

- [Cell Phones](#)
- [Computers](#)
- [Video Games](#)
- [Reviews](#)
- [Downloads](#)

[Computers](#), [Advice](#), [Windows Software](#), [Mac Software](#)

[Just How Risky Are Public Wi-Fi Hotspots?](#)

by [Terrence O'Brien](#) — Nov 2nd 2009 at 6:16AM



Ever wonder how safe all your personal information is when it's beamed through the air over [Wi-Fi](#)? If you haven't, then chances are, you haven't taken the right precautions to keep that information safe, either. In clear, easy-to-understand language, the ['Today Show'](#) recently examined the security of Wi-Fi networks. While the video above is a little on the fear-mongering side, it does make some good points about the vulnerability of wireless traffic, in particular, those public hot-spots at your local coffee shop, park, or airport.

11
diggs

[digg it](#)

Here's what you need to know: Public hot-spots -- most of which are open and don't require a password -- are, by nature, insecure. Sure, they may be easy and convenient to hop on from your computer, but that very openness is also what allows anyone, including hackers, to just walk in and sign on. In other words, when you're signed on to a public Wi-Fi hotspot (or at an unsecured network at your or someone's private home), it's entirely possible for someone to come along and snatch your data, literally out of the air.

Luckily, there are some essential precautions you can take to protect yourself when you're in a public hotspot. First and foremost, get a good [firewall](#) program -- not the one built into Windows or Macs, though. Most [security suites from Norton, McAfee, and others](#) come with one, and you can download free ones from the likes of [Zone Alarm and Comodo](#). These apps are designed to prevent hackers from gaining access to the data on your PC, and will block and alert you to any attempts to wirelessly access your computer.

However, these programs do not protect what you send out over the air (like passwords) when trying to get access to your bank account online or credit card information when making online purchases. The biggest piece of advice we can give is not to make any transactions involving a credit card at a public Wi-Fi spot, and don't log into any service that doesn't use [https](#) to secure your data traffic. You can easily identify such sites by looking at

the address bar in your browser, since they'll begin with "https" instead of just "http," and they encrypt all information being passed back and forth. Even most e-mail services such as [Gmail](#) offer this as an option -- just check the settings panel.

Do you use your laptop at coffee shops?

Yes. No. I'm not sure.

At home, securing your info is easier, but requires more steps. First, make sure you have a good [wireless router](#) that has a built-in [firewall](#) (most new ones including those handed out by ISPs do) and supports the latest security protocols -- [WPA2](#). There are three methods of protecting your data on Wi-Fi, WEP (easily hacked, but still better than nothing), [WPA](#) (better), and WPA2 (best). Most modern routers support WPA2 and you should use it, with the highest level of encryption possible (256-bit).

If your router only supports WEP -- as many older ones do -- then get a new router, seriously. An additional measure is to turn off the SSID (or network name) broadcast in your router's settings. This will prevent other computers and devices from seeing your network automatically, though dedicated hackers will still be able to locate it. Also, change the default password on your router to something long and complex -- avoid dictionary words and mix letters, numbers and special characters to prevent anyone from easily guessing the password (for more tips on choosing a secure password, see '[5 Tips on Keeping Your PC Safe](#)').

The 'Today Show' makes a big deal of [wardriving](#), an old trend in which hackers drive around neighborhoods looking for open Wi-Fi networks to steal data from. But the practice is far less prevalent than the show's reporters would have you believe. And if you follow our suggestions, such data thieves will likely pass your network by in favor of a less secure one that will make a much easier target.

Safe surfing!

[Next >> 'How to Prevent Spam on Your PC and Cell Phone'](#)

Related Links:

- [5 Essential Tips on to Keep Your PC Safe](#)
- [12 Ways Technology Threatens Your Privacy \(and How to Protect Yourself\)](#)

switched on facebook

Tags: [hackers](#), [hacking](#), [security](#), [top](#), [wi-fi](#), [wifi](#), [wifisecurity](#)

- [Permalink](#)
- [Email this](#)
- [Share](#)
- [Comments \(29\)](#)

Related Articles

from [switched](#)