

Smartphone bị bẻ khóa sẽ bị chặn quyền giao dịch ngân hàng từ 1/3

10:44 10/01/2026

Kể từ ngày 1/3/2026, những thiết bị di động không đáp ứng đầy đủ các tiêu chuẩn về an toàn và bảo mật sẽ chính thức bị chặn quyền thực hiện giao dịch trên các ứng dụng ngân hàng. Đây là nội dung trọng tâm tại Thông tư số 77/2025/TT-NHNN vừa được Thống đốc Ngân hàng Nhà nước ký ban hành. Những thay đổi này yêu cầu người dùng phải chủ động kiểm tra thiết bị để tránh tình trạng gián đoạn giao dịch trực tuyến trong thời gian tới.



Nếu thiết bị di động của bạn nằm trong nhóm các thiết bị không đáp ứng được tiêu chuẩn an toàn và bảo mật thì sẽ không thể tiếp tục dùng các ứng dụng ngân hàng để giao dịch từ ngày 1/3.

Ba dấu hiệu khiến ứng dụng ngân hàng tự động ngừng hoạt động

Để đối phó với các công nghệ lừa đảo tinh vi như Deepfake hay mã độc, Ngân hàng Nhà nước đã thiết lập cơ chế phòng vệ chủ động ngay trên thiết bị của khách hàng thông qua các quy định kỹ thuật nghiêm ngặt. Theo đó ứng dụng

Mobile Banking sẽ tự động thoát hoặc ngừng hoạt động đồng thời phát thông báo cho người dùng nếu phát hiện một trong ba tình trạng mất an toàn hệ thống.

Đầu tiên là các thiết bị đã bị can thiệp sâu vào hệ thống như bẻ khóa root đối với hệ điều hành Android hoặc jailbreak đối với iPhone cùng các thiết bị đã mở khóa cơ chế bảo vệ bootloader. Việc người dùng tự ý thay đổi thiết lập hệ thống để cài ứng dụng ngoài luồng được đánh giá là tạo môi trường lý tưởng cho mã độc xâm nhập và đánh cắp thông tin.

Tiếp theo là trường hợp phần mềm ứng dụng bị chèn mã bên ngoài hoặc bị đóng gói lại nhằm thực hiện các hành vi ghi lại lịch sử dữ liệu trái phép khi đang vận hành. Cuối cùng các giao dịch sẽ bị từ chối nếu hệ thống phát hiện ứng dụng chạy trên môi trường giả lập hoặc máy ảo cũng như khi thiết bị đang kết nối trực tiếp với máy tính qua chế độ giao tiếp kỹ thuật dành cho lập trình viên.

Siết chặt trách nhiệm của ngân hàng trong việc bảo mật ứng dụng

Thông tư 77 không chỉ đặt ra yêu cầu đối với thiết bị của người dùng mà còn quy định trách nhiệm rất cao đối với các đơn vị phát hành ứng dụng ngân hàng. Các tổ chức tín dụng có nhiệm vụ định kỳ tối thiểu ba tháng một lần phải thực hiện đánh giá an toàn toàn diện để xác định và vá các lỗ hổng tiềm ẩn trước khi chúng bị tội phạm mạng khai thác.

Trong trường hợp phát hiện lỗ hổng ở mức độ cao hoặc đặc biệt nghiêm trọng, đơn vị phát hành phải lập tức triển khai biện pháp kiểm soát giao dịch để bảo vệ tài sản cho khách hàng. Đặc biệt thời hạn khắc phục các lỗ hổng này đã được rút ngắn tối đa theo quy định mới. Cụ thể là các thành phần hệ thống kết nối trực tiếp với Internet phải được xử lý và cập nhật phiên bản mới trong vòng hai mươi tư giờ. Đối với các thành phần còn lại thời hạn xử lý dao động từ một đến hai tháng tùy theo mức độ nghiêm trọng của lỗ hổng bảo mật.

Quy định mới này được xem là bước đi quyết liệt nhằm làm sạch hệ sinh thái giao dịch trực tuyến và xây dựng lá chắn vững chắc trước các cuộc tấn công mạng ngày càng tinh vi. Những người dùng đang sử dụng smartphone không đáp ứng tiêu chuẩn an toàn cần sớm khôi phục thiết bị về trạng thái nguyên bản hoặc cập nhật phần mềm để đảm bảo quyền lợi giao dịch khi Thông tư chính thức có hiệu lực từ đầu tháng 3.

Tâm An (t/h)