

Không được có chức năng ghi nhớ mật khẩu truy cập trên tất cả App ngân hàng

14:36 19/11/2024

Không được có chức năng ghi nhớ mật khẩu truy cập trên tất cả App ngân hàng, là một trong những quy định tại Thông tư 50 vừa được NHNN ban hành.

Theo đó, Thông tư 50/2024/TT-NHNN ban hành ngày 31/10/2024 quy định các yêu cầu bảo đảm an toàn, bảo mật cho việc cung cấp dịch vụ trực tuyến trong ngành Ngân hàng, bao gồm:

- Hoạt động ngân hàng và các hoạt động kinh doanh khác của tổ chức tín dụng, chi nhánh ngân hàng nước ngoài;
- Hoạt động cung ứng dịch vụ trung gian thanh toán;
- Hoạt động thông tin tín dụng.

Đối tượng áp dụng của Thông tư 50/2024/TT-NHNN bao gồm các tổ chức tín dụng, chi nhánh ngân hàng nước ngoài, tổ chức cung ứng dịch vụ trung gian thanh toán, công ty thông tin tín dụng (sau đây gọi chung là đơn vị).



Tại Điều 8, NHNN quy định Phần mềm ứng dụng Mobile Banking do đơn vị cung cấp phải bảo đảm tuân thủ các quy định tại Điều 7 Thông tư (quy định về Online Banking) và các yêu cầu sau:

Phải được đăng ký và quản lý tại kho ứng dụng chính thức của hãng cung cấp hệ điều hành cho thiết bị di động và hướng dẫn cài đặt rõ ràng trên trang tin điện tử đơn vị để khách hàng tải và cài đặt phần mềm ứng dụng Mobile Banking. Trong trường hợp vì lý do khách quan mà phần mềm ứng dụng Mobile Banking không được đăng ký và quản lý tại kho ứng dụng chính thức của hãng cung cấp hệ điều hành cho thiết bị di động, đơn vị phải có phương thức hướng dẫn, thông báo, hỗ trợ cài đặt phần mềm ứng dụng Mobile Banking bảo đảm an toàn, bảo mật cho khách hàng và báo cáo về Ngân hàng Nhà nước (Cục Công nghệ thông tin) trước khi cung cấp dịch vụ.

Phải được áp dụng các biện pháp bảo vệ để hạn chế dịch ngược mã nguồn.

Có biện pháp bảo vệ, chống can thiệp vào luồng trao đổi dữ liệu trên ứng dụng Mobile Banking và giữa ứng dụng Mobile Banking với máy chủ cung cấp dịch vụ Online Banking.

Triển khai các giải pháp nhằm phòng, chống, phát hiện các hành vi can thiệp trái phép vào ứng dụng Mobile Banking đã cài đặt trong thiết bị di động của khách hàng.

Không cho phép chức năng ghi nhớ mã khóa bí mật truy cập.

Đối với khách hàng cá nhân, phải có chức năng kiểm tra khách hàng khi khách hàng truy cập lần đầu hoặc khi khách hàng truy cập trên thiết bị khác với thiết bị đã thực hiện giao dịch bằng ứng dụng Mobile Banking lần gần nhất. Việc kiểm tra khách hàng tối thiểu bao gồm:

a) Khớp đúng SMS OTP hoặc Voice OTP thông qua số điện thoại đã được khách hàng đăng ký hoặc Soft OTP/Token OTP;

b) Khớp đúng thông tin sinh trắc học theo quy định tại khoản 5 Điều 11 Thông tư này trong trường hợp văn bản pháp luật chuyên ngành liên quan đến dịch vụ cung cấp trên phần mềm ứng dụng Mobile Banking có quy định thu thập, lưu trữ thông tin sinh trắc học của khách hàng.

Được biết, hình thức xác nhận bằng mã khóa bí mật (Password) là Khách hàng sử dụng mã khóa bí mật gồm một chuỗi ký tự để xác nhận quyền truy cập của khách hàng vào hệ thống thông tin, ứng dụng, dịch vụ hoặc xác nhận khách hàng thực hiện giao dịch: Hình thức xác nhận bằng mã khóa bí mật phải đáp

ứng yêu cầu:

- Mã khóa bí mật có độ dài tối thiểu 8 ký tự và cấu tạo bao gồm tối thiểu các ký tự: số, chữ hoa, chữ thường;
- Thời gian hiệu lực của mã khóa bí mật tối đa 12 tháng, đối với mã khóa bí mật được cấp phát mặc định lần đầu: thời gian hiệu lực tối đa là 30 ngày.

Thu Trang (t/h)