

NGÂN HÀNG NHÀ NƯỚC
VIỆT NAM
CHI NHÁNH THÀNH PHỐ ĐÀ NẴNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc Lập - Tự Do - Hạnh Phúc

Số: 591 / ĐAN-KTTT

Đà Nẵng, ngày 16 tháng 05 năm 2024

V/v báo cáo tình hình an toàn bảo mật
trong hoạt động thanh toán không dùng
tiền mặt

VĂN PHÒNG UBND TP. ĐÀ NẴNG

gửi:

Số: 2.2988
ĐẾN Ngày: 17-05-2024
Chuyển: a. Lâm
Lưu hồ sơ số:

- Thành ủy Đà Nẵng;
- Hội đồng Nhân dân thành phố Đà Nẵng;
- Ủy ban Nhân dân thành phố Đà Nẵng.

Nhằm tăng cường công tác thông tin tuyên truyền về an toàn bảo mật trong hoạt động thanh toán, Ngân hàng Nhà nước Việt Nam Chi nhánh thành phố Đà Nẵng (NHNN) đã có văn bản số 718/ĐAN-KTTT ngày 01 tháng 06 năm 2023 báo cáo tình hình an toàn bảo mật trong hoạt động TTKDTM gửi Thành ủy, Hội đồng Nhân dân thành phố Đà Nẵng, Ủy ban Nhân dân thành phố Đà Nẵng. Hiện nay, một số đối tượng xấu vẫn tiếp tục lợi dụng kẽ hở của công nghệ thanh toán, công nghệ mạng và sự thiếu cảnh giác của người dân để lừa đảo, chiếm đoạt tiền trong tài khoản bằng nhiều thủ đoạn mới, biến hóa tinh vi. Để ngăn chặn và phòng ngừa các rủi ro có thể xảy ra đối với người dân, NHNN tổng hợp và bổ sung thêm một số trường hợp lừa đảo trong TTKDTM thời gian gần đây và báo cáo Thành ủy, Hội đồng Nhân dân, Ủy ban Nhân dân thành phố Đà Nẵng cụ thể như sau:

1. Lừa khách hàng tự chuyển tiền, chuyển tiền nhầm

- Giả mạo cơ quan điều tra thông báo liên quan đến một vụ án bất kỳ và yêu cầu khách hàng chuyển tiền để phục vụ điều tra;
- Giả mạo thông báo trúng thưởng từ ngân hàng hoặc các công ty lớn và yêu cầu cung cấp mã OTP của khách hàng;
- Giả mạo người thân, bạn bè nhờ chuyển tiền hộ, mua giúp thẻ điện thoại;
- Giả mạo thầy cô giáo của con điện thoại thông báo con bị tai nạn cần tiền để phẫu thuật gấp;
- Lập trang web "Trại hè kỹ năng", "Trại hè học kỳ quân đội" với giao diện, địa chỉ, số điện thoại giống với thông tin của các cơ quan Công an, quân đội để lừa đảo phụ huynh có nhu cầu đăng ký cho con tham gia các khóa học
- Giả mạo biên lai chuyển tiền thành công: Thủ đoạn của các đối tượng lừa đảo là mua hàng số lượng lớn, sau đó vay thêm tiền mặt của nạn nhân rồi chuyển khoản trả. Các đối tượng đề nghị chuyển khoản theo hình thức Internet

Banking cho người bán hàng. Nhưng thực chất là không có việc chuyển tiền thật, mà các đối tượng đã dùng một số phần mềm tạo dựng bill thanh toán giả rồi đưa cho người bán hàng xem nhằm chứng minh là đã thực hiện việc chuyển khoản. Cho đến khi các nạn nhân không thấy tài khoản báo có tiền và nhận ra mình đã bị lừa, thì các đối tượng đã “cao chạy xa bay”.

- Cố ý chuyển nhầm tiền vào tài khoản của khách hàng, sau đó đối tượng chủ động điện thoại xin trả lại số tiền chuyển nhầm và cung cấp tài khoản nhận lại khác với tài khoản người chuyển tiền ban đầu. Sau khi khách hàng chuyển tiền trả lại theo tài khoản được cung cấp, một đối tượng khác tự xưng là chủ tài khoản chuyển tiền nhằm gọi điện đến đòi lại tiền, nếu khách hàng không chuyển trả, chúng đe dọa gửi đơn kiện đến công an, cơ quan làm việc, bêu xấu trên mạng xã hội...

2. Đánh cắp thông tin bảo mật từ khách hàng rồi chiếm đoạt tiền từ tài khoản

Đây là hành vi của cá nhân, tổ chức thu thập các thông tin cá nhân của khách hàng để lừa đảo, chiếm đoạt tiền từ tài khoản ngân hàng hoặc sử dụng thông tin của khách hàng để mở tài khoản mang tên khách hàng và sử dụng tài khoản đó để thực hiện các hành vi vi phạm pháp luật thông qua các phương thức:

- Giả mạo cán bộ ngân hàng, yêu cầu cung cấp mật khẩu, mã PIN, thông tin thẻ hoặc truy cập vào đường dẫn để xử lý sự cố liên quan đến các dịch vụ ngân hàng điện tử hoặc thẻ;

- Gửi email, tin nhắn có chứa đường dẫn truy cập vào website của dịch vụ chuyển tiền, nhận tiền từ nước ngoài, nhập thông tin đăng nhập tài khoản ngân hàng trực tuyến (Internet Banking), hoặc thông tin thẻ để nhận tiền. Thực chất đây là các website giả mạo;

- Lừa khách hàng cài đặt các phần mềm ứng dụng gián điệp: Đối tượng giả danh điều tra viên, cán bộ cơ quan công an, viện kiểm sát, tòa án... gọi điện thông báo khách hàng có liên quan đến vụ án hình sự đang bị điều tra. Sau đó yêu cầu khách hàng cung cấp thông tin tài khoản ngân hàng hoặc tải ứng dụng có biểu tượng của ngành công an về điện thoại và nhập thông tin tài khoản ngân hàng vào ứng dụng. Thực chất ứng dụng mà khách hàng cài đặt là phần mềm gián điệp, khi khách hàng cài đặt những phần mềm này, mọi tin nhắn, cuộc gọi đến máy điện thoại của nạn nhân đều được phần mềm gián điệp kiểm soát, ngầm chuyển về máy chủ do đối tượng phạm tội quản lý. Nguy hiểm hơn, các đối tượng này còn có thể điều khiển smartphone của người dùng từ xa như gửi tin nhắn, thực hiện cuộc gọi, mở, khóa thiết bị di động, truy cập vào các ứng dụng ngân hàng cài đặt trên điện thoại và chiếm đoạt tiền của khách hàng;

- Lưu trữ trái phép các thông tin thẻ và dịch vụ ngân hàng đã nhập của khách hàng trên website có rủi ro cao;
- Giả mạo là người cho vay trực tuyến để lừa khách hàng có nhu cầu vay vốn và yêu cầu cung cấp thông tin về thẻ hoặc tài khoản ngân hàng điện tử;
- Lừa đảo khoá sim: Các đối tượng mạo danh là cán bộ, nhân viên của cơ quan quản lý Nhà nước hoặc nhà mạng gọi điện và thông báo số điện thoại của người sử dụng sẽ bị khóa 2 chiều trong 2 tiếng với các lý do như “chưa nộp phạt”, “thuê bao sai thông tin”. Sau khi yêu cầu cung cấp thông tin, chúng sẽ tiếp tục hướng dẫn người dùng thực hiện một số bước tiếp theo như: thực hiện các cú pháp sang tên đổi chủ thông tin số điện thoại, cú pháp chuyển hướng cuộc gọi... Khi đã chiếm được quyền nhận cuộc gọi, các đối tượng sẽ đăng nhập ứng dụng, tài khoản mạng xã hội... của nạn nhân và khai báo quên mật khẩu đăng nhập, chọn tính năng nhận cuộc gọi thông báo mã OTP. Từ đó, chúng dễ dàng kiểm soát, chiếm đoạt tiền trong ví, tài khoản ngân hàng liên kết với ví điện tử.
- Lừa đảo lập website giả mạo các tổ chức, doanh nghiệp, nhà cung cấp, dịch vụ lớn như các mạng xã hội, ngân hàng, thư điện tử, dịch vụ công,... Khi truy cập vào trang web giả mạo này, người dùng bị dụ cài ứng dụng có chứa mã độc. Ứng dụng này cho phép đối tượng lừa đảo chiếm quyền điều khiển điện thoại và đánh cắp thông tin, tài sản. Một số trang web như “vietgcv[.]cc” giả mạo cổng thông tin Bộ Thông tin truyền thông, “dichvucong[.]dancuso[.]com”; “dichvucong[.]jhhlp[.]com” giả mạo cổng dịch vụ công quốc gia, “vdbank[.]com[.]vn” giả mạo ngân hàng phát triển Việt Nam,...
- Giả mạo cán bộ cơ quan chức năng, người thân quen của nạn nhân (đối tượng sử dụng công nghệ Deepfake để giả dạng hình ảnh và giọng nói) thực hiện cuộc gọi “video call” với nạn nhân nhằm tạo sự tin tưởng, yêu cầu nạn nhân nhìn thẳng, nghiêng trái, nghiêng phải để ghi hình, rồi sử dụng hình ảnh đó để mở tài khoản ngân hàng, ví điện tử mang tên người bị hại và sử dụng cho mục đích lừa đảo hoặc các hành vi vi phạm pháp luật. Điều đáng lưu ý là các cuộc gọi “video call” đều có âm thanh, hình ảnh không rõ nét, tín hiệu chập chờn khiến người bị hại khó nhận biết thật giả;
- Giả mạo công an gọi điện yêu cầu ra công an xã, huyện, tỉnh để khắc phục đồng bộ VneID mức 2 (báo là bị lỗi). Nếu ra theo địa chỉ và yêu cầu của đối tượng thì chúng sẽ trì hoãn và báo bận, sau đó sẽ hướng dẫn người dân cài đặt và đồng bộ online. Khi trả lời là bận không ra được ngay thì đối tượng sẽ hướng dẫn đồng bộ online theo hướng cài đặt phần mềm có logo VneID có yêu cầu khuôn mặt, vân tay và số điện thoại. Sau đó chiếm quyền kiểm soát điện thoại và

thực hiện chuyển hết số tiền từ tài khoản đi (mặc dù không yêu cầu số tài khoản hay mã OTP);

- Lừa đảo chiếm quyền điều khiển thiết bị di động hoặc cài đặt các phần mềm nghe lén lên thiết bị di động: Các đối tượng sẽ gửi email, tin nhắn có mã độc đến người dùng hoặc lừa người dùng cài đặt các app mà chúng tạo ra. Khi người dùng bấm vào link, file, hoặc cài đặt app sẽ bị chiếm đoạt quyền điều khiển thiết bị hoặc bị cài phần mềm nghe lén lên thiết bị. Từ đó đối tượng sẽ truy cập được tài khoản ngân hàng trên thiết bị và chuyển tiền vào tài khoản của chúng

- Bỏ các phiếu cào trúng thưởng trên các bưu phẩm nhận từ shipper. Trên phiếu cào, khi cào ra có giải thưởng, để được nhận thưởng phải truy cập đường link trên mã QR và cung cấp thông tin cá nhân để làm thủ tục nhận thưởng. Khi truy cập link trên mã QR người dân sẽ bị lấy cắp thông tin và nguy cơ bị lừa đảo chiếm đoạt tài sản.

3. Mua, bán, thuê, cho thuê tài khoản ngân hàng

Lợi dụng tình hình kinh tế khó khăn và sự thiếu nắm bắt thông tin pháp luật của nhiều người, các đối tượng thuyết phục, lôi kéo người dân, đặc biệt là các em học sinh, sinh viên, người lớn tuổi mở tài khoản sau đó bán hoặc cho thuê mỗi tài khoản nhận được từ 100.000 đến 700.000 đồng. Các đối tượng sau khi mua, thuê tài khoản, sử dụng những tài khoản đó để thực hiện hành vi phạm tội hoặc tiếp tục bán lại hoặc cho thuê lại để kiếm tiền. Hành vi bán, cho thuê, cho mượn tài khoản thanh toán là hành vi vi phạm pháp luật và bị xử lý vi phạm theo quy định tại Khoản 5, 6, 7 Điều 26, Mục 8, Chương 2 Nghị định số 88/2019/NĐ-CP ngày 14 tháng 11 năm 2019 của Chính phủ quy định về xử phạt vi phạm hành chính trong lĩnh vực tiền tệ và ngân hàng.

4. Một số biện pháp phòng ngừa, đảm bảo an toàn trong TTKDTM

Nhìn chung, những vụ lừa đảo gần đây chủ yếu phát sinh từ sự cả tin, mất cảnh giác của người dân. Vì vậy, khách hàng khi sử dụng dịch vụ TTKDTM, cần lưu ý các nội dung sau để phòng tránh rủi ro mất tiền từ tài khoản:

4.1. Thực hiện đúng các quy định về an toàn bảo mật và quy trình thanh toán của ngân hàng, không dùng máy tính và mạng internet công cộng để truy cập, thực hiện giao dịch Internet Banking, không lưu lại tên đăng nhập và mã khóa bí mật trên các trình duyệt web, thoát khỏi ứng dụng Internet Banking khi không sử dụng và cài đặt, sử dụng phần mềm diệt vi rút trên thiết bị cá nhân sử dụng để giao dịch Internet Banking;

4.2. Đăng ký nhận thông báo biến động số dư tài khoản qua tin nhắn di động hoặc tin nhắn qua ứng dụng trên di động do ngân hàng cung cấp để kịp

thời cập nhật các thông tin giao dịch, biến động số dư khi sử dụng các dịch vụ tài khoản, thanh toán thẻ ngân hàng;

4.3. Tuyệt đối không cung cấp tên đăng nhập, mật khẩu đăng nhập, mã xác thực OTP của dịch vụ ngân hàng điện tử, ngân hàng số cho bất kỳ ai, kể cả nhân viên ngân hàng. Các ngân hàng không bao giờ yêu cầu khách hàng cung cấp thông tin bảo mật của khách hàng dưới bất kỳ hình thức nào;

4.4. Thiết lập mã khóa bí mật ứng dụng thanh toán điện tử, thanh toán số khó đoán có tính bảo mật cao (tránh đặt ngày sinh, tên người thân, số điện thoại...) và thay đổi mã khóa bí mật tài khoản truy cập theo định kỳ tối thiểu một năm một lần hoặc khi bị lộ, nghi bị lộ. Không sử dụng các phần mềm lưu trữ mật khẩu, không dùng chung một mật khẩu để đăng nhập vào ứng dụng ngân hàng điện tử và đăng nhập vào các mạng xã hội;

4.5. Lưu lại thông tin về đầu mối tiếp nhận thông tin, số điện thoại đường dây nóng của ngân hàng và thông báo ngay cho ngân hàng các trường hợp: mất, thất lạc số điện thoại đăng ký nhận tin nhắn SMS, thiết bị lưu trữ khóa bảo mật tạo chữ ký số; bị lừa đảo hoặc nghi ngờ bị lừa đảo; bị tin tặc hoặc nghi ngờ bị tin tặc tấn công để được hướng dẫn xử lý kịp thời;

4.6. Đăng ký sử dụng phương thức xác thực bảo mật được tích hợp trên ứng dụng di động (Soft OTP) khi thực hiện các giao dịch trực tuyến. Không sử dụng các thiết bị di động đã bị phá khóa để tải và sử dụng phần mềm ứng dụng Internet Banking, phần mềm tạo OTP;

4.7. Chỉ nhận thông tin qua các kênh thông tin chính thức, đáng tin cậy của hệ thống ngân hàng (thông tin tại quầy giao dịch, trang web ngân hàng, ứng dụng internet banking của ngân hàng...). Trường hợp nhận được thông tin qua tin nhắn, email, mạng xã hội của người tự nhận là nhân viên ngân hàng hướng dẫn thực hiện thủ tục cho vay, mở tài khoản, gửi tiết kiệm trực tuyến,... hãy liên hệ trực tiếp với ngân hàng đó để xác minh thông tin trước khi thực hiện theo hướng dẫn. Tuyệt đối không truy cập vào các đường dẫn tới trang thông tin, ứng dụng giả mạo ngân hàng, các cơ quan nhà nước, các doanh nghiệp, tổ chức được gửi qua tin nhắn, email, mạng xã hội.

4.8. Không thực hiện các thao tác làm theo hướng dẫn từ các số điện thoại lạ gọi đến, kể cả đối tượng tự xưng là cán bộ ngân hàng và các cơ quan khác khi chưa xác minh được thông tin chính xác. Lực lượng công an và cơ quan chức năng Nhà nước trong quá trình điều tra, giải quyết vụ việc không làm việc với công dân qua điện thoại, tuyệt đối không có lời lẽ đe dọa hoặc gửi những tài liệu khởi tố, khởi kiện qua điện thoại. Nếu cơ quan chức năng mời làm việc sẽ gửi giấy mời thông qua chính quyền, đoàn thể địa phương nơi công dân cư trú để làm việc đúng theo quy định của pháp luật;

4.9. Không truy cập vào website, đường dẫn lạ (đường link,...) trên mã QR khi nhận được các bưu phẩm có phiếu cào trúng thưởng, không nhận các bưu phẩm lạ không do mình đặt hàng, không nhận hộ bưu phẩm của người khác.

4.10. Không cho thuê, cho mượn hoặc bán tài khoản ngân hàng của mình cho người khác. Đồng thời, khi phát hiện các hành vi mua, bán, thuê, cho thuê tài khoản ngân hàng hoặc các trường hợp nghi ngờ về hoạt động lừa đảo chiếm đoạt tài sản qua tài khoản ngân hàng, người dân cần kịp thời báo cho cơ quan công an nơi gần nhất để được xử lý.

4.11. Phụ huynh nên khuyến cáo con em không nên để các đối tượng lừa đảo lôi kéo mở tài khoản để phục vụ cho các hành vi vi phạm pháp luật.

Trên đây là báo cáo của Ngân hàng Nhà nước Việt Nam chi nhánh thành phố Đà Nẵng về một số trường hợp lừa đảo trong TTKDTM thời gian gần đây, kính báo cáo Thành ủy, Hội đồng Nhân dân, Ủy ban Nhân dân thành phố Đà Nẵng quan tâm chỉ đạo các Sở ban ngành, UBND các quận, huyện, xã phường phối hợp tuyên truyền những nội dung này để người dân trên địa bàn thành phố nắm bắt các phương thức, thủ đoạn cũng như cách thức phòng tránh các rủi ro trong hoạt động TTKDTM. /.

Nơi nhận:

- Như trên (để b/cáo);
- Ban Nội chính Thành ủy (để b/cáo);
- Ban Dân vận Thành ủy (để b/cáo);
- Công an TP Đà Nẵng (để p/hợp);
- Các Sở, ngành thành phố (để p/hợp);
- Các Quận, Huyện trên địa bàn thành phố (để p/hợp);
- Các TCTD trên địa bàn (để p/biến đến khách hàng);
- Lưu: VT, KT-TT.

GIÁM ĐỐC



Võ Minh