

Công an TP.HCM cảnh báo tội phạm lừa đảo chiếm đoạt tài sản thông qua ngân hàng

10:30 23/12/2021

Công an TP.HCM cảnh báo tội phạm lừa đảo chiếm đoạt tài sản thông qua hệ thống ngân hàng bằng một số thủ đoạn và cách phòng ngừa để người dân cảnh giác.

Theo Công an TP.HCM, thời gian qua tội phạm lừa đảo chiếm đoạt tài sản thông qua hệ thống ngân hàng diễn ra khá phổ biến. Trong đó, nổi lên một số thủ đoạn như: “Giả mạo SMS Brandname”, “Chuyển tiền nhầm”, “Mạo danh ngân hàng cho vay”...

Với thủ đoạn “Giả mạo SMS Brandname”, các đối tượng đã sử dụng các thiết bị viễn thông công nghệ cao giả mạo tin nhắn SMS có tên thương hiệu các tổ chức ngân hàng, tài chính (Sacombank, ACB, BIDV, TPBank, Zalopay...) gửi đến các thuê bao di động được lưu trữ cùng thư mục với các tin nhắn thương hiệu thật của các ngân hàng trên điện thoại di động của người dùng với nội dung cảnh báo giả mạo để tạo tâm lý hoang mang lo sợ của người dân. Đồng thời, gây nhầm tưởng đây là thông báo chính thức từ ngân hàng.



Công an TP.HCM khuyến cáo người dân cảnh giác các thủ đoạn lừa đảo thông qua ngân hàng. (Ảnh: minh họa)

Tinh vi hơn, trong nội dung tin nhắn SMS giả mạo này có kèm đường link website có địa chỉ tên miền gần giống với tên ngân hàng để dẫn dụ nạn nhân nhập thông tin tài khoản ngân hàng trực tuyến (user và password đăng nhập), số điện thoại và mã OTP xác nhận tài khoản trên website giả mạo đó.

Những thông tin do nạn nhân cung cấp trên đường link đồng thời được truyền về cho đối tượng hacker. Người dùng lập tức bị mất quyền sử dụng tài khoản ngân hàng trực tuyến về tay hacker, đồng thời toàn bộ tiền trong tài khoản cũng bị chiếm đoạt tức thời.

Để đối phó với các thủ đoạn trên, ngành Công an khuyến cáo người dân nên nhớ các trang web của tổ chức tài chính, ngân hàng thường được đăng ký tên miền (.vn) hoặc (.com.vn); Các trang web đăng ký giống nhưng đuôi khác như (.vip), (.top), (.cc), (.com)... đều là giả mạo. Khi nhận tin nhắn được cho là từ phía ngân hàng mà có những dấu hiệu như thủ đoạn nói trên, người dân gọi tổng đài chính thức của ngân hàng kiểm tra lại thông tin mới nhận, phản ánh nội dung các tin nhắn vừa nhận được.

Đối với thủ đoạn “chuyển nhầm tiền”, khi nạn nhân bị lộ, lọt thông tin tài khoản ngân hàng (do nạn nhân, hoặc bị mua lại thông tin) thì tội phạm cố tình chuyển một khoản tiền vào tài khoản ngân hàng của nạn nhân. Sau đó, mạo danh ngân hàng gọi điện hoặc gửi tin nhắn thông báo giao dịch chuyển tiền bị treo hoặc có người chuyển nhầm và yêu cầu khách hàng truy cập đường link website mạo danh ngân hàng để tra soát giao dịch, xác nhận thông tin, mở khóa lệnh chuyển tiền. Từ đây khách hàng bị dẫn dụ lấy thông tin bảo mật (tên truy cập, mật khẩu, mã OTP), chiếm đoạt tiền trong tài khoản.

Đối tượng có thể gọi điện trực tiếp tự xưng là người chuyển nhầm tiền vào tài khoản nạn nhân. Để xin lại số tiền trên, chúng kết bạn Zalo, Facebook và gửi đường link mạo danh ngân hàng cho nạn nhân với lý do chuyển tiền nhanh. Sau đó dẫn dụ nạn nhân cung cấp thông tin bảo mật của dịch vụ ngân hàng điện tử và chiếm đoạt tài khoản ngân hàng trực tuyến cùng toàn bộ số tiền có trong tài khoản của nạn nhân.

Với thủ đoạn này, người dân lưu ý không sử dụng số tiền “chuyển nhầm” vào mục đích chi tiêu cá nhân mà gọi điện theo số hotline ngân hàng nơi mình mở tài khoản để trao đổi sự việc rồi yêu cầu nhân viên phong tỏa giao dịch với số tiền “chuyển nhầm” trên, hoặc có thể đến chi nhánh ngân hàng gần nhất trực tiếp yêu cầu phong tỏa giao dịch số tiền “chuyển nhầm”.

Tuyệt đối không hoàn chuyển tiền cho người lạ (tự xưng người chuyển nhầm tiền qua điện thoại) khi không có bên thứ 3 làm chứng (đại diện ngân hàng hoặc

cơ quan Công an). Đồng thời không tự ý hoàn chuyển vào tài khoản khác với tài khoản ngân hàng đã “chuyển nhầm” cho mình, phải chờ phía ngân hàng có phản hồi, giải quyết trước.

Khi nhận được điện thoại lạ tự xưng đại diện ngân hàng hay tổ chức liên quan thì lấy lý do để gọi lại sau và kiểm tra lại thông tin số điện thoại trên có đúng số điện thoại ngân hàng hay tổ chức có liên quan. Để chắc chắn hơn, người dân nên yêu cầu bên chuyển nhầm tiền cùng mình lên ngân hàng để giải quyết.

Đặc biệt, không bao giờ cung cấp thông tin tài khoản đăng nhập khi sử dụng dịch vụ Internet Banking, SmartBanking (tên truy cập, mật khẩu, mã OTP) cho người khác trong mọi trường hợp. Không truy cập vào các đường link giả mạo ngân hàng khi chưa kiểm chứng.

Với thủ đoạn “Mạo danh ngân hàng cho vay”, các đối tượng sẽ sử dụng Fanpage Facebook, website, Zalo có hình ảnh logo, hình ảnh phòng giao dịch, hội thảo tư vấn của các ngân hàng..., thậm chí hình ảnh của nhân viên ngân hàng để liên hệ với khách hàng, giới thiệu các gói vay hay tiền gửi hấp dẫn giải ngân nhanh với thủ tục đơn giản qua mạng. Sau đó, đối tượng yêu cầu khách hàng cần nộp một khoản phí chuyển Internet Banking vào tài khoản lừa đảo để được hưởng ưu đãi rồi chiếm đoạt tiền phí, sau đó chặn mọi liên lạc.

Cơ quan Công an khuyến cáo, mọi khoản vay người dân nên liên hệ chi nhánh ngân hàng gần nhất nơi mình cư trú để làm thủ tục vay. Người dân tuyệt đối không làm việc với người tự xưng là nhân viên ngân hàng thông qua Fanpage Facebook, website, Zalo.

Nguyễn Tùng - Hoàng Dương