

Dù đã bật xác thực 2 yếu tố, nhiều người dùng vẫn bị hacker chiếm dụng tài khoản Gmail

16:48 16/04/2024

Hacker đã vượt qua được lớp bảo mật xác thực hai yếu tố (2FA) để chiếm đoạt tài khoản Gmail của nhiều người dùng. Nạn nhân của vụ tấn công này thường là những người đã tham gia vào một chương trình khuyến mãi tiền số Ripple (XRP) giả mạo.

Một nhóm hacker đã vượt qua được lớp bảo mật xác thực hai yếu tố (2FA) để chiếm đoạt tài khoản Gmail của nhiều người dùng. Nạn nhân của vụ tấn công này thường là những người đã tham gia vào một chương trình khuyến mãi tiền số Ripple (XRP) giả mạo. Họ đã không thể truy cập vào tài khoản Google của mình mặc dù có bật chức năng 2FA.

Ngay sau đó, nhiều người dùng đã lên các diễn đàn như Reddit và trang hỗ trợ của Google để tìm kiếm sự giúp đỡ trong việc khôi phục tài khoản. Trong quá khứ, các câu hỏi thường xoay quanh việc quên mật khẩu hay thay đổi số điện thoại dùng để xác thực. Tuy nhiên, việc lấy lại tài khoản Google mà không thể sử dụng 2FA cũng khiến nhiều người đặt ra câu hỏi cho tính khả thi của chuyện này.



Hacker thậm chí có thể bỏ qua bảo mật 2 bước (2FA) để tấn công và chiếm dụng tài khoản Gmail

Theo nhiều nguồn tin đã chỉ ra, các hacker đã phát tán một đường link giả mạo, mời chào người dùng gửi vào một ví mà kẻ lừa đảo dựng lên với vỏ bọc là "do Ripple quản lý". Hacker còn sử dụng video deepfake của CEO Ripple Labs để thuyết phục người dùng. Nếu người dùng nhấp vào liên kết này, một mã độc sẽ xâm nhập vào máy tính và thu thập cookie từ trình duyệt, sau đó gửi chúng về máy chủ từ xa. Điều này cho phép hacker xóa bỏ lớp bảo mật 2FA và truy cập vào tài khoản mà không cần mật khẩu.

Ngoài ra, Google cũng thừa nhận rằng vấn đề đánh cắp cookie đã tồn tại từ lâu và vẫn chưa có cách khắc phục hoàn toàn. Google đang cập nhật liên tục các kỹ thuật để phát hiện và chặn quyền truy cập đáng ngờ khi cookie bị đánh cắp. Đối với những tài khoản bị hack, Google cung cấp quy trình khôi phục tự động, cho phép sử dụng các yếu tố khôi phục ban đầu trong vòng tối đa 7 ngày.

Trong bối cảnh này, các chuyên gia an ninh mạng khuyên rằng người dùng nên kết hợp nhiều biện pháp bảo mật khác như đổi mật khẩu thường xuyên, bật bảo mật hai lớp, và sử dụng phần mềm có bản quyền. Họ cũng cảnh báo người dùng về việc thận trọng với các tệp và liên kết đáng ngờ, đặc biệt là trên YouTube, nơi mà các video có thể chứa các mô tả đính kèm liên kết độc hại.

Hà Trần (t/h)