

Hàng rào mới cho ví điện tử: MoMo và ZaloPay siết chặt bảo mật theo Thông tư 77/2025

13:08 07/03/2026

Tiếp nối làn sóng thắt chặt an ninh của các ngân hàng, những nền tảng thanh toán hàng đầu Việt Nam như MoMo và ZaloPay đã đồng loạt nâng cấp hệ thống bảo mật theo Thông tư 77/2025/TT-NHNN. Động thái này nhằm phát hiện và ngăn chặn các thiết bị "không sạch" truy cập vào hệ thống, đảm bảo an toàn tuyệt đối cho tài sản của người dùng trong bối cảnh tội phạm mạng ngày càng tinh vi.



Các nền tảng thanh toán như MoMo, Zalopay đã nâng cấp bảo mật theo Thông tư 77/2025/TT-NHNN và chặn những thiết bị thiếu an toàn

Theo nội dung nâng cấp, cả MoMo và ZaloPay đều thiết lập cơ chế tự động thoát hoặc dừng ứng dụng nếu hệ thống phát hiện dấu hiệu mất an toàn từ thiết bị của người dùng. Một thiết bị được đánh giá là không đủ tiêu chuẩn bảo mật khi rơi vào các trường hợp như đã bị can thiệp hệ thống (root, jailbreak hoặc mở khóa bootloader), hoặc đang chạy trên các trình giả lập, máy ảo.

Bên cạnh đó, việc người dùng bật các công cụ can thiệp kỹ thuật dành cho nhà phát triển như USB Debugging (gỡ lỗi USB), ADB cũng sẽ bị hệ thống từ chối truy cập. Quy định này cũng áp dụng nghiêm ngặt đối với các bản ứng dụng bị chỉnh sửa hoặc đóng gói lại không chính thức (thường là các tệp APK hoặc IPA lậu), vốn tiềm ẩn nguy cơ bị chèn mã độc để đánh cắp thông tin giao dịch.

Việc các ví điện tử phải "mạnh tay" thắt chặt bảo mật là hệ quả tất yếu khi nền tảng di động trở thành mục tiêu hàng đầu của tội phạm mạng. Chỉ riêng trong năm 2025, hệ thống phòng chống lừa đảo nTrust đã ghi nhận hơn 62.900 loại mã độc mới trên điện thoại tại Việt Nam. Đáng lo ngại hơn, có gần 1.000 ứng dụng giả mạo được thiết kế tinh vi nhằm chiếm quyền điều khiển thiết bị hoặc âm thầm đánh cắp mã OTP.

Các chuyên gia an ninh mạng cảnh báo rằng, những hành vi tưởng chừng vô hại như tùy biến giao diện hay cài ứng dụng ngoài nguồn chính thống thực chất đã mở ra "cánh cửa hậu" cho phần mềm gián điệp. Những mã độc này có thể theo dõi toàn bộ thao tác bàn phím và màn hình, cho phép kẻ xấu kiểm soát ví điện tử của nạn nhân một cách dễ dàng.

Để xử lý triệt để tình trạng bị chặn truy cập, người dùng được khuyến cáo nên khôi phục cài đặt gốc của điện thoại để đưa hệ điều hành về trạng thái nguyên bản. Đối với những thiết bị đã bị can thiệp sâu vào phần mềm, việc tìm đến các trung tâm kỹ thuật uy tín để chạy lại firmware chính hãng là giải pháp bắt buộc.

Mặc dù việc siết chặt bảo mật theo Thông tư 77/2025 có thể gây ra những bất tiện nhất thời, đặc biệt với nhóm người dùng am hiểu kỹ thuật thích tùy biến máy, nhưng đây là bước đi không thể đảo ngược. Trong kỷ nguyên mà chiếc điện thoại đã thực sự trở thành một ví tài chính số di động, việc duy trì một thiết bị "sạch" và hệ điều hành nguyên bản chính là cách hữu hiệu nhất để bảo vệ tài sản cá nhân trước mọi nguy cơ tấn công từ không gian mạng.

Tâm An