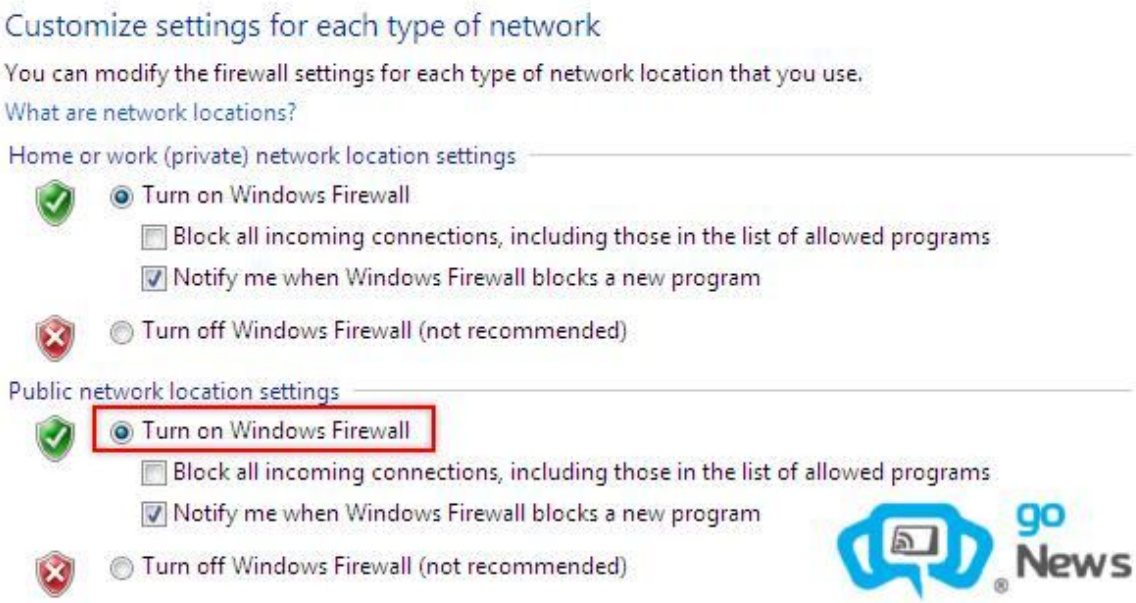
Bảo mật dữ liệu khi dùng Wi-Fi công cộng

Kết nối Wi-Fi nơi công cộng thật tiện lợi nhưng cũng tiềm ẩn những nguy cơ khôn lường. Mách bạn một số biện pháp bảo mật dữ liệu khi dùng Wi-Fi công cộng.

1. Bật tường lửa

Bạn có thể sử dụng tường lửa sẵn của Windows, hoặc cài đặt phần mềm tường lửa của hãng thứ ba, song nhớ bật tường lửa trước khi truy cập mạng Wi-Fi công cộng.

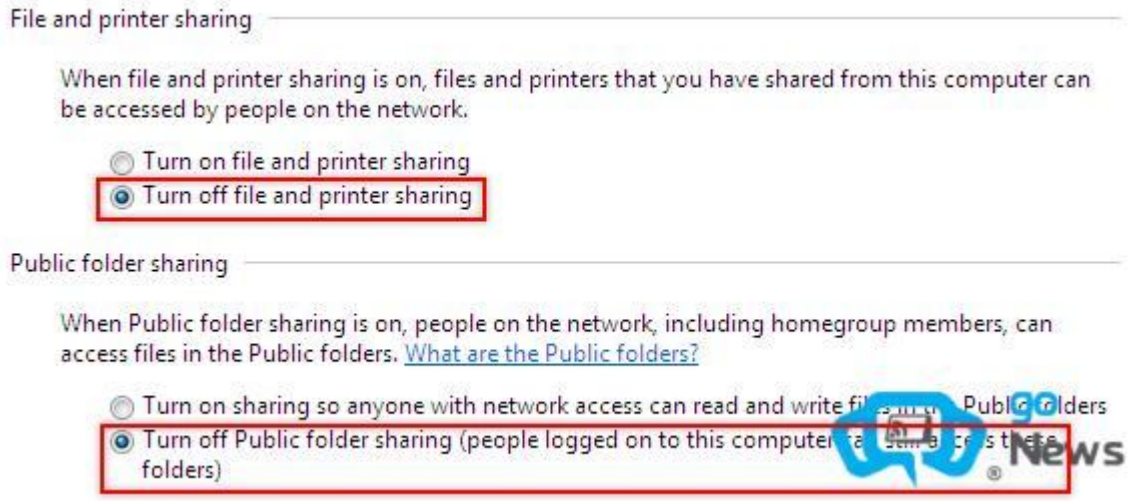
Để bật tường lửa trong Windows 7, bạn vào menu *Start* > *Control Panel* > *Windows Firewall* (nếu không thấy xuất hiện mục *Windows Firewall* trong *Control Panel*, bạn chọn *Large icons* tại mục *View by*). Tiếp đến, bạn nhấn *Turn Windows Firewall on or off* từ cột bên trái màn hình, đánh dấu trước tùy chọn *Turn on Windows Firewall* bên dưới *mục Public network location settings*. Xong, nhấn *OK*.



2. Tắt tất cả các tài nguyên chia sẻ

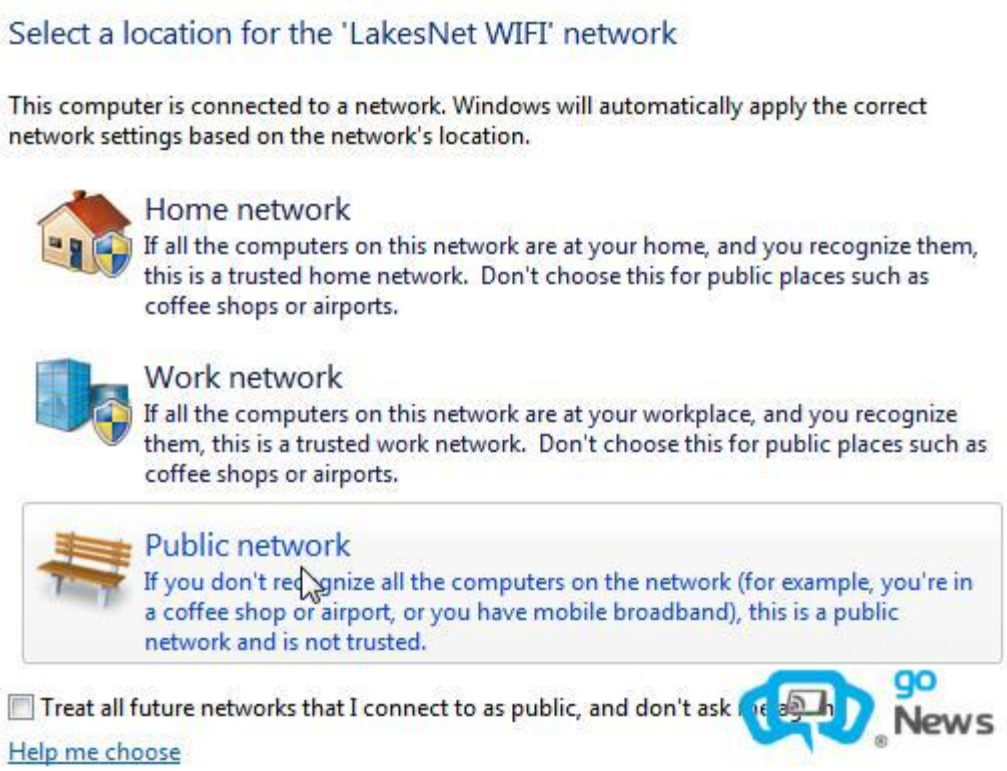
Nếu không tắt các tài nguyên chia sẻ, những người cùng mạng có thể "đánh cắp" dữ liệu trên laptop của bạn rất dễ dàng. Trong Windows 7, bạn nhấn biểu tượng kết nối mạng trên khay hệ thống, chọn *Open Network and Sharing Center*, sau đó nhấn *Change advanced sharing settings* tại cột bên trái màn hình, đánh dấu trước tùy chọn *Turn off file and printer sharing* và *Turn off Public folder sharing,* rồi nhấn *Save changes* để lưu lại.

[/URL]



3. Chọn kết nối Wi-Fi công cộng

Ngay sau khi kết nối thành công đến một mạng Wi-Fi công cộng, bạn chọn *Public network* từ hộp thoại vừa xuất hiện. Với tùy chọn này, các chức năng chia sẻ (gồm *Network discovery, File and printer sharing, Public folder sharing*) mặc định sẽ tắt, nhằm đảm bảo an toàn dữ liệu cho bạn trong suốt quá trình sử dụng mạng Wi-Fi công cộng.



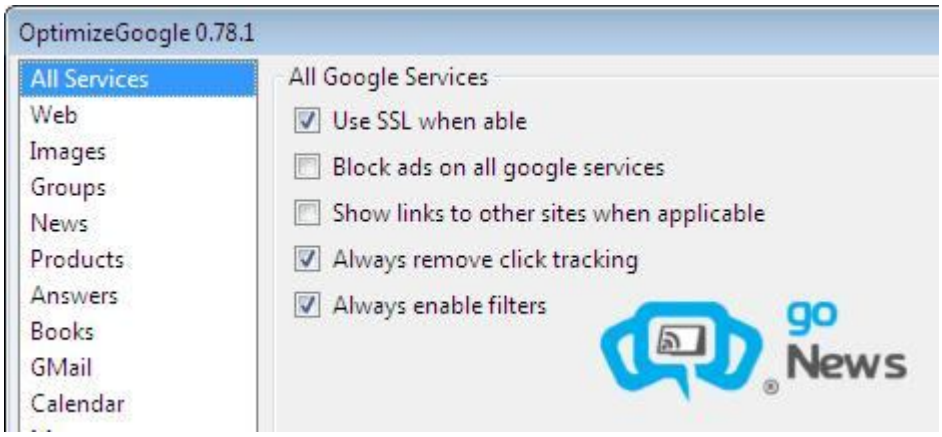
4. Sử dụng giao thức HTTPS hoặc SSL thay cho giao thức HTTP thông thường

Nếu sử dụng giao thức HTTP thông thường, người cùng mạng có thể dễ dàng "coi cọp" (sniffer) thông tin của bạn, bao gồm cả mật khẩu đăng nhập các webmail, tài khoản trực tuyến,… Do vậy, bạn nên bật giao thức HTTPS hoặc SSL khi sử dụng các dịch vụ yêu cầu đăng nhập bằng tài khoản cá nhân.

Để bật giao thức HTTPS trong Gmail, bạn đăng nhập hộp thư cá nhân theo cách thông thường, tiếp đó nhấp vào liên kết *Settings* > *General*, đánh dấu trước tùy chọn *Always use https tại mục Browser connection*. Xong, nhấn *Save Changes*.

Từ giờ, mỗi khi truy cập vào Gmail hay các dịch vụ khác của Goole bằng tài khoản đã thiết lập giao thức HTTPS, bạn sẽ thấy phía trên thanh Address xuất hiện dòng địa chỉ bắt đầu bằng *https://* thay cho *http://*.

Để bật giao thức SSL cho các dịch vụ của Google, bạn tải về và cài đặt add-on *OptimizeGoogle* dành cho Firefox tại [URL="https://addons.mozilla.org/firefox/addon/52498/"]đây (dung lượng 329 KB, tương thích với Firefox 3.7 trở về trước). Sau khi cài đặt, bạn khởi động lại Firefox, vào menu *Tools* > *Add-ons* > *OptimizeGoogle* > *Options* > *All Services*, đánh dấu trước tùy chọn *Use SSL when able,* rồi nhấn *OK*.



5. Tắt kết nối Wi-Fi khi không sử dụng

Khi không sử dụng đến kết nối Wi-Fi, bạn nên tắt đi nhằm đảm bảo không ai có thể truy xuất dữ liệu trái phép trên máy của mình được. Rất đơn giản, bạn chỉ việc nhấn biểu

tượng kết nối mạng trên khay hệ thống, nhấn chuột phải lên kết nối Wi-Fi đang dùng và chọn *Disconnect.*

6. Thường xuyên cập nhật bản vá lỗi Windows và dữ liệu mới nhất cho trình anti-virus

Các bản vá lỗi Windows giúp bạn "bịt kín" những lỗ hổng mà hacker lợi dụng để xâm nhập trái phép vào máy tính của bạn thông qua kết nối Wi-Fi. Bên cạnh đó, các trình anti-virus cũng đóng vai trò quan trọng trong việc phát hiện kịp thời những nguy cơ tiềm ẩn trong quá trình kết nối Wi-Fi.

Do đó, bạn nên thường xuyên cập nhật các bản vá lỗi và cơ sở dữ liệu mới nhất cho trình anti-virus.

Trên đây là một số biện pháp nhằm đảm bảo an toàn khi bạn kết nối đến một mạng Wi-Fi công cộng, tuy nhiên không có gì là tuyệt đối. Hacker vẫn có cách để xâm nhập trái phép máy tính của bạn dù bạn đã áp dụng tất cả biện pháp phòng vệ. Do đó, tốt nhất là bạn nên hạn chế sử dụng Wi-Fi công cộng, nếu sử dụng thì nên hạn chế truy cập những thông tin nhạy cảm như đăng nhập tài khoản ngân hàng, thư điện tử, giao dịch trực tuyến,...