

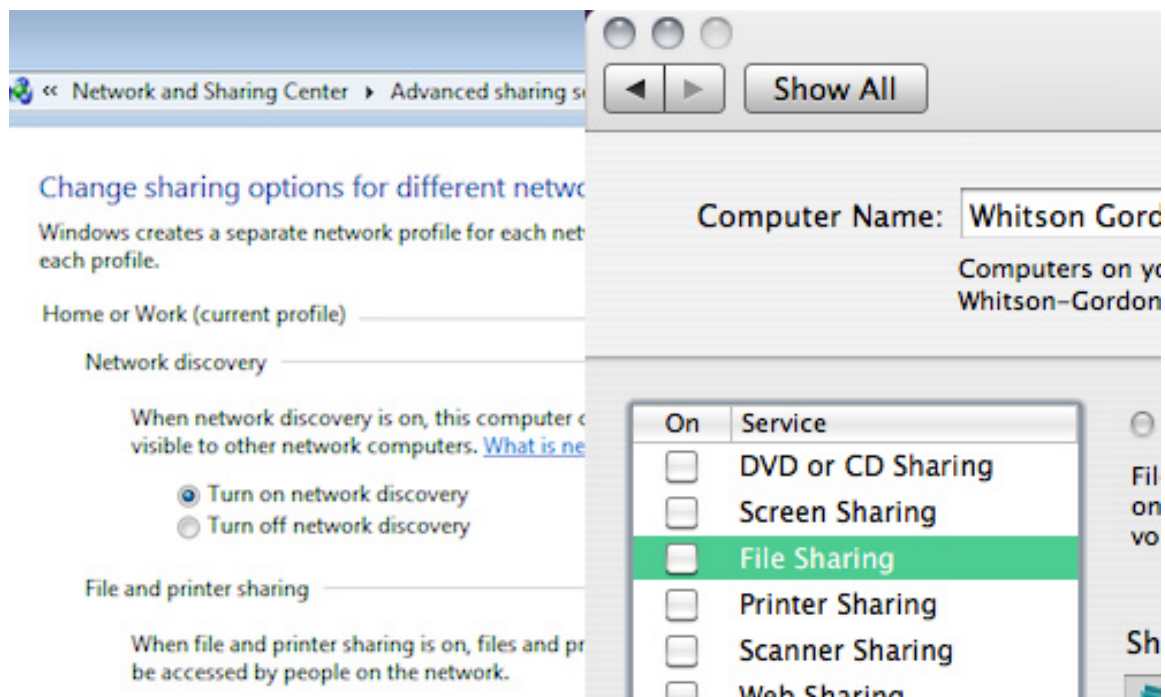
How to Stay Safe on Public Wi-Fi Networks

Starbucks is now offering free Wi-Fi to all customers at every location. Whether you're clicking connect on Starbucks' Wi-Fi or some other unsecured, public Wi-Fi network, here's how to stay safe and secure while surfing a public hotspot.



Just because most wireless routers have a firewall to protect you from the internet doesn't mean you're protected from others connected to the same network. Lots of wireless hotspots these days are completely unencrypted, usually so they're easier to connect to (baristas don't need to be giving out the internet password to everyone that walks in). However, this leaves you unprotected against malicious users in the same coffee shop, so there are a few settings you should always make sure to tweak when you're connected to a public network. We're going to show you which settings are the most important ones, as well as how to automatically change your settings to the appropriate level of security every time you connect to a public network.

The Settings



1. Turn Off Sharing

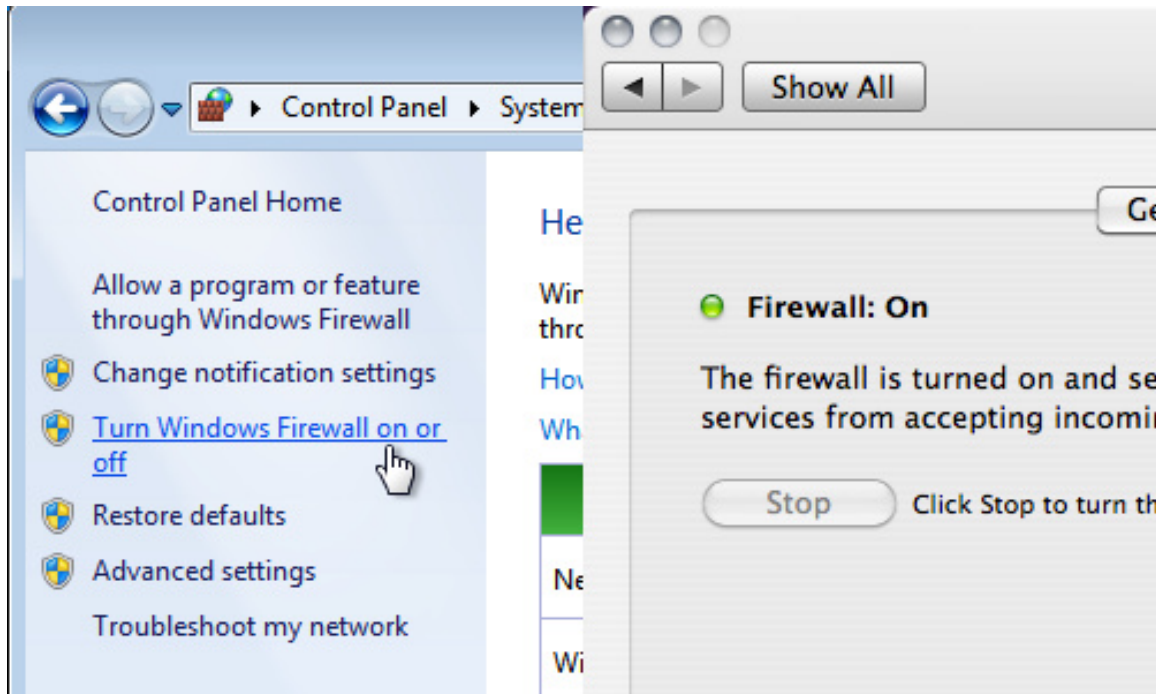
When you're at home, you may share files, printers, or even allow remote login from other computers on your network. When you're on a public network, you'll want to turn these things off, as anyone can access them—they don't even need to be a hacker, and depending on your setup, some of that stuff probably isn't even password protected. Here's how to turn off sharing:

In Windows: Open your Control Panel, then browse to Network and Internet -> Network and Sharing Center, then click Choose Homegroup and Sharing Options -> Change Advanced Sharing Settings. Once here, you should definitely turn off file and printer sharing, and you may as well turn off network discovery and Public folder sharing. Some of this is done automatically by Windows if you specify the network as public (more on this later).

In Mac OS X: Go to System Preferences -> Sharing and make sure all the boxes are unchecked.

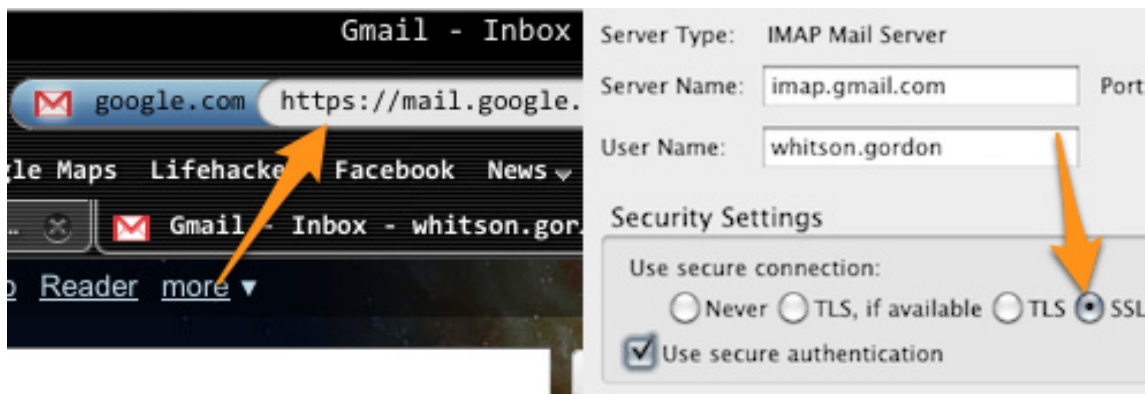
You'll also want to turn off network discovery, which will be in the same place. This will prevent others from even seeing your machine on the network, meaning you're less likely to be targeted. On Windows (as I mentioned), it's just another check box under advanced sharing settings. On OS X, it will be called "stealth mode" and be under your firewall's advanced settings (see below).

2. Enable Your Firewall



Most operating systems come with at least a basic firewall nowadays, and it's a simple step to keeping unwanted local users from poking at your computer. You may already be using a firewall, but just in case, go into your security settings (in Windows under Control Panel -> System and Security -> Windows Firewall; and on Mac under System Preferences -> Security -> Firewall) and make sure your firewall is turned on. You can also edit which applications are allowed access by clicking on "allow a program or feature" in Windows and "advanced" in OS X. Your firewall is not an end-all, be-all protector, but it's always a good idea to make sure it's turned on.

3. Use SSL Whenever Possible

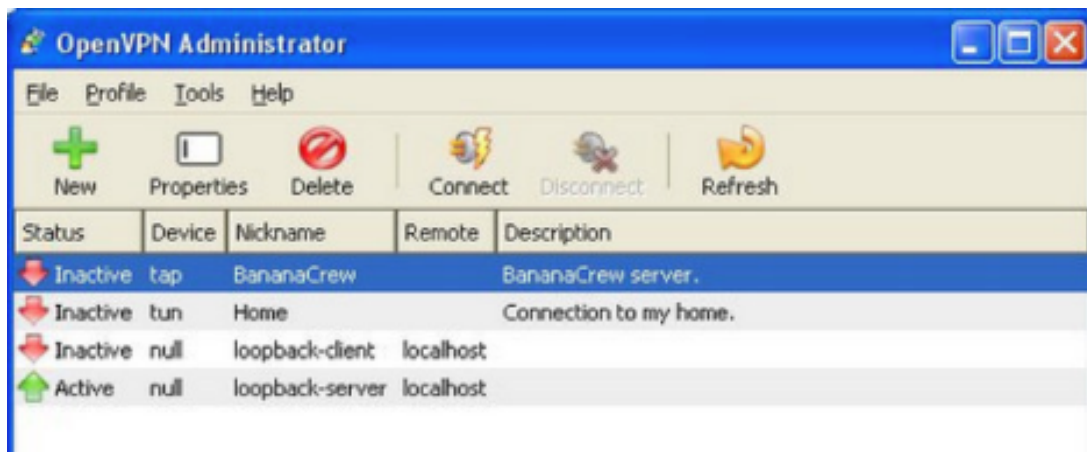


Regular web site connections over HTTP exchange lots of plain text over the wireless network you're connected to, and someone with the right skills and bad intent can sniff out that traffic. It's not that big of a deal when the text is some search terms you entered at Lifehacker, but it is a big deal when it's the password to your email account. Using HTTPS (for visiting web sites) or enabling SSL (when using applications that access the internet, such as a mail client) encrypts the data passed back and forth between your computer and that web server and keep it away from prying eyes.

Some sites will do it automatically, but keep an eye on the address bar and make sure the "s" in "https" is always there when you're exchanging sensitive information. If it disappears, you should log out immediately. Note that if the sensitive browsing can wait, you might as well just do it at home—no reason in risking more than you have to. Other sites will default to HTTP connections, but support HTTPS if you manually type it in. Gmail, for example, will allow you to log in using HTTPS, and you can specify in your Gmail Settings whether you want it to use HTTPS automatically in the future. (Go to Settings, find the Browser connection setting, and set to Always use https.)

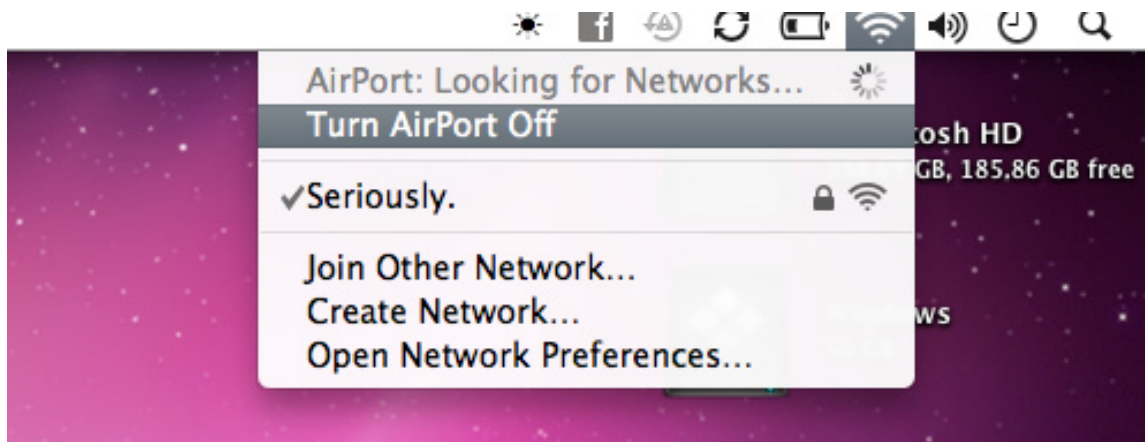
If you access your email from a desktop client such as Outlook or Mail.app, You'll want to make sure that your accounts are SSL encrypted in their settings. If not, people could not only theoretically read your emails, but also get your usernames, passwords, or anything else they wanted. You'll need to make sure your domain supports it, and sometimes the setup might require different settings or ports—it's not just a matter of checking the "use SSL" box—so check your email account's help page for more details. If it doesn't support SSL, make sure you quit the application when you're on an insecure public network..

4. Consider Using a Virtual Private Network



Unfortunately, not all sites offer SSL encryption. Other search engines and email providers may still be vulnerable to people watching your activity, so if you use one of these sites frequently (or really just want the extra protection), you may want to try using a VPN, or virtual private network. These services let you route all your activity through a separate secure, private network, thus giving you the security of a private network even though you're on a public one. We've detailed how to set up a VPN with Hamachi, though there are a number of great services—check out our [Hive Five](#) for best VPN tools for more ideas. If all that's a bit too complicated, you can always go with previously mentioned Hotspot Shield, which is a fairly popular app that will run in the background and set up the VPN automatically.

5. Turn It Off When You're Not Using It



If you want to guarantee your security and you're not actively using the internet, simply turn off your Wi-Fi. This is extremely easy in both Mac and Windows. On a Mac, just click the Wi-Fi icon in the menu bar and select the turn off AirPort option. On Windows, you can just right-click on the wireless icon in the taskbar to turn it off. Again, this isn't all that useful if you need the internet, but when you're not actively using it, it's not a bad idea to just turn it off for the time being. The longer you stay connected, the longer people have to notice you're there and start snooping around.

How to Automate Your Public Wi-Fi Security Settings

You don't want to have to manually adjust all of these settings every single time you go back and forth between the coffee shop and your secure home network. Luckily, there are a few ways to automate the process so you automatically get extra protection when connected to a public Wi-Fi network.

On Windows

Select a location for the 'Network' network

This computer is connected to a network. Windows will automatically apply the correct network settings based on the network's location.



Home network

If all the computers on this network are at your home, and you recognize them, this is a trusted home network. Don't choose this for public places such as coffee shops or airports.



Work network

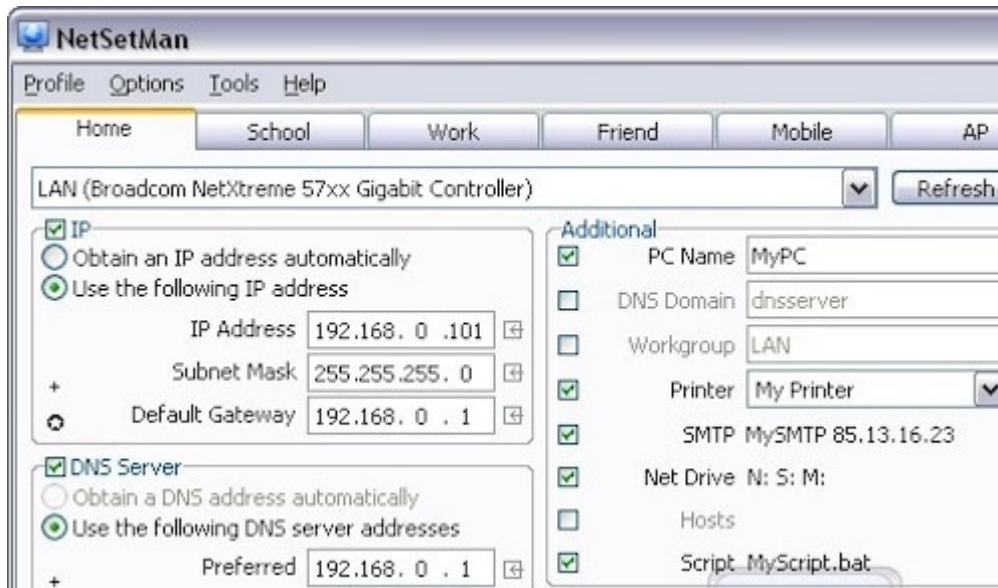
If all the computers on this network are at your workplace, and you recognize them, this is a trusted work network. Don't choose this for public places such as coffee shops or airports.



Public network

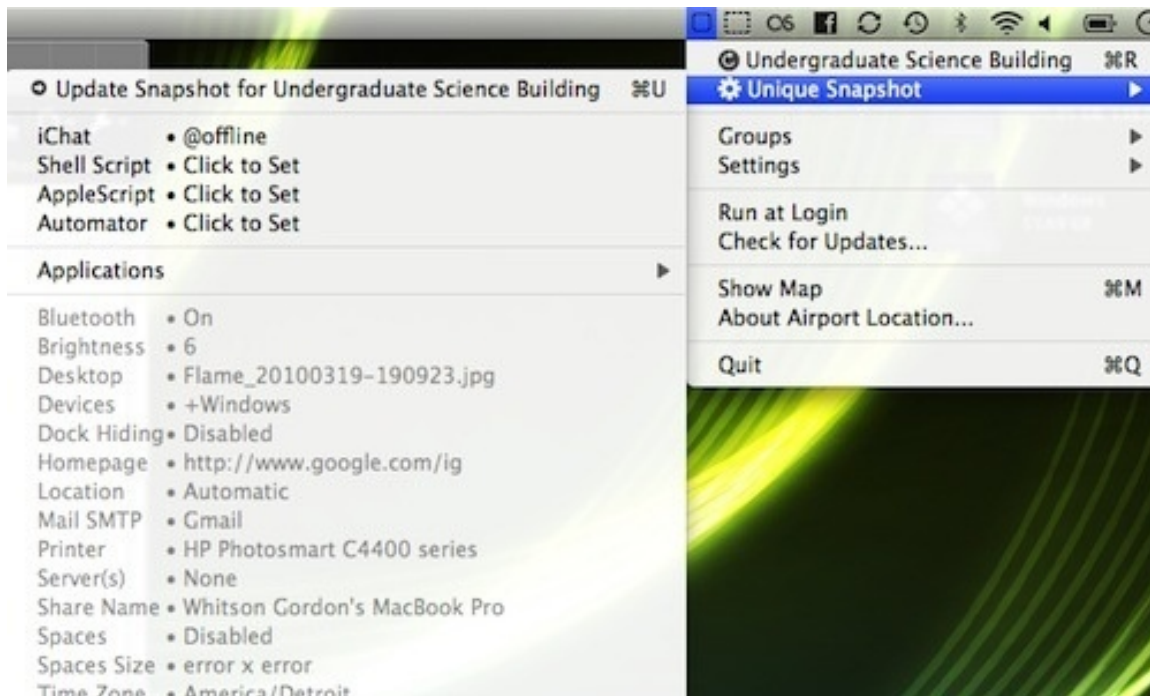
If you don't recognize all the computers on the network (for example, you're in a coffee shop or airport, or you have mobile broadband), this is a public

When you first connect to any given network on Windows, you'll be asked whether you're connecting to a network at your home, work, or if it's public. Each of these choices will flip the switch on a preset list of settings. The public setting, naturally, will give you the most security. You can customize what each of the presets entails by opening your Control Panel and navigating to Network and Sharing Center -> Advanced Sharing Settings. From there, you can turn network discovery, file sharing, public folder sharing, media streaming, and other options on or off for the different profiles.



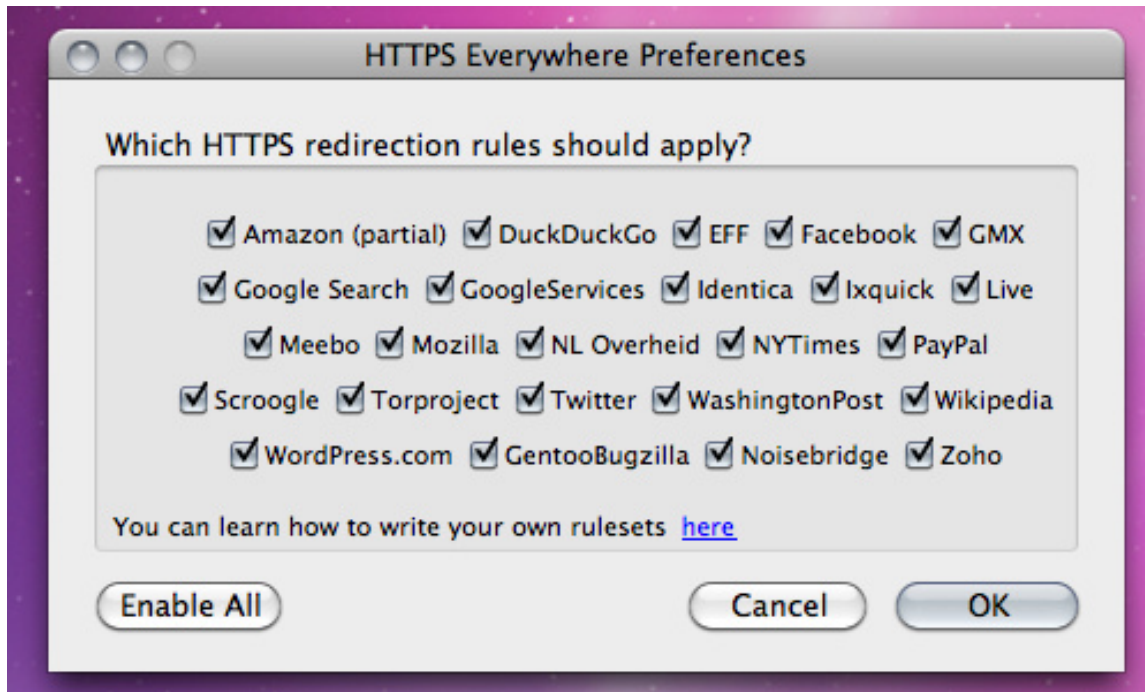
That's a good start, but what if you want a bit more control? Previously mentioned NetSetMan is a great program to customize your network profiles for different networks; you choose your IP address, DNS server, or even run scripts (opening the window for pretty much any action) every time you connect to one of your preset networks.

On OS X



On OS X, you don't have a lot of options for automating your network preferences, but previously mentioned Airport Location will do everything you could possibly want and more. With it, you can turn on your firewall, turn off SMTP mail, connect to a VPN, and a whole lot more, all depending on the network you've connected to. Heck, you can even change your desktop background for each given network, as well as run Applescripts for those functions that just aren't built in to the app.

In Your Browser



The previously mentioned HTTPS Everywhere Firefox extension automatically chooses the secure HTTPS option for a bunch of popular web sites, including the New York Times, Twitter, Facebook, Google Search, and others, ensuring secure HTTPS connections to any supported web site, every time you visit. You can even add your own to their XML config file. Note that as a Firefox extension, this works on Windows, Mac, and Linux.

Consider a Safety-First Approach

If you're a real road warrior, you may find yourself adding so many profiles that automating your safe settings at every step along the way may seem like a lot of work. While most chains like Starbucks or McDonald's should have the same names for each of their Wi-Fi networks (and thus your profiles will carry over), a better approach may be to make your more secure settings the default for your system, and create just one profile for your home network. Thus, by default, file sharing would be turned off, your firewall would be at its most secure state, and so on—then, when you

return home to your protected network, you can have Airport Location or NetSetMan turn your less secure settings on.

This isn't all-encompassing by any means, but should give you a good quick checklist of things you should do every time you connect to a public network. There are certainly a number of other things you could do (such as setting up a SOCKS proxy over SSH), but these steps will take you a long way on the road to security when you're browsing on those public hotspots. Of course, some of you already have your own public browsing routines, so be sure to share your safe networking tips in the comments.

Wally, I got this from the MUG here in Wisconsin. You may want to share it with the group. *Ed Ogurek*