

Apple có kế hoạch trang bị tính năng chống trộm trong bản cập nhật phần mềm iOS 17.3 sắp tới

11:02 14/12/2023

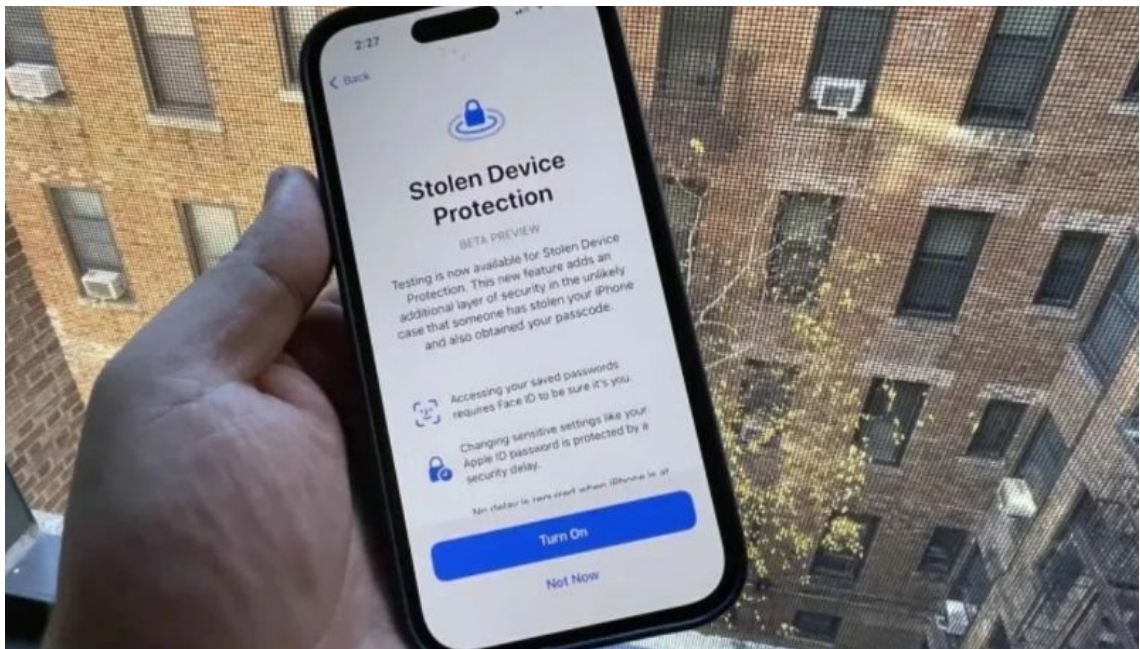
Apple có kế hoạch ra mắt tính năng Stolen Device Protection trong bản cập nhật phần mềm iOS 17.3 sắp tới, nhằm tăng cường bảo mật cho iPhone bị mất cắp.

Theo *Wall Street Journal*, từ đầu năm 2023 đến nay, tại Mỹ xảy ra hàng trăm vụ trộm iPhone ở New York, Chicago, New Orleans, Minneapolis và các thành phố khác. Trong đó, kẻ trộm theo dõi nạn nhân để biết mật khẩu điện thoại, sau đó đánh cắp thiết bị, thay đổi tài khoản Apple, trộm tiền và dữ liệu người dùng trong iCloud.

Trước tình trạng trên, Apple dự kiến đưa tính năng Bảo vệ thiết bị bị đánh cắp (Stolen Device Protection) vào bản cập nhật phần mềm iOS 17.3 sắp tới.

Những thay đổi trên iPhone khi cài “Bảo vệ thiết bị bị đánh cắp”

Sau khi tính năng Bảo vệ thiết bị bị đánh cắp được bật, iPhone sẽ hạn chế một số tác vụ quan trọng khi người dùng ở xa các địa điểm quen thuộc (như nhà riêng hoặc cơ quan).



Trong bản iOS 17.3 beta, Apple sẽ nhắc người dùng kích hoạt tính năng Bảo vệ thiết bị bị đánh cắp.

Đầu tiên là việc thay đổi mật khẩu ID Apple. Nhiều tên trộm sau khi biết được mật khẩu iPhone sẽ thay đổi mật khẩu Apple ID, tắt chế độ Find My và xóa sạch dữ liệu của nạn nhân trong điện thoại để bán lại. Với tính năng Bảo vệ thiết bị bị đánh cắp, khi người dùng muốn thay đổi mật khẩu Apple ID khi ở xa một địa điểm quen thuộc, thiết bị sẽ yêu cầu Face ID hoặc Touch ID. Sau một giờ chờ đợi, người dùng phải xác nhận lại bằng một lần quét Face ID hoặc Touch ID nữa. Lúc này mật khẩu mới được thay đổi.

Mật khẩu cũng là “chìa khóa” để cài đặt Khóa khôi phục trên iPhone. Khi kẻ trộm thêm hoặc thay đổi Khóa khôi phục cho thiết bị, chủ nhân của nó sẽ không thể đặt lại mật khẩu Apple ID bằng số điện thoại hoặc email, đồng nghĩa với việc họ sẽ mất quyền truy cập vào tất cả dữ liệu được lưu trong iCloud. Với tính năng Bảo vệ thiết bị bị đánh cắp, tương tự khi thay đổi mật khẩu Apple ID, việc bật hoặc thay đổi Khóa khôi phục cũng yêu cầu hai lần quét sinh trắc học cách nhau một giờ.

Chuỗi khóa trong iPhone là nơi lưu trữ mật khẩu cho các ứng dụng ngân hàng, tài khoản MXH... Kẻ trộm có thể sử dụng mật mã iPhone để mở Chuỗi khóa và truy cập tất cả chúng. Tính năng Bảo vệ thiết bị bị đánh cắp yêu cầu người dùng cung cấp Face ID hoặc Touch ID để truy cập Chuỗi khóa, mật khẩu hoàn toàn không có hiệu lực.

Vẫn có hạn chế

Ngay cả khi tính năng Bảo vệ thiết bị bị đánh cắp được bật, những ứng dụng không được bảo vệ bằng mật khẩu hoặc mã PIN đều dễ dàng bị tấn công nếu kẻ trộm biết được mật khẩu điện thoại. Ngoài ra, Apple Pay vẫn hoạt động với mật khẩu nếu Face ID hoặc Touch ID không thành công.

Để ngăn chặn tình trạng này, người dùng cần tránh tiết lộ mật khẩu điện thoại cho người lạ, sử dụng Face ID hoặc Touch ID và hạn chế nhập mật khẩu điện thoại ở nơi công cộng. Việc tạo mật khẩu có cả chữ và số cũng rất hữu ích, bạn chỉ cần đi tới Cài đặt --> Face ID & Mật mã > Thay đổi mật mã --> Tùy chọn mật mã --> Mã chữ và số tùy chỉnh.

Đối với các ứng dụng tiền mặt và tiền điện tử, người dùng có thể thêm mã PIN hoặc sinh trắc học bổ sung để tăng tính bảo mật. Khi phát hiện điện thoại đã mất, cần xóa thiết bị từ xa càng nhanh càng tốt thông qua địa chỉ icloud.com/find. Người dùng có thể truy cập địa chỉ này trên mọi thiết bị hoặc trình duyệt web để đăng nhập và xóa dữ liệu từ xa.

Khi Apple phát hành Bảo vệ thiết bị bị đánh cắp, hãng có kế hoạch nhắc người dùng bật tính năng này. Bạn sẽ tìm thấy tính năng này trong mục Face ID & Passcode.

Hà Trần (t/h)