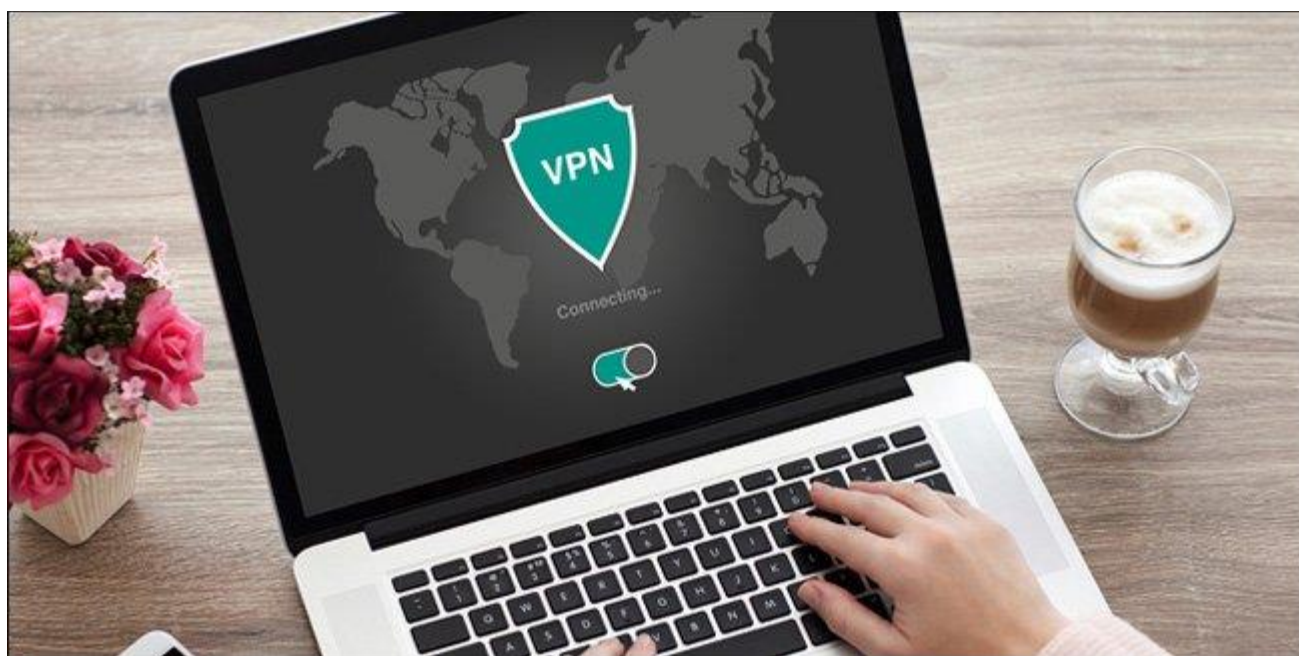


Các phương pháp fake IP giúp bạn truy cập ẩn danh

Trong nhiều bài viết trước đây, chúng tôi đã từng đề cập tới vấn đề ẩn danh trực tuyến là điều vô cùng quan trọng. Những thông tin riêng tư bị rò rỉ mỗi năm khiến vấn đề bảo mật trực tuyến ngày càng trở nên cần thiết. Đó cũng chính là lý do chúng ta nên sử dụng địa chỉ IP ảo. Dưới đây, chúng ta sẽ cùng tìm hiểu các phương pháp tạo fake IP nhé!

Phương pháp 1 - Sử dụng VPN



VPN là mạng riêng ảo nhưng cách sử dụng thì đơn giản hơn nhiều so với cái tên của nó. Về cơ bản, bạn có thể kết nối máy tính hoặc thiết bị của mình với mạng của người khác, sau đó duyệt web qua mạng của họ. Khi bạn kết nối với VPN, nghĩa là bạn đang giấu địa chỉ IP của mình bằng một trong những địa chỉ IP khác trong mạng đó. Tuy nhiên, để đạt được sự riêng tư cao nhất, chúng tôi khuyên bạn nên sử dụng dịch vụ VPN phiên bản trả phí để đảm bảo an toàn tuyệt đối.

Bắt đầu với VPN

Có rất nhiều dịch vụ VPN nhưng bạn nên xem xét ExpressVPN và NordVPN bởi chúng đều là những lựa chọn tuyệt vời. Dù bạn chọn bất kỳ dịch vụ nào, bạn cũng chỉ cần tải ứng dụng về, chạy và sử dụng nó để kết nối với VPN theo yêu cầu. Các thao tác này thực sự rất đơn giản.

VPN là một dịch vụ hữu ích và rất đáng tin cậy.

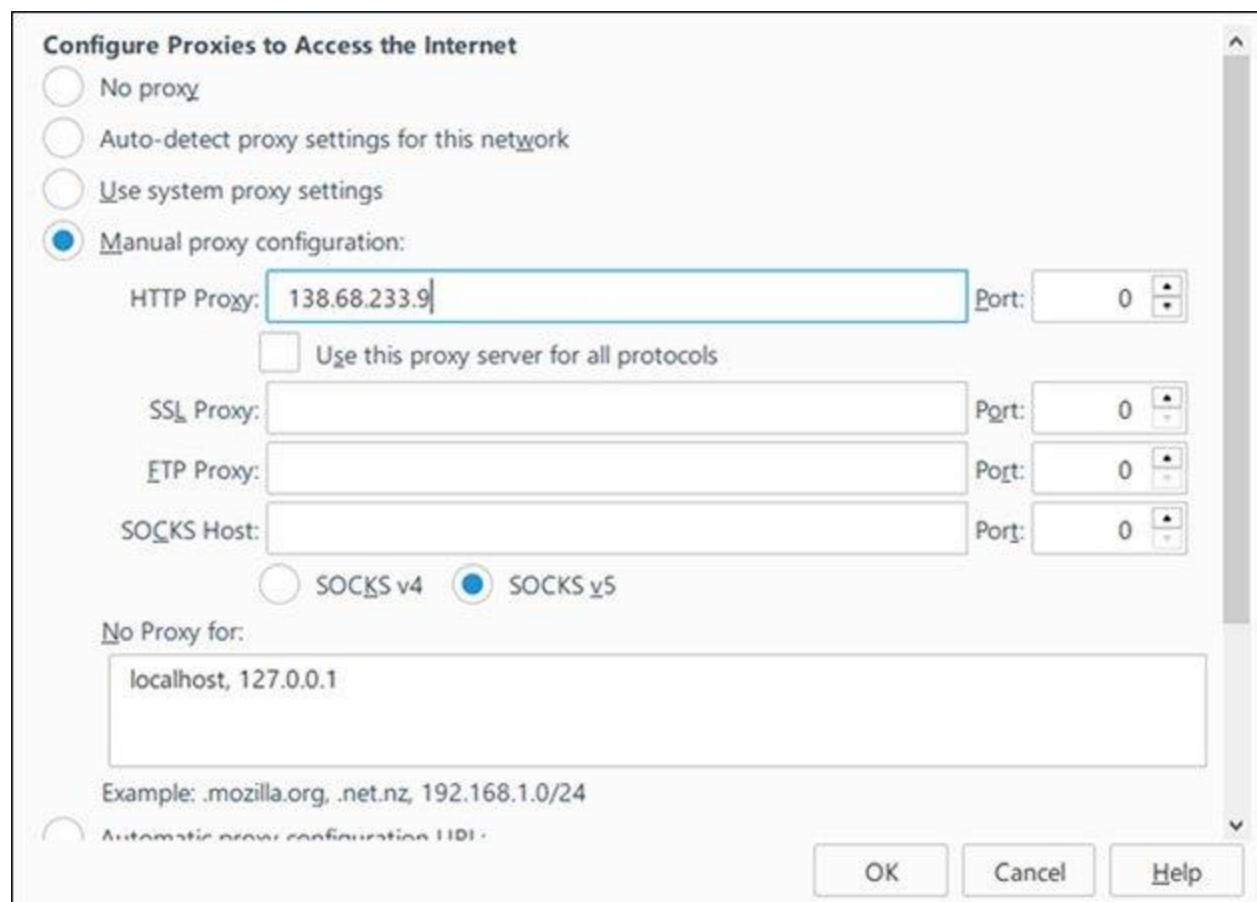
Phương pháp 2 – Sử dụng Web Proxy

Web proxy hoạt động tương tự như VPN: bạn kết nối tới máy chủ proxy, sau đó tất cả lưu lượng truy cập web của bạn sẽ chạy qua máy chủ proxy. Như vậy, địa chỉ IP của bạn sẽ được ẩn bởi địa chỉ IP của máy chủ này.

Cách thiết lập web proxy

Tìm một dịch vụ web proxy miễn phí sử dụng như một trang web như PremProxy hoặc Proxy List.

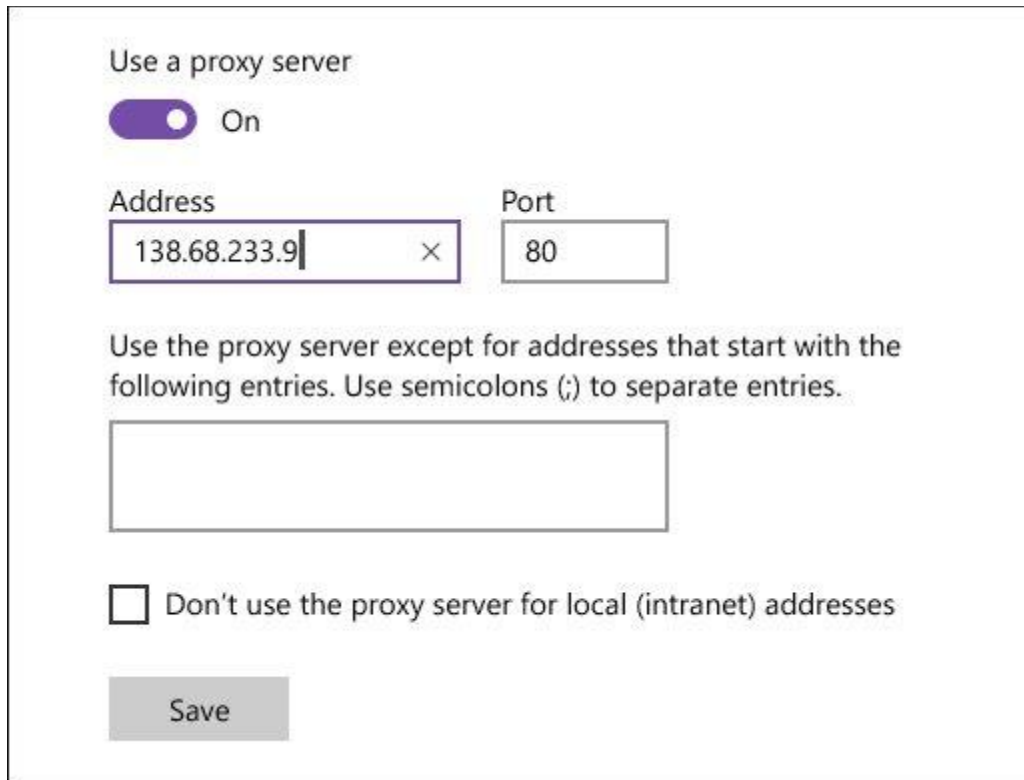
Trong Firefox



- Trong menu chính, chọn **Options**.
- Điều hướng tới tab **Advanced**, sau đó tới phần **Network**.

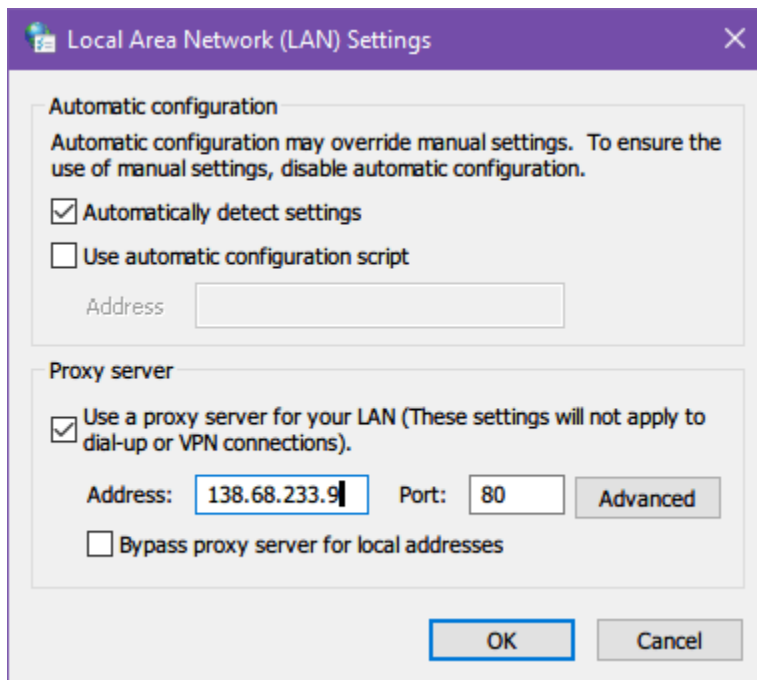
- Trong Connection, nhấp chọn **Settings**.
- Chọn **Manual proxy configuration**, sau đó nhập địa chỉ vào công proxy vào trường HTTP Proxy.

Trong trình duyệt Edge

The image shows the proxy settings interface in the Microsoft Edge browser. At the top, there is a toggle switch labeled "Use a proxy server" which is currently turned "On". Below this, there are two input fields: "Address" containing "138.68.233.9" and "Port" containing "80". Underneath these fields is a text area with the instruction: "Use the proxy server except for addresses that start with the following entries. Use semicolons (;) to separate entries." Below the text area is an empty input field for these exceptions. At the bottom, there is a checkbox labeled "Don't use the proxy server for local (intranet) addresses" which is currently unchecked. A "Save" button is located at the very bottom of the settings panel.

- Trong menu chính, chọn **Settings**.
- Cuộn xuống và nhấp vào **View advanced settings**.
- Tiếp tục cuộn xuống và nhấp chọn **Open proxy settings**.
- Trong Manual proxy setup, kích hoạt **Use a proxy server**, sau đó nhập địa chỉ và công proxy vào trường Address.

Trong trình duyệt Chrome, Opera và Vivaldi



- Trong phần Network, nhấp chọn **Change proxy settings**.
- Trong tab Connection, nhấp chọn **LAN settings**.
- Kích hoạt **Use a proxy server for your LAN**, sau đó nhập địa chỉ và cổng proxy vào Address.

Chrome, Opera, Vivaldi và các trình duyệt dựa trên Chromium khác không có tính năng proxy được tích hợp sẵn trong trình duyệt mà nó sử dụng cài đặt proxy cho toàn hệ thống.

Phương pháp 3 – Sử dụng Wi-Fi công cộng

Thay vì định tuyến lưu lượng truy cập của bạn qua mạng của người khác, bạn có thể chọn cách kết nối trực tiếp với mạng của họ - và cách đơn giản nhất là sử dụng Wi-Fi công cộng.

Khi bạn sử dụng Wi-Fi công cộng, không có cách nào để ai đó có thể theo dõi bạn cả. Với những địa điểm như các quán cà phê Starbuck hay sân bay thì hoạt động của bạn sẽ bị che khuất bởi hàng chục người dùng khác nữa.



Tuy nhiên, sử dụng Wi-Fi công cộng đôi lúc cũng có những rủi ro. Theo mặc định, hầu hết các điểm truy cập Wi-Fi công cộng không được mã hóa nên thiết bị của bạn có nguy cơ bị lây nhiễm phần mềm độc hại. Bên cạnh đó, tin tặc có thể đánh cắp danh tính của bạn trên Wi-Fi công cộng. Vì vậy, dù bạn đang ẩn địa chỉ IP của mình thì vẫn có nguy cơ gặp các rủi ro bảo mật và riêng tư khác.

Hầu hết chúng ta đều có xu hướng chia sẻ quá nhiều thông tin trực tuyến. Nếu bạn thực sự lo lắng về vấn đề bảo mật thì hãy thay đổi các thói quen xấu đó và chú ý tới các mẹo bảo mật trực tuyến trên nhé.