# 9 Tips to Stay Safe on Public Wi-Fi

By Dann Berg, LAPTOP Contributor | Feb 1, 2013 12:46 PM EDT

Your bank calls you to verify your recent $750 bill at an out-of-state Taco Bell, but you haven't left town in weeks. You quickly contest the charge and request a new credit card, but when you check your wallet the compromised card is still there. You try to think of shady ATMs or recent cashiers, but nothing comes to mind. Nothing, except the online purchase you made while browsing the Internet at your local coffee shop.

The number of free public WiFi hotspots is growing, but not every hotspot can provide the protection of a private home network. Your notebook, Tablet or smartphone's default settings and firewalls may not be enough to keep you safe from prying eyes while on the go. If you want to keep your information and files secure, read these essential tips for protecting yourself when you're away from home.

## 1. Turn Off Sharing

You may share your music library, printers or files, or even allow remote login from other computers on your Wi-Fi network in the privacy of your own home. Unless you disable these settings before connecting to a public Wi-Fi network, anyone else in the vicinity may be able to hack into your PC.

If you're using a Windows PC, you'll want to start by opening the advanced sharing settings of the Homegroup section of the Network and Internet settings in the Control Panel. From here, you'll be able to toggle file and printer sharing as well as network discovery, which will make your computer visible to anyone connected to the same network. For Mac, just go to System Preferences, then Sharing, and make sure none of the options are checked.

## 2. Get a VPN

The most secure way to browse on a public network is to use a virtual private network. A VPN routes your traffic through a secure network even on public Wi-Fi, giving you all the perks of your private network while still having the freedom of public Wi-Fi.

While free VPN services exist, a paid VPN service guarantees the connection's integrity. If you regularly connect to unknown networks, setting up a VPN is smart to protect your personal information.

One VPN provider is Private Internet Access, which costs $6.95 monthly and allows for unlimited bandwidth and multiple exit points, which will let you choose which country your network traffic is routed through.

## 3. Avoid Automatically Connecting to Wi-Fi Hotspots

Your smartphone or tablet may be set to automatically connect to any available Wi-Fi hotspot, a setting that can seriously endanger your privacy. Not only will this allow your device to connect to public networks without your express permission, you may also be automatically connecting to malicious networks set up specifically to steal your information.

Most modern smartphones have this option disabled by default, but this isn't always the case, and it's a setting you should always double-check. First, open the Wi-Fi section of your phone's settings app. If you don't see an option to disable auto-connecting, you're already safe. Otherwise, turn this setting off.

## 4. Use HTTPS


Regular websites transfer content in plain text, making it an easy target for anyone who has hacked into your network connection. Many websites use HTTPS to encrypt the transfer data, but you shouldn't rely on the website or Web service to keep you protected.

You can create this encrypted connection with the browser extension HTTPS Everywhere. With this plugin enabled, almost all website connections are secured with HTTPS, ensuring that any data transfer is safe from prying eyes.

## 5. Use Two-Factor Authentication

Two-factor authentication means you need two pieces of information to log into an account: One is something you know and the other is something you have. Most often this takes the form of a password and a code sent to your cellphone.

Many popular websites and services support two-factor authentication. This means that even if someone is able to get your password due to a hole in a public Wi-Fi network, they won't be able to log into your account.

To enable this feature for Gmail, log into your account and open the settings page. Navigate to the Accounts And Import tab and click Other Google Account Settings. The second section will be two-step verification, and you can click Settings to start.

First, enter your phone number and choose whether you'd like a text message or a phone call. Next, Google will send a six-digit code to your phone. Enter this when prompted. Now, whenever you log into Google from a new computer, you'll be asked to verify your identity by entering both pieces of info.

The login process will now take a few extra seconds when you use a different device, but you can rest peacefully knowing that your account is safe and secure.

## 6. Confirm the Network Name

Sometimes hackers will set up a fake Wi-Fi network to attract unwitting public Wi-Fi users. The Starbucks public Wi-Fi network might not be named “Free Starbucks Wi-Fi.” Connecting to a fake network could put your device into the hands of a malicious ne’er-do-well.

If you’re not sure if you’re connecting to the official network, ask. If you’re in a café or coffee shop, employees will know the name of the official network and help you get connected. If there’s no one around to ask, you may want to move to a different location where you can be sure that the Wi-Fi network isn’t fake.

## 7. Protect Your Passwords

Using unique passwords for different accounts can help if one of your accounts is compromised. Keeping track of multiple secure passwords can be tricky, so using a password manager such as KeePass or LastPass can help keep you safe and secure.

Both KeePass and LastPass are free, but they store your information in different ways. KeePass keeps an encrypted database file on your computer, while LastPass stores your credentials in the cloud. There are pros and cons to each approach, but both services are completely secure.

## 8. Turn on Your Firewall

Most OS’s include a built-in firewall, which monitors incoming and outgoing connections. A firewall won’t provide complete protection, but it’s a setting that should always be enabled.

On a Windows notebook, locate your firewall settings in the Control Panel under System And Security. Click on Windows Firewall, then click Turn Windows Firewall On or Off. Enter your administrator password, then verify that the Windows Firewall is on.

These settings are in System Preferences, then Security & Privacy on a Mac. Navigate to the Firewall tab and click Turn On Firewall. If these settings are grayed out, click the padlock icon in the lower left, enter your password, then follow these steps again.

## 9. Run Anti-Virus Software

Always running up-to-date anti-virus software can help provide the first alert if your system has been compromised while connected to an unsecured network. An alert will be displayed if any known viruses are loaded onto your PC or if there's any suspicious behavior, such as modifications to registry files.

While running anti-virus software might not catch all unauthorized activity, it's a great way to protect against most attacks.