

VIB cảnh báo: Nhiều kịch bản lừa đảo tinh vi đang nhắm vào khách hàng

13:40 25/01/2026

VIB khuyến nghị khách hàng đặc biệt thận trọng trước khi thực hiện các giao dịch tài chính.

Càng gần Tết Nguyên đán, nhu cầu giao dịch tài chính, mua sắm và thanh toán của người dân càng gia tăng. Lợi dụng tâm lý bận rộn, chủ quan và nhu cầu chi tiêu cao dịp cuối năm, các đối tượng lừa đảo trực tuyến liên tục tung ra nhiều chiêu thức mới với mức độ ngày càng tinh vi, gây thiệt hại đáng kể cho khách hàng.

Trước thực trạng này, Ngân hàng TMCP Quốc Tế Việt Nam (VIB) vừa phát đi cảnh báo về loạt kịch bản lừa đảo đang diễn biến phức tạp trong thời gian gần đây, khuyến nghị khách hàng đặc biệt thận trọng trước khi thực hiện các giao dịch tài chính.



Giả mạo nhân viên ngân hàng để chiếm quyền kiểm soát tài khoản

Theo VIB, một trong những thủ đoạn phổ biến nhất hiện nay là giả mạo nhân viên ngân hàng. Các đối tượng gọi điện, nhắn tin hoặc liên hệ qua mạng xã hội

với danh nghĩa hỗ trợ xác thực sinh trắc học, nâng cấp tài khoản hoặc xử lý sự cố. Sau đó, chúng dẫn dụ khách hàng kết bạn, thực hiện cuộc gọi video và yêu cầu cung cấp thông tin cá nhân, hình ảnh giấy tờ tùy thân, khuôn mặt hoặc giọng nói. Những dữ liệu này có thể bị lợi dụng để chiếm quyền sử dụng tài khoản thanh toán hoặc phục vụ các mục đích phi pháp.

Dụ khách hàng sập bẫy khuyến mại, hoàn tiền giả mạo

Ngoài ra, kẻ gian còn tung ra các chương trình ưu đãi hoàn toàn bịa đặt như miễn phí thường niên thẻ nhiều năm, hỗ trợ hủy hoặc khóa thẻ tạm thời để “tránh phát sinh phí”, thông báo thu phí duy trì thẻ kèm gợi ý hoàn tiền, hay hoàn tiền từ 10-15% khi mua sắm. Khi khách hàng tin tưởng, đối tượng yêu cầu cung cấp thông tin bảo mật thẻ như số thẻ, mã CVV, mã OTP để thực hiện các giao dịch trái phép và chiếm đoạt tiền.

Lừa đảo qua mạng xã hội, mã QR và đường link độc hại

Một thủ đoạn khác cũng đang gia tăng là tiếp cận khách hàng qua mạng xã hội, giả danh người quen nội bộ hoặc nhân viên hỗ trợ mở thẻ. Sau khi thẻ được phê duyệt, các đối tượng tiếp tục viện lý do cần xác thực hoặc kích hoạt hạn mức, rồi yêu cầu khách hàng quét mã QR hoặc thực hiện giao dịch theo hướng dẫn để chiếm đoạt tiền.

Bên cạnh đó, nhiều đối tượng chạy quảng cáo bán hàng với mức giá rẻ bất thường hoặc gửi email, tin nhắn thông báo gia hạn dịch vụ, đánh trúng tâm lý ham ưu đãi. Khi khách hàng nhấn vào đường link và nhập thông tin thẻ, dữ liệu bị thu thập và thẻ có thể bị liên kết trái phép vào các ví điện tử do kẻ gian kiểm soát.

Giả mạo cơ quan nhà nước, dịch vụ công và hỗ trợ Tết

VIB cũng cảnh báo tình trạng giả mạo website, ứng dụng của các cơ quan dịch vụ công như định danh điện tử, cơ quan thuế, bảo hiểm xã hội... Những nền tảng giả mạo này thường chứa mã độc, cho phép kẻ gian kiểm soát thiết bị, đánh cắp thông tin ngân hàng và thực hiện chuyển tiền trái phép.

Ngoài ra, các đối tượng còn giả danh cán bộ cơ quan nhà nước hoặc bảo hiểm xã hội, gọi điện thông báo khách hàng được nhận “tiền hỗ trợ Tết” hoặc “tiền hỗ trợ từ quỹ bảo hiểm thất nghiệp”. Sau đó, chúng dẫn dụ nạn nhân truy cập đường link lạ, tải ứng dụng giả hoặc mở tệp tin độc hại nhằm chiếm quyền kiểm soát thiết bị.

Bẫy lừa đặt vé, du lịch và mạo danh người thân dịp lễ

Trong dịp cao điểm du lịch, nghỉ dưỡng, kẻ gian giả mạo đại lý bán vé tàu xe, vé máy bay, khách sạn, khu nghỉ dưỡng với mức giá rẻ bất thường. Sau khi tạo lòng tin bằng mã đặt chỗ giả, chúng yêu cầu khách hàng chuyển tiền đặt cọc hoặc cài ứng dụng để “giữ chỗ”, rồi cắt đứt liên lạc hoặc chiếm đoạt thông tin cá nhân.

Đáng chú ý, nhiều đối tượng còn mạo danh người thân, bạn bè trên mạng xã hội, viện lý do “việc gấp”, “nhờ chuyển tiền hộ” để tạo áp lực, thúc giục khách hàng chuyển khoản trong thời gian ngắn.

Khuyến cáo từ VIB

Trước các thủ đoạn trên, VIB khuyến cáo khách hàng tuyệt đối không cung cấp thông tin cá nhân, thông tin thẻ, tên đăng nhập, mật khẩu hoặc mã OTP cho bất kỳ ai dưới bất kỳ hình thức nào. Ngân hàng khẳng định không yêu cầu khách hàng cung cấp thông tin bảo mật qua điện thoại, tin nhắn hay mạng xã hội.

Khách hàng không nên làm theo hướng dẫn của các cá nhân tự xưng là cán bộ cơ quan nhà nước, nhân viên ngân hàng hoặc đơn vị chuyển phát thẻ; không truy cập đường link lạ, không cài đặt ứng dụng không rõ nguồn gốc và không cấp quyền trợ năng cho các ứng dụng đáng ngờ.

VIB cũng lưu ý, việc mua bán, cho thuê, cho mượn hoặc mở hộ tài khoản thanh toán là hành vi vi phạm pháp luật, tiềm ẩn nhiều rủi ro và có thể bị lợi dụng cho các hoạt động bất hợp pháp.

Để đảm bảo an toàn, khách hàng chỉ nên thực hiện xác thực sinh trắc học trên ứng dụng ngân hàng chính thức hoặc trực tiếp tại quầy giao dịch của VIB; thường xuyên kiểm tra biến động tài khoản, kịp thời khóa thẻ hoặc tài khoản khi phát hiện dấu hiệu bất thường và liên hệ ngay với tổng đài VIB hoặc cơ quan chức năng để được hỗ trợ.

Minh Thành