm, cần tiếp tục chuyển tiền để hoàn thành 100 điểm… và nhiều người tiếp tục chuyển tiền và bị lừa số tiền đến vài trăm triệu đồng.

21. Lừa đảo giả mạo SMS brandname của Ngân hàng: Đối tượng sử dụng các thiết bị chuyên dụng, giả trạm phát sóng BTS, đem đến khu vực đông người để phát đi số lượng tin nhắn lớn tới các thuê bao lọt vào vùng phủ sóng của thiết bị. Do tin nhắn giả mạo sử dụng brandname giống với ngân hàng, các thiết bị smartphone sẽ xếp chung luồng với các tin nhắn thật đến từ ngân hàng nên rất khó để phân biệt và dễ bị mắc lừa. Nội dung tin nhắn lừa đảo ví dụ: "Ứng dụng VCB Digibank của bạn được phát hiện kích hoạt trên thiết bị lạ. Nếu không phải bạn kích hoạt vui lòng bấm vào http://vietcombank.vn-vm.top để đổi thiết bị hoặc hủy để tránh mất tài sản" hoặc "Tài khoản của bạn đã đăng ký chương trình quảng cáo trên TikTok, mỗi tháng thu phí 2.250.000 VND. Vui lòng vào https://msb.vn-cvs.top để kiểm tra hoặc hủy". Tin nhắn giả mạo thường chứa các đường link bất

thường như: vietcombank.vn-cbs.xyz; vietcombank.vn-cbs.pop; vietcombank.vn-ms.top…

II. CÁC BIỆN PHÁP PHÒNG NGỪA TỘI PHẠM SỬ DỤNG CÔNG NGHỆ CAO LỪA ĐẢO, CHIẾM ĐOẠT TÀI SẢN

1. Giữ bí mật, không cung cấp thông tin cá nhân, thông tin về tài khoản ngân hàng,… cho bất kỳ người lạ nào gọi đến. Tuyệt đối không cung cấp mã OTP cho người khác.

2. Cảnh giác với những cuộc điện thoại từ số máy lạ. Khi có số điện thoại lạ liên lạc, thông báo có liên quan đến tội phạm, vi phạm giao thông, bưu phẩm gửi bị lỗi và yêu cầu cung cấp thông tin cá nhân hoặc chuyển tiền, thì tuyệt đối không chuyển tiền, thông báo cho người thân trong gia đình và nhanh chóng trình báo với Cơ quan Công an gần nhất để kịp thời phối hợp xử lý. Với những cuộc gọi từ người lạ báo người nhà phải vào viện cấp cứu, hối thúc chuyển tiền để nộp viện phí thì không chuyển tiền theo yêu cầu của đối tượng mà cần tỉnh táo, xác nhận lại thông tin có chính xác hay không.

3. Không truy cập các đường link gắn kèm trong nội dung tin nhắn lạ; không thực hiện thao tác theo các cú pháp được hướng dẫn bởi người lạ.

4. Không thực hiện các yêu cầu chuyển tiền thông qua tin nhắn của các trang mạng xã hội, kể cả người thân, bạn bè. Cần xác nhận qua nhiều kênh khác nhau, không tin tuyệt đối vào cuộc gọi video để xác nhận người thân, bạn bè (Do đối tượng có thể sử dụng công nghệ "Deepfake" - công nghệ ứng dụng trí tuệ nhân tạo (AI) tạo ra các sản phẩm công nghệ âm thanh, hình ảnh và video làm giả đối tượng ngoài đời thực với độ chính xác rất cao. Dựa trên tệp tin hình ảnh khuôn mặt, giọng nói của một người ngoài đời thực, Deepfake sẽ sử dụng thuật toán để tái tạo lại khuôn mặt và giọng nói phù hợp với nét mặt, biểu cảm của một người khác; sau đó tại ra video giả mạo hoàn toàn người đó ngoài đời thực). Nếu chưa xác nhận chắc chắn, tuyệt đối không chuyển tiền.

5. Không mua, bán, cho mượn Giấy chứng minh nhân dân/Căn cước công dân, tài khoản cá nhân, tài khoản ngân hàng, các loại thẻ ngân hàng,…

6. Không tin vào những chiêu trò nhận quà từ nước ngoài chuyển về hoặc nhận thưởng qua mạng với yêu cầu nạp tiền qua thẻ điện thoại hoặc chuyển tiền qua tài khoản ngân hàng để làm thủ tục nhận thưởng.

7. Nếu tài khoản bỗng dưng nhận được một khoản tiền "chuyển nhầm" thì không được sử dụng số tiền ấy vào việc chi tiêu cá nhân. Đồng thời, chỉ làm việc và liên lạc với ngân hàng để giải quyết đối với số tiền chuyển nhầm đó.

8. Khi trao đổi, mua bán trực tuyến, qua mạng xã hội Zalo, Facebook phải tìm hiểu rõ nguồn gốc, hạn chế mua các đồ vật có giá trị lớn qua mạng xã hội hoặc các trang web bán hàng online.

9. Khi quen biết, kết bạn với người nước ngoài qua mạng xã hội Facebook không nên gửi, chuyển tiền để đóng các khoản phí vào tài khoản ngân hàng do đối tượng cung cấp với bất kỳ lý do gì, vì đây có khả năng cao là hành vi lừa đảo chiếm đoạt tài sản.

10. Không vay tiền online từ các ứng dụng không rõ nguồn gốc, đây là hình thức lừa đảo hoặc cho vay lãi nặng qua Internet và các ứng dụng trên điện thoại di động. Nếu các cá nhân có nhu cầu vay tiền thì liên hệ và đến trực tiếp ngân hàng, các tổ chức tín dụng gần nhất để được hỗ trợ. Khi thực hiện các giao dịch qua mạng hoặc qua các ứng dụng di động của các ngân hàng, tuyệt đối không được cung cấp mã xác thực OTP nhận được cho bất kỳ ai.

11. Tuyệt đối không tham gia đầu tư vào các sàn đầu tư tài chính, tiền ảo trái phép hoặc làm công tác viên cho các sàn thương mại điện tử theo quảng cáo "việc nhẹ lương cao" để tránh bị lừa đảo, chiếm đoạt tài sản.

12. Tuyệt đối không tham gia chơi "lô, đề".

13. Không quyên góp, ủng hộ tiền từ thiện khi chưa biết rõ người kêu gọi là ai và mục đích là gì, có phải để làm từ thiện thật hay không.

14. Nếu phát hiện, nghi ngờ có hành vi lừa đảo, chiếm đoạt tài sản, kịp thời thông báo cho Cơ quan công an gần để được tiếp nhận, giải quyết./.