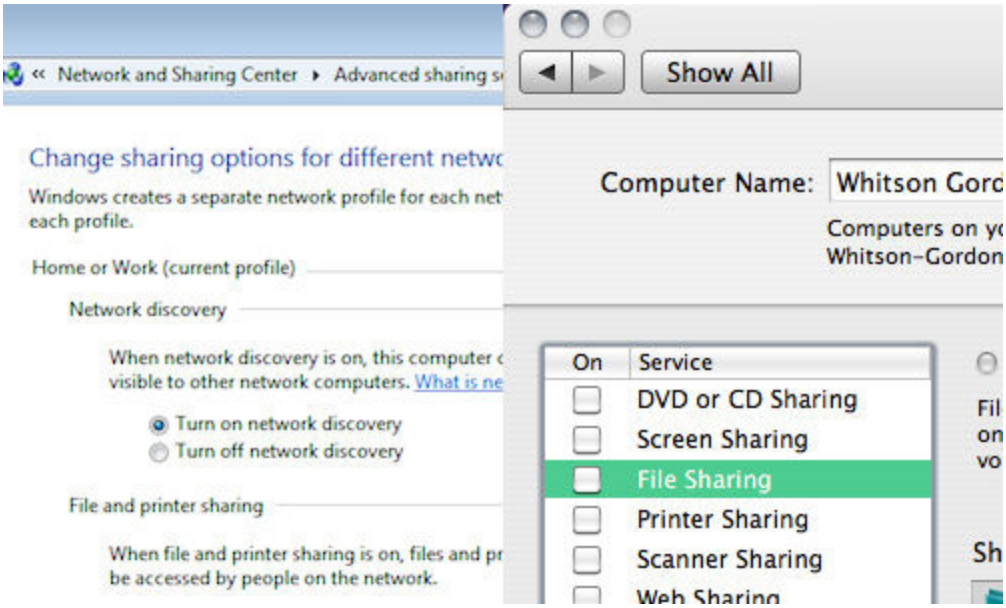
Giữ an toàn khi sử dụng mạng Wi – Fi công cộng-P1

Việc sử dụng các mạng không dây công cộng luôn mang lại nhiều rủi ro không đáng có cho máy tính của bạn. Trong bài viết này, chúng tôi sẽ cung cấp tới bạn một số giải pháp hữu dụng cho cả máy PC lẫn máy Mac cần đảm bảo để an toàn khi vào mạng công cộng.

Hầu hết các đường truyền không dây đều có firewall bảo vệ, nhưng điều này không có nghĩa là bạn sẽ được bảo vệ hoàn toàn khỏi các mạng tương tự. Rất nhiều địa điểm truy cập Wi Fi hiện nay không được bảo mật, và thường rất dễ kết nối. Chính vì thế, điều này sẽ không bảo vệ bạn chống lại những kẻ hacker ở cùng quán cafe mà bạn đang ngồi, do đó cần có một vài cài đặt bảo vệ bạn khi kết nối với mạng công cộng. *Chúng tôi sẽ chỉ ra cho bạn những cài đặt quan trọng nhất cũng như cách thiết lập tự động thay đổi thích hợp với từng mức độ an toàn cụ thể mỗi khi bạn kết nối với mạng công cộng*

Cài đặt



Tắt hệ thống chia sẻ

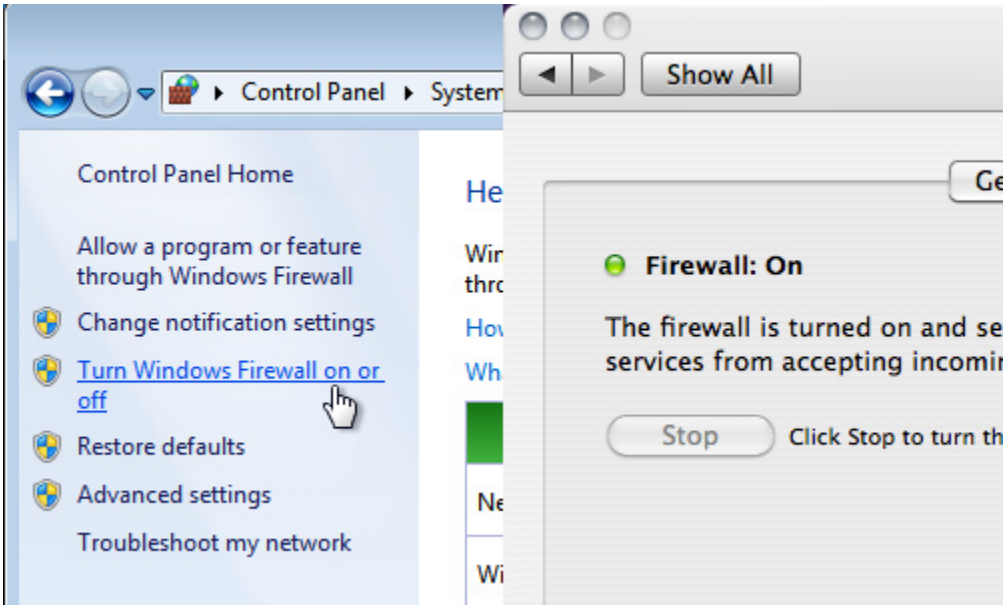
Khi ở nhà, bạn có thể chia sẻ dữ liệu, kết nối máy in, thậm chí cho phép đăng nhập từ xa bởi một chiếc máy tính khác cùng mạng. Khi kết nối mạng công cộng, bạn nên tắt những chức năng này,

vì có thể bất cứ ai cũng có thể truy cập nó, thậm chí không cần phải là hacker, mà chỉ cần dựa trên cài đặt của bạn. Vậy làm thế nào có thể tắt được cài đặt chia sẻ.

Trong Windows: Mở **Control Panel**, sau đó vào trình duyệt **Network and Internet** -> chọn **Network and Sharing Center**, sau đó click chọn **Homegroup and Sharing Option** và đổi thiết lập chia sẻ theo nhu cầu, tại đây bạn nên tắt các chức năng chia sẻ file và kết nối máy in. Tốt nhất bạn cũng nên tắt chức năng tìm kiếm mạng và chia sẻ thông tin công cộng. Một trong số này được Window thực hiện tự động nếu bạn định rõ mạng công cộng.

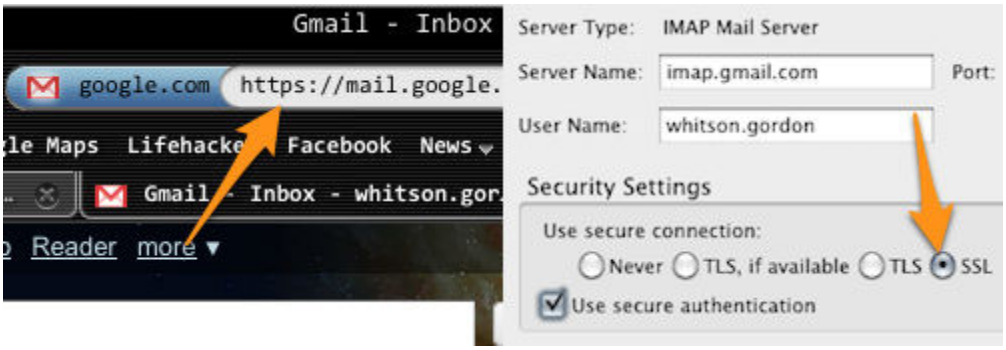
Trong Mac OS X: Tới **System Preferences** -> **Share**, và chắc chắn là các ô đều đã được bỏ chọn

Bạn nên tắt chức năng tìm kiếm mạng ở một nơi cụ thể nào đó. Điều này sẽ ngăn cản những người khác có thể thấy máy bạn trên hệ thống, nghĩa là bạn ít có khả năng bị tấn công hơn. Trong Window (như được đề cập ở trên) có thêm một ô check ở phía dưới thiết lập chia sẻ. Trên OS X, nó chính là "*stealth mode*" ở dưới thiết lập firewalls.



Hiện nay hầu hết OS X đều cài đặt firewall, đây là bước đơn giản bảo vệ chiếc máy tính của bạn khỏi những kẻ truy cập không mong đợi. Bạn cũng có thể sử dụng firewall, nhưng trong trường hợp này hãy thiết lập bảo mật (Trong Window chọn **Control Panel -> System and Security -> Windows Firewall**; và trong Mac tới **System Preferences -> Security -> Firewall**) đảm bảo rằng firewall đã được cài đặt. Bạn cũng có thể chọn ứng dụng cho phép được truy cập bằng cách click vào "*Allow a program or feature*" trong Windows và "*Advance*" trong OS X. Firewall sẽ bảo vệ máy bạn, nhưng đây không phải là ý tưởng hay để đảm bảo chắc chắn hoàn toàn.

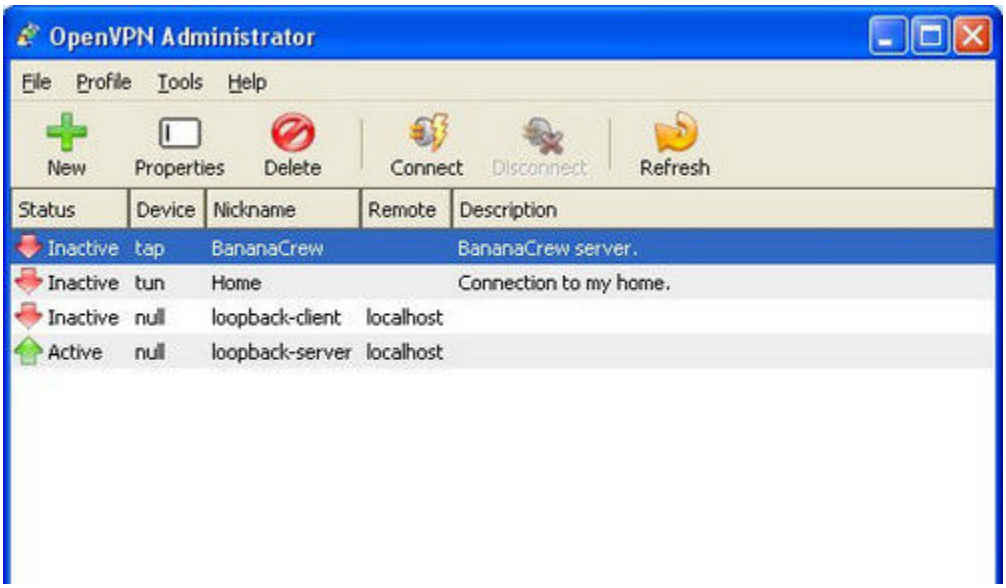
Sử dụng SSL bất cứ khi nào có thể



Một vài trang sẽ tự động đăng nhập, tuy nhiên nên chú ý đến thanh địa chỉ, và đảm bảo có chữ "*s*" trong chữ "*hppts*" luôn xuất hiện khi bạn thay đổi những thông tin nhạy cảm. Chú ý rằng trình duyệt này có thời gian đợi, bạn có thể thực hiện từng bước một. Một số trang khác cũng sẽ thiết lập kết nối HTTP, nếu bạn gõ tên nó. Gmail là một ví dụ, nó sẽ cho phép bạn đăng nhập sử dụng HTTPS và có thể lập Gmail cho dù bạn có muốn sử dùng HTTPS tự động hay không?

Nếu bạn truy cập email từ desktop như Outlook, hay ứng dụng mail, bạn sẽ muốn đảm bảo rằng tài khoản của bạn đã được cài đặt bảo mật. Nếu không những người khác có thể đọc được email của bạn, có được tên sử dụng, mật khẩu hay bất kì thứ gì họ muốn. Bạn sẽ cần bảo đảm hỗ trợ vùng, và đôi khi thiết lập này có thể yêu cầu thêm cài đặt khác. Vì thế hãy kiểm tra ô *"use SSL"* kiểm tra tài khoản email trợ giúp để biết thêm chi tiết. Nếu không hỗ trợ SSL đảm bảo thoát khỏi ứng dụng khi bạn đang ở trong mạng công cộng không an toàn.

Cân nhắc việc sử dụng Mạng riêng ảo

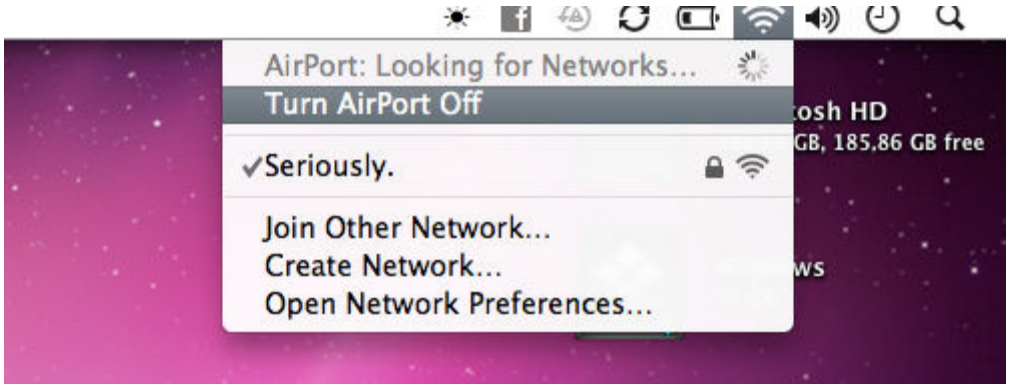


Thật không may mắn, không phải tất cả các trang đều cung cấp bảo mật SSL, công cụ tìm kiếm, và email có thể bị lộ với những người đang thấy hoạt động của bạn. Vì thế nếu bạn sử dụng một trong số những trang này thường xuyên (hoặc thực sự muốn có thêm chức năng bảo vệ), bạn có

thể sử dụng VPN hoặc mạng riêng ảo, nó sẽ cung cấp cho bạn việc bảo mật ở bất cứ một địa điểm công cộng nào.

Giữ an toàn khi sử dụng mạng Wi – Fi công cộng-P2

Tắt mạng khi không sử dụng nữa

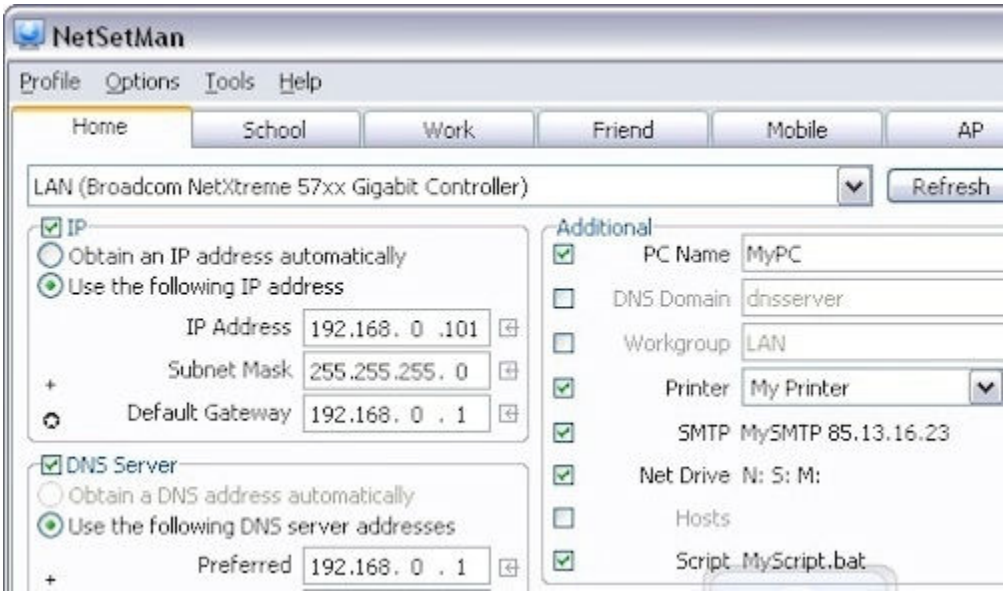


Nếu bạn muốn đảm bảo an toàn cho máy, và bạn đang cần dùng mạng internet, đơn giản hãy tắt kết nối Wi Fi. Điều này khá dễ dàng trong cả Windows và Mac. Trong Mac, *Click* vào biểu tượng Wi Fi trên thanh công cụ chọn *Turn off AirPort*. Trong Window, bạn chỉ cần click chuột phải vào biểu tượng Wi Fi ở trên thanh taskbar để tắt. Đây không hoàn toàn là cách tốt nhất khi đang cần kết nối internet, nhưng khi bạn không sử dụng nữa thì cách tốt nhất là nên tắt nó. Càng kết nối lâu, bạn càng có khả năng bị xâm nhập nhiều hơn.

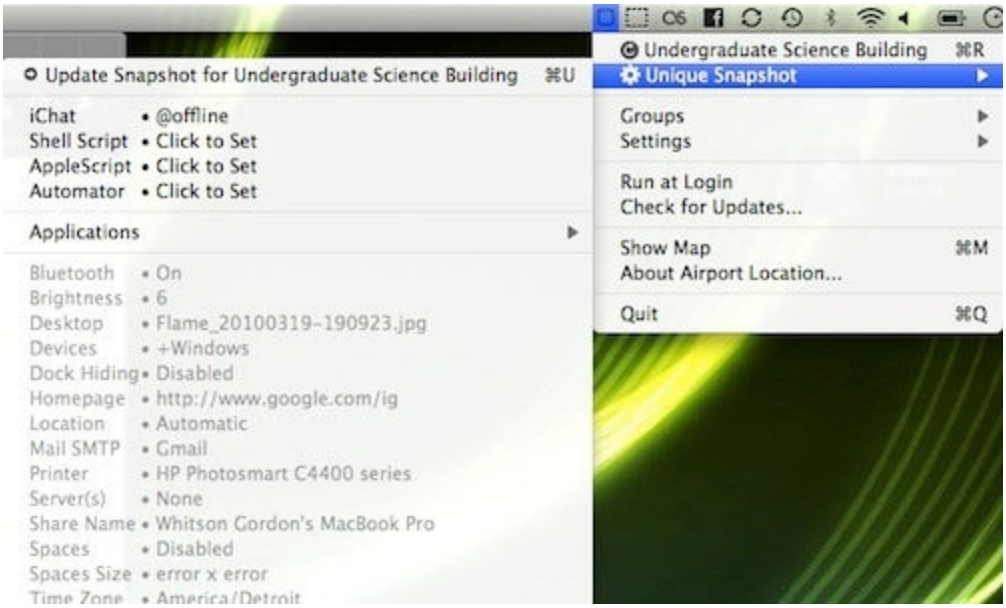
Làm thế nào để có thể cài đặt tự động bảo mật Wi Fi

Bạn không muốn phải điều chỉnh tất cả thiết lập cho máy mỗi khi đi lại giữa những quán cafe và nhà mình. Thật may mắn, có một số cách giúp quá trình cài đặt tự động, vì thế bạn có thể được bảo vệ tăng cường khi kết nối Wi Fi công cộng

Trên Windows

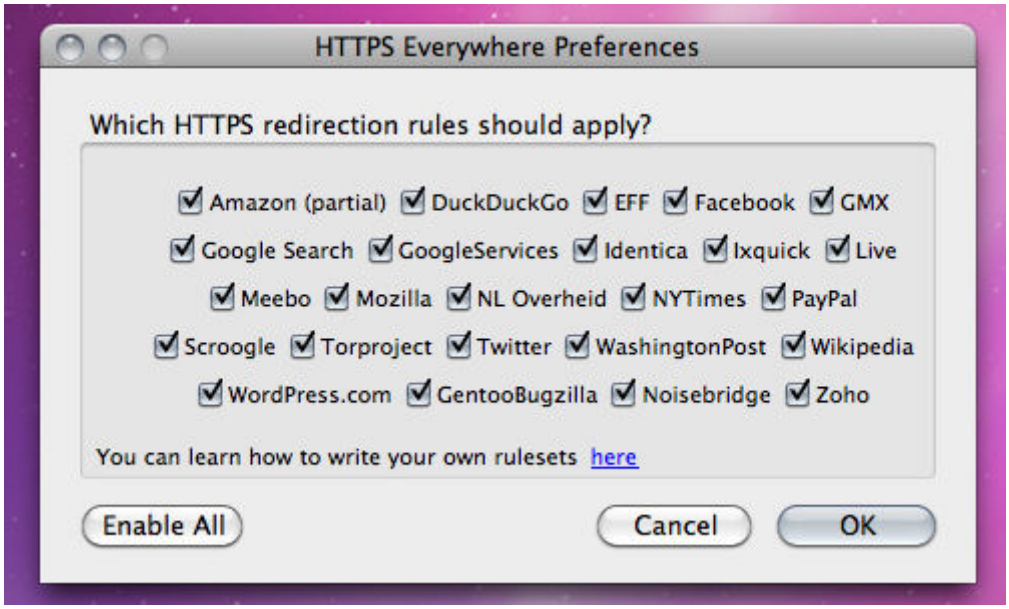


Khi lần đầu tiên kết nối với bất kì mạng nào trên Windows, bạn sẽ được hỏi xem đó là kết nối mạng tại nhà hay công cộng. Với mỗi lựa chọn bạn sẽ có một danh sách cài đặt, thông thường thiết lập công cộng sẽ cho bạn bảo mật tốt nhất. Bạn có thể thực hiện chi tiết bằng cách chọn: **Control Panel** rồi tới **Network and Sharing Center** -> **Advanced Sharing Settings**. Từ đó bạn có thể thiết lập mạng, chia sẻ thông tin thêm lựa chọn, bật hay tắt những file khách nhau



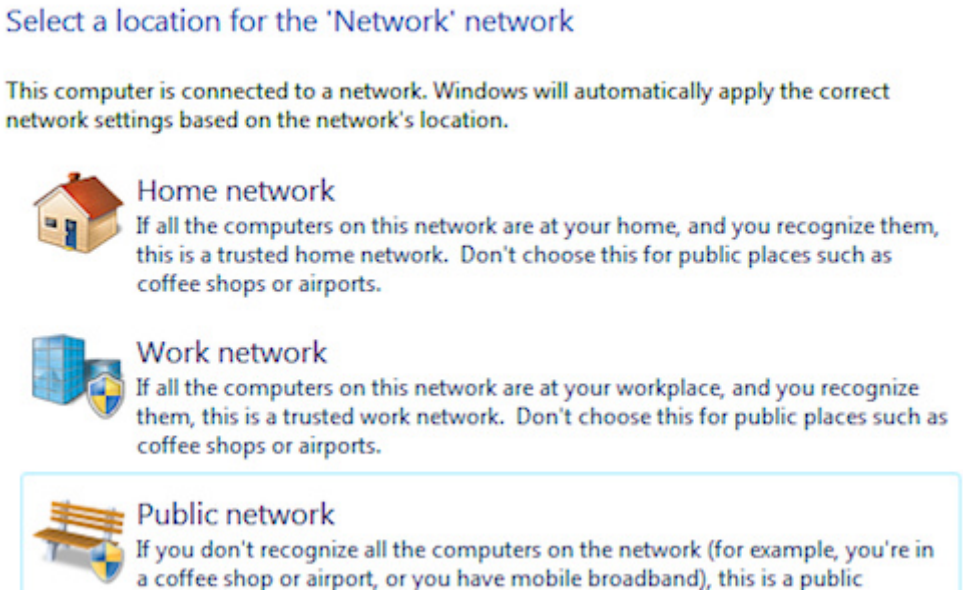
Nếu bạn muốn có thêm kiểm soát, chương trình **MetSetMan** được đề cập ở trên có thể giúp bạn xử lí network profile cho những mạng khác nhau; bạn chọn địa chỉ IP, DNS server mỗi khi kết nối mạng.

Trong OS X



Trong OS X bạn không có nhiều lựa chọn cho việc thiết lập tự động, tuy nhiên **Airport Location** (đã được đề cập trước đây) sẽ giúp làm mọi thứ bạn muốn thậm chí hơn cả thế. Bạn có thể bật firewall, tắt SMTP mail, kết nối với VPN, và nhiều hơn thế. Tất cả phụ thuộc chính vào mạng bạn kết nối. Bạn cũng có thể thay đổi hình nền desktop cho mỗi mạng cài đặt cũng như chạy **Applescripts** cho những chức năng không có trong ứng dụng.

Trên trình duyệt của bạn



HTTPS được đề cập đến ở trên cùng với sự mở rộng của Firefox tự động chọn HTTPS cho mỗi nhóm web sites phổ biến bao gồm: *New York Times, Twitter, Facebook, Google Search*, và một số trang khác, đảm bảo bảo mật kết nối HTTPS tới bất kì trang web nào mỗi lần bạn truy cập

Xem xét thiết lập bảo mật an toàn đầu tiên

Bạn cũng có thể thêm nhiều profile có thể tự động cài đặt bảo vệ từng bước. Tốt nhất là thiết lập bảo vệ cho từng hệ thống một. Vì thế, việc chia sẻ file sẽ bị tắt, firewall của bạn sẽ ở trong trạng thái an toàn nhất, vì thế khi bạn trở về với mạng ở nhà bạn có thể có thể thiết lập **Airport Location or NetSetMan**

Đây dù sao đi nữa đây không phải là những bước hoàn hảo nhất nên làm mỗi khi kết nối mạng Wi Fi công cộng, nhưng là những bước bạn nên chú ý để đảm bảo an toàn cho những thông tin của chính mình.