TẠP CHÍ ĐIỆN TỬ
THƯƠNG HIỆU & CÔNG LUẬN

Các ngân hàng phát cảnh báo về thủ đoạn lừa đảo mới

16:08 24/05/2026

Các ngân hàng liên tiếp phát đi cảnh báo về làn sóng lừa đảo công nghệ cao với thủ đoạn ngày càng tinh vi, từ giả danh nhân viên ngân hàng, doanh nghiệp đến dựng kịch bản tuyển dụng xuất khẩu lao động hoặc giả mạo cuộc gọi bằng công nghệ AI.

Kienlongbank cho biết, thời gian gần đây, xuất hiện nhiều trường hợp đối tượng mạo danh nhân viên công ty, doanh nghiệp, trong đó có ngân hàng để liên hệ với khách hàng qua điện thoại, Facebook, Zalo hoặc các nền tảng mạng xã hội khác. Các đối tượng thường sử dụng tên gọi, hình ảnh, logo thương hiệu, thậm chí làm giả thẻ nhân viên hoặc giấy tờ liên quan nhằm tạo dựng lòng tin và đánh lừa khách hàng.

Sau khi tiếp cận, các đối tượng thường đưa ra nhiều lời mời hấp dẫn như hỗ trợ nhận ưu đãi, xác minh tài khoản, cập nhật thông tin, tham gia chương trình tri ân khách hàng hoặc xử lý các vấn đề liên quan đến tài chính, dịch vụ. Một số trường hợp còn tự nhận đây là “chương trình nội bộ”, “ưu đãi giới hạn” hoặc “hỗ trợ khẩn cấp” nhằm tạo cảm giác cấp bách, khiến khách hàng mất cảnh giác và làm theo hướng dẫn của đối tượng.

Khi khách hàng bắt đầu tin tưởng, các đối tượng sẽ yêu cầu cung cấp thông tin bảo mật như mã OTP, tên đăng nhập, mật khẩu, số thẻ, mã CVV/CVC... với nhiều lý do như “xác minh tài khoản”, “cập nhật thông tin”, “kích hoạt ưu đãi” hoặc “hỗ trợ xử lý sự cố”. Ngoài ra, các đối tượng còn gửi đường link giả mạo có giao diện tương tự website hoặc ứng dụng chính thức của doanh nghiệp, ngân hàng nhằm đánh cắp thông tin cá nhân và chiếm đoạt tài sản.

Các ngân hàng phát cảnh báo về thủ đoạn lừa đảo mới (Ảnh minh họa)

Ngay khi có được dữ liệu bảo mật, đặc biệt là mã OTP, các đối tượng sẽ nhanh chóng thực hiện giao dịch chuyển tiền và chiếm đoạt tài sản của khách hàng.

LPBank cũng vừa phát thông báo tới toàn bộ khách hàng liên quan tới thủ đoạn lừa đảo chiếm đoạt tài khoản ngân hàng bằng chiêu trò xuất khẩu lao động.

Theo LPBank, các đối tượng thường đăng tải thông tin tuyển dụng đi lao động tại Đức, Nhật Bản, Hàn Quốc, Đài Loan (Trung Quốc)… với mức lương hấp dẫn, điều kiện dễ dàng, thủ tục nhanh gọn để thu hút nạn nhân. Sau khi tạo được lòng tin, kẻ gian giả danh nhân viên công ty xuất khẩu lao động, chủ động liên hệ và hướng dẫn các bước làm hồ sơ.

Thủ đoạn phổ biến là yêu cầu người có nhu cầu cung cấp giấy tờ cá nhân như căn cước công dân, ảnh chân dung, thông tin tài khoản ngân hàng hoặc chuyển các khoản phí như tiền hồ sơ, đặt cọc, phí xử lý thủ tục. Đáng chú ý, nhiều trường hợp còn bị dụ cài đặt ứng dụng lạ hoặc truy cập đường link không rõ nguồn gốc với lý do “xác thực hồ sơ” hoặc “hoàn thiện thủ tục”. Đây là bước để đối tượng cài mã độc, chiếm quyền kiểm soát điện thoại và đánh cắp thông tin ngân hàng.

Không ít nạn nhân đã bị chiếm đoạt số tiền lên tới hàng trăm triệu đồng sau khi làm theo hướng dẫn của các đối tượng.

Không chỉ dừng ở chiêu trò xuất khẩu lao động, các ngân hàng cũng cảnh báo nhiều hình thức lừa đảo công nghệ cao khác đang gia tăng.

Theo VPBank, trên không gian mạng xuất hiện các ứng dụng có khả năng giả mạo số điện thoại và giọng nói (Voice Phishing), giúp kẻ gian tạo cuộc gọi giống hệt từ ngân hàng, cơ quan chức năng hoặc người thân để thao túng tâm lý nạn nhân.

Các cuộc gọi này thường đi kèm kịch bản khẩn cấp như thông báo tài khoản gặp sự cố, yêu cầu xác minh thông tin hoặc đề nghị chuyển tiền vào "tài khoản an toàn". Trong quá trình trao đổi, đối tượng sẽ tìm cách khai thác mã OTP, mật khẩu, thông tin sinh trắc học hoặc dẫn dụ người dùng cài ứng dụng chứa mã độc.

Trước tình trạng trên, các ngân hàng khuyến nghị người dân tuyệt đối không chuyển tiền hoặc cung cấp thông tin cá nhân cho người lạ qua mạng xã hội; không cài ứng dụng không rõ nguồn gốc; không chia sẻ mã OTP, mật khẩu hay thông tin đăng nhập trong bất kỳ tình huống nào. Khi có nhu cầu đi xuất khẩu lao động, người dân nên làm việc trực tiếp với doanh nghiệp được cấp phép, kiểm tra kỹ thông tin và chỉ giao dịch qua các kênh chính thức.

Nếu phát hiện dấu hiệu bất thường hoặc nghi ngờ bị lừa đảo, người dùng cần liên hệ ngay với ngân hàng để khóa tài khoản và trình báo cơ quan chức năng để được hỗ trợ kịp thời.

Thu Trang