

Cảnh giác bẫy lừa đảo từ dịch vụ rút tiền thẻ tín dụng

14:10 15/09/2026

Từ lời mời hỗ trợ rút tiền mặt từ thẻ tín dụng với tỷ lệ lên tới 75% hạn mức, không mất phí và được trả góp, một nhóm đối tượng đã lừa đảo hơn 200 nạn nhân, thực hiện hơn 7.000 giao dịch và chiếm đoạt 24 tỷ đồng của người bị hại chỉ trong 10 tháng hoạt động.

Đằng sau những lời mời tưởng như một dịch vụ tài chính thông thường là cả một kịch bản được dàn dựng nhằm chiếm đoạt tiền của khách hàng. Các đối tượng thành lập doanh nghiệp để tạo vỏ bọc hợp pháp, mua dữ liệu khách hàng, đồng thời thuê nhân viên giả danh ngân hàng gọi điện tư vấn, từ đó từng bước dẫn dụ người sử dụng thẻ tín dụng thực hiện giao dịch.

Vụ việc vừa được Tòa án Nhân dân TP HCM xét xử cũng cho thấy mức độ tinh vi của các chiêu thức lừa đảo nhắm vào người dùng dịch vụ ngân hàng. Đây là nội dung vừa được chương trình Cảnh giác 247 phát sóng ngày 12/9 phân tích, cảnh báo tới người dân. Chương trình do Đài Truyền hình Việt Nam (VTV) phối hợp với Ngân hàng Thương mại TNHH MTV Kỹ Nguyên Thịnh Vượng (GPBank) và Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (A05 - Bộ Công an) thực hiện.

Theo cơ quan cảnh sát điều tra, các đối tượng này đã tiếp cận nạn nhân dưới danh nghĩa nhân viên ngân hàng để giới thiệu dịch vụ rút tiền mặt với hạn mức 75% thẻ tín dụng về tài khoản, cam kết không mất phí và được trả góp từ 6 - 12 tháng.

Khi người bị hại đồng ý, các đối tượng yêu cầu cung cấp số thẻ, ngày hết hạn, mã bảo mật CVV, mã OTP xác thực giao dịch và số tài khoản nhận tiền. Các thông tin được sử dụng để tạo giao dịch thanh toán khống tại gian hàng trực tuyến do chính nhóm lừa đảo này thiết lập. Không có hoạt động mua bán nào diễn ra, toàn bộ số tiền từ hạn mức thẻ tín dụng của nạn nhân được đưa vào hệ thống thanh toán dưới hình thức giao dịch mua hàng, nhưng thực chất đã chuyển về tài khoản do chúng kiểm soát.

Sau đó, các đối tượng này chuyển lại khoảng 75% số tiền cho nạn nhân và chiếm đoạt 25% còn lại. Trường hợp người bị hại thắc mắc về phần chênh lệch, chúng giải thích đây là khoản đối ứng trả góp và sẽ được hoàn lại sau khi tất toán.

Tuy nhiên trên thực tế, người bị hại vẫn phải trả toàn bộ 100% số tiền cho ngân hàng. Điểm đặc biệt trong thủ đoạn này là nạn nhân không lập tức nhận ra mình vừa bị lừa, ngược lại, họ tin rằng đang sử dụng một dịch vụ tài chính hợp pháp sau khi nhận lại số tiền từ kẻ lừa đảo. Rủi ro còn tăng cao khi các đối tượng có thể dùng thông tin thẻ và mã OTP để đăng ký mua sắm trực tuyến hoặc liên kết thẻ với ví điện tử.

Theo đại diện Ngân hàng Thương mại TNHH MTV Kỹ Nguyên Thịnh Vượng (GPBank), người dùng cần nắm vững quy tắc "3 không" nhằm bảo vệ thông tin và tài sản. "Thứ nhất là không cung cấp thông tin cá nhân, mật khẩu, mã OTP, mã PIN hoặc quét khuôn mặt qua bất kỳ ứng dụng nào từ cá nhân hay tổ chức bên thứ ba ngoài ngân hàng. Thứ hai là không bấm vào đường link hoặc tải ứng dụng lạ. Và thứ ba là không chuyển tiền trước đối với bất kỳ một yêu cầu phí đặt cọc, phí làm hồ sơ, phí kích hoạt hạn mức, phí nâng hạn mức thẻ", bà Hoàng Thị Thúy Hà, Giám đốc Khối Vận hành Ngân hàng GPBank, cho biết.



Bà Hoàng Thị Thúy Hà, Giám đốc Khối Vận hành Ngân hàng GPBank

Cũng theo chuyên gia từ GPBank, khi gặp những yêu cầu này, người dân hãy liên hệ với ngân hàng qua tổng đài chính thức, hoặc đến chi nhánh của ngân hàng để được xác minh.

Về bản chất, thẻ tín dụng là công cụ thanh toán dựa trên hạn mức tín dụng do ngân hàng cấp cho khách hàng. Chủ thẻ có thể sử dụng hạn mức này để thanh toán hàng hóa, dịch vụ hoặc thực hiện một số giao dịch khác theo quy định của ngân hàng, sau đó có nghĩa vụ hoàn trả số tiền đã sử dụng trong thời gian và theo các điều kiện đã thỏa thuận.

Thẻ tín dụng cũng có thể được sử dụng để rút tiền mặt tại ATM hoặc qua một số hình thức khác, tùy chính sách của từng ngân hàng và sản phẩm thẻ qua các thời kỳ. Tuy nhiên, giao dịch rút tiền mặt thường có hạn mức riêng và có thể phát sinh phí, lãi suất theo quy định.

Ngoài lời mời hỗ trợ rút tiền từ hạn mức, nhiều kịch bản khác cũng có thể khiến chủ thẻ tiết lộ thông tin bảo mật như giả danh nhân viên ngân hàng gọi điện thông báo thẻ sắp bị khóa, có giao dịch bất thường, được hoàn phí, đổi điểm thưởng hoặc hỗ trợ chuyển khoản chi tiêu sang trả góp. Cũng với những lý do này, các đối tượng lừa đảo còn có thể dẫn dắt nạn nhân đến website giả mạo ngân hàng để nhập thông tin thẻ, mã CVV, mã OTP và chiếm đoạt thông tin của người dùng.

Bên cạnh việc nhận diện các thủ đoạn lừa đảo, các chuyên gia khuyến nghị người dùng nên chủ động giảm thiểu rủi ro bằng cách tận dụng các công cụ kiểm soát do ngân hàng cung cấp, như thông báo biến động giao dịch, thiết lập hạn mức, bật hoặc tắt chức năng thanh toán trực tuyến và sử dụng các phương thức xác thực bổ sung.

Tuy nhiên, yếu tố quan trọng nhất vẫn là sự thận trọng của chính chủ thẻ. Người dùng không nên cung cấp thông tin bảo mật, truy cập đường link do người lạ gửi hoặc xác nhận bất kỳ giao dịch nào khi chưa hiểu rõ mình đang thực hiện giao dịch gì, với ai và với số tiền bao nhiêu. Trong mọi trường hợp, khi nhận được yêu cầu bất thường liên quan đến tài khoản, thẻ hoặc thông tin bảo mật, người dùng nên chủ động liên hệ ngân hàng qua các kênh chính thức để kiểm tra trước khi thực hiện.