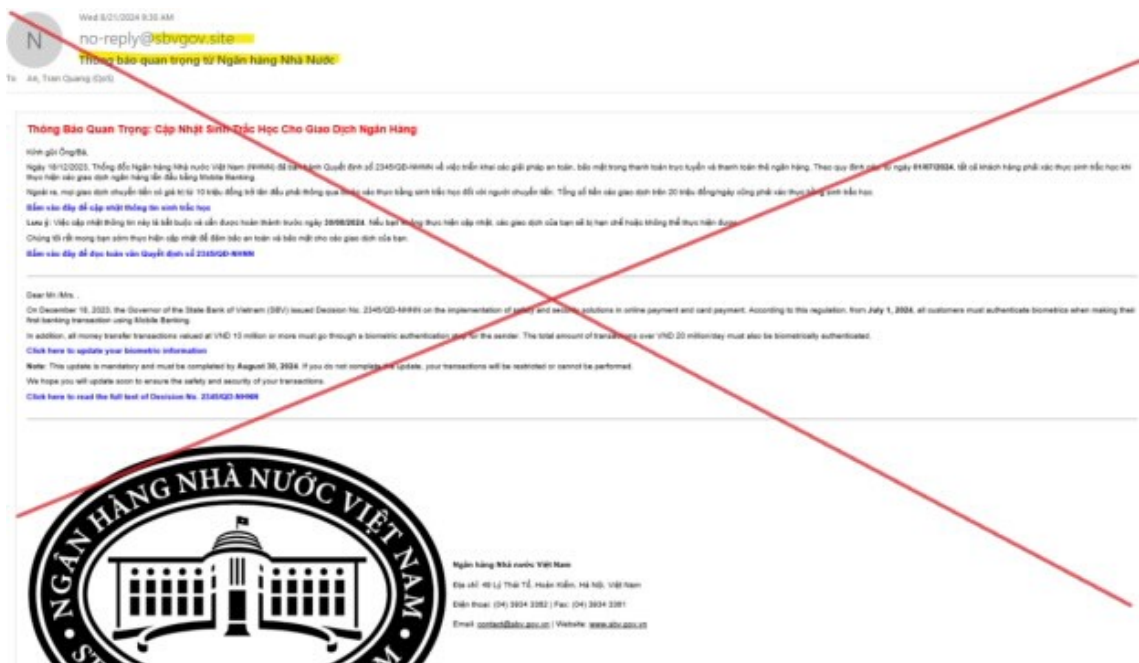


Ngân hàng Nhà nước cảnh báo lừa đảo từ link yêu cầu cập nhật sinh trắc học

17:34 23/08/2024

Đối tượng lừa đảo mạo danh Ngân hàng Nhà nước (NHNN), giả mạo giao diện hộp thư điện tử (e-mail) của NHNN để gửi thông tin dẫn dụ người dân, khách hàng bấm vào đường link lừa đảo cập nhật thông tin sinh trắc học cho giao dịch ngân hàng.



NHNN vừa phát đi thông tin cho biết gần đây có hiện tượng đối tượng lừa đảo mạo danh NHNN, giả mạo giao diện hộp thư điện tử (e-mail) của NHNN để gửi thông tin dẫn dụ người dân, khách hàng bấm vào đường link lừa đảo cập nhật thông tin sinh trắc học cho giao dịch ngân hàng.

Theo đó, nhằm tạo sự tin tưởng của khách hàng nhận thư, đối tượng lừa đảo đã trích dẫn một số quy định tại Quyết định số 2345/QĐ-NHNN ngày 18/12/2023 của NHNN về việc triển khai các giải pháp, an toàn, bảo mật trong thanh toán trực tuyến và thanh toán thẻ ngân hàng và yêu cầu người nhận thư cập nhật thông tin sinh trắc học theo đường link lừa đảo có trong email.

Cụ thể, hòm thư điện tử giả mạo có địa chỉ “no-reply@sbgov.site” gửi thông tin lừa đảo kèm 2 đường link: cập nhật thông tin sinh trắc học, yêu cầu thực hiện trước ngày 30/08/2024; toàn văn Quyết định số 2345/QĐ-NHNN (đính kèm email giả mạo).

NHNN khẳng định đây là hành vi mạo danh NHNN lừa người nhận thư thực hiện theo yêu cầu của kẻ lừa đảo để thu thập thông tin khách hàng. Cụ thể, bằng cách dẫn dụ khách hàng nhận thư bấm vào đường link giả mạo để tải và cài đặt ứng dụng thu thập thông tin sinh trắc học nhưng thực chất là tải về tệp (file) có chứa mã độc, phần mềm gián điệp, khai thác thông tin của khách hàng để chiếm quyền kiểm soát thiết bị cá nhân, tài khoản ngân hàng của khách hàng hoặc đánh cắp thông tin, dữ liệu nạn nhân để thực hiện những hành vi vi phạm pháp luật.

Hiện nay, NHNN chỉ cung cấp thông tin đến công chúng chính thức qua Cổng thông tin điện tử NHNN tại địa chỉ (<https://www.sbv.gov.vn>). NHNN không gửi thư điện tử (email) trực tiếp đến khách hàng của tổ chức tín dụng để nghị cập nhật thông tin sinh trắc học.

NHNN đề nghị người dân, khách hàng các tổ chức tín dụng hết sức đề cao cảnh giác, không bấm vào các đường link lạ được gửi qua chat, SMS hoặc email; không cung cấp thông tin cá nhân cho các trang web không rõ nguồn gốc; không cung cấp mật khẩu dùng một lần (mã OTP), mật khẩu ngân hàng điện tử/ ứng dụng ngân hàng di động (internet banking/ mobile banking)... cho bất kỳ ai, kể cả nhân viên ngân hàng; phải cẩn trọng, cảnh giác khi tiếp nhận, xử lý thông tin, yêu cầu từ các kênh thông tin không chính thức, không rõ nguồn gốc (như thông tin không phải từ các kênh thông tin chính thức của cơ quan nhà nước đã được công bố công khai).

PV