

# Tuyệt chiêu chống đạo tặc Wi-Fi

Source: Tin Viet Online



**Kết nối mạng không dây mang lại nhiều lợi ích cho người dùng nhưng thực tế nó cũng ẩn chứa nhiều rủi ro. Rủi ro từ những kẻ thường xuyên sử dụng Wi-Fi chùa khiến cước thanh toán của bạn “đội” lên hàng chục lần và máy tính của bạn bỗng nhiên trở thành nạn nhân tấn công của virus.**

Sau đây là một vài “chiêu” giúp bạn giảm thiểu rủi ro khi dùng chùa Wi-Fi.

## 1. Sử dụng mã hóa

Nếu bạn không thuyết phục nên nghĩ xem: dữ liệu không dây được truyền trong không khí nên tin tức dễ dàng bị phát hiện nếu ai đó nghe trộm trên dây cáp. Hacker mạng Ethernet, hacker sử dụng công cụ tấn công mạng này hoặc phần mềm để truy cập vào cáp Ethernet và mã hóa khóa mã. Tuy nhiên, thậm chí nếu không dây, tin tức vẫn có thể bị rò rỉ qua sóng của Wi-Fi. Một số có thể ứng dụng nghe lén và dùng máy tính để bắt sóng Wi-Fi bằng ngón tay, nó sẽ kêu bíp bíp hay bắt đèn xanh đèn đỏ khi phát hiện ra có sóng radio Wi-Fi với giá vài chục ngàn đồng.

**Mã hóa:** Tất cả các thiết bị Wi-Fi sử dụng công nghệ mã hóa WEP (Wired Equivalent Privacy). WEP sử dụng thuật toán mã hóa dữ liệu trên mạng không dây nên các thiết bị dò sóng không thể bắt được tín hiệu. Khi cài đặt WEP, bạn nên nhập mật khẩu cho các cấu hình của thiết bị trên mạng. Nếu thiết bị này sử dụng mã hóa WEP - sử dụng mã hóa và giải mã dữ liệu truyền trên mạng.

## 2. Kỹ thuật NAT

Kiểm tra Wi-Fi thường xuyên thì rất tốt nhưng nếu bạn là thành viên của một gia đình nhỏ. Bạn nên sử dụng tường lửa để ngăn chặn kẻ xấu thích dùng “Wi-Fi chùa”. Hầu hết các router đều tích hợp tính năng NAT (network address translation). Tường lửa này có chức năng giúp các địa chỉ IP cá nhân ẩn giấu. Vì thế, khi kết nối Internet, trên máy tính sẽ xuất hiện một địa chỉ của router. Vì vậy, khi nhận tin tức khó lòng xác định được địa chỉ cá nhân của bạn trên Wi-Fi.

Tuy nhiên, NAT không có khả năng kiểm tra dữ liệu bên trong gói thông tin truyền qua router. Vì thế, nếu bạn dùng nên sử dụng thêm một tường lửa cá nhân cho mình, có thể là SPI. Tường lửa SPIs xác định gói dữ liệu truyền nào có hợp pháp, từ đó quyết định việc cho nó đi hay không. Không phải tất cả các router đều có tường lửa này nên khi mua sản phẩm bạn nên lưu ý.

## 3. Những “thủ thuật” cho kỹ thuật

Hầu hết các thiết bị Wi-Fi sử dụng sản phẩm của nhà sản xuất cài đặt theo cách mặc định thì tin tức dễ dàng bị kẻ xấu dùng Wi-Fi miễn phí.

Ví dụ, các router sử dụng giao thức DHCP (dynamic host configuration protocol) có thể tự động quản lý thông tin địa chỉ IP cho các máy tính sử dụng mạng. Tuy nhiên, việc kiểm soát thông tin này là nguyên nhân có nhiều khách không muốn dùng chùa Wi-Fi. Vì thế, bạn nên tự quản lý các địa chỉ IP tĩnh cho các máy tính và thiết bị mạng máy chủ (server) DHCP của router.

Để cấu hình cho địa chỉ IP, click chuột phải vào biểu tượng *Network Neighborhood* và chọn *Properties*. Một cửa sổ xuất hiện liệt kê các bộ vi xử lý (adapter) của mạng. Chọn chuột phải vào adapter mà bạn dùng kết nối với mạng LAN, sau đó chọn *Properties*.

Trong cửa sổ *Local area connection properties* xuất hiện, chọn *Internet Protocol (TCP/IP)* và nhấp vào nút *Properties* để cấu hình. Cửa sổ này sẽ cho phép bạn sử dụng địa chỉ IP tĩnh, dải con, *subnet mask*, *default gateway* và *DNS server*.

Hầu hết các mạng gia đình sử dụng bộ công cụ các "war drivers", đó là những người giúp cho các hacker thâm nhập, phá hoại mạng không dây của bạn. Có rất nhiều cách bạn có thể thực hiện việc này như thi công lắp đặt router để bảo vệ chính mình.

Nhưng bạn không muốn loay hoay quanh việc địa chỉ MAC, thay vì SSID (tên mạng) hay vô hiệu hóa tên quảng bá SSID? Bạn nên sử dụng một chương trình bảo mật miễn phí có thể chỉ định vị trí thay cho bạn. Network Magic là sản phẩm nổi tiếng nhất hiện nay, miễn phí và trực tuyến.

Sau khi cài đặt, nó sẽ kiểm tra router, toàn bộ mạng và xây dựng một mạng vật lý các thiết bị kết nối bên trong. Sau đó nó kiểm tra các thiết bị kết nối cho router và ghi danh sách nó tìm thấy. Ví dụ, nếu nó phát hiện ra bạn đang quảng bá SSID của bạn, nó sẽ cảnh báo bạn. Chọn một tùy chọn nhấp chuột vào hộp checkbox, Network Magic sẽ ngay lập tức quảng bá cho bạn.

Phiên bản trực tuyến có thêm một số tính năng khác như cấu hình cho thẻ mạng và chia sẻ máy in, nhưng nếu bạn quan tâm đến vấn đề bảo mật thì bạn không cần dùng phiên bản đó.

**Th o Trang**  
Theo *CNet*