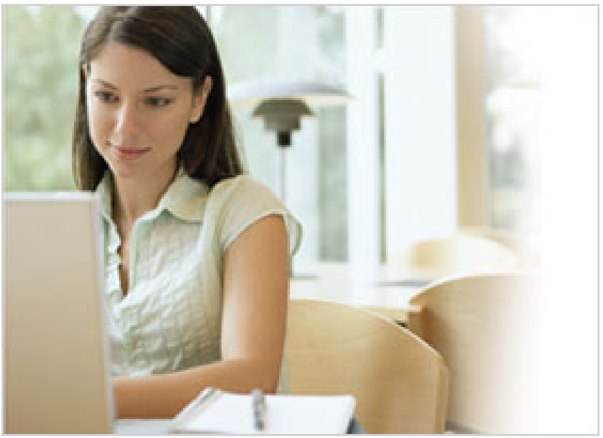
McAfee for Consumer McAfee SECURE TESTED 17-OCT intel Security

McAfee Security Advice Center

Fall 2014 — Security News and Advice

Also in this issue

- When Popular Searches Produce Risky Results
- Simple Tips That Will Keep Your Smartphone Data Safe
- Introducing Intel Security



The proliferation of mobile devices means that we can work or play online from almost anywhere, so it's no surprise that public Wi-Fi networks have become more common. From hotels and coffee shops, to universities and city centers, Wi-Fi is widely available, but is connecting to these networks safe?

Most of us have heard about the importance of making sure that our home networks are secure, so that strangers can't access our information and we have a reduced chance of encountering viruses and other malware. What you may not realize is that we face the same threats when we connect to public Wi-Fi, but it's harder to tell if the network or hotspot is secure.

In fact, most public networks don't use a standard security measure called encryption, which encodes the information you send so it cannot be read by a third-party. And, these days, most public networks don't even require a password to connect to them, so they are open to anyone in the area, including people with bad intentions.

Using an unsecured Wi-Fi network is especially dangerous if you are logging in to your bank or other sensitive accounts because your login credentials could potentially be read as they travel across the network. If a cybercriminal who is using the same network gets a hold of your login details, they could then access your money or identity information by logging into your accounts as you.

So, if you are going to connect to public Wi-Fi, make sure that you take some steps to keep your device and information safe.

Follow these tips to stay protected:

- **Turn off sharing**—Keep others from accessing your computer and files by turning off sharing when you are on a public network. This can be accomplished by visiting your computer's control panel (on Windows), or System Preferences (Mac OS X).
- **Avoid automatically connecting to hotspots**—Keep your computer or device from automatically connecting to available Wi-Fi hotspots to reduce the chances of connecting to a malicious hotspot set up to steal information.
- **Use a "Virtual Private Network"**—If you frequently use public Wi-Fi, it might be a good idea to use a Virtual Private Network (VPN). A VPN is like your own private network you can access from anywhere. You can subscribe to VPN services for a low monthly fee.
- **Avoid information-sensitive sites**—When using public Wi-Fi, try to avoid logging in to banking and shopping sites where you share your personal and financial information. Only do these transactions from a trusted connection, such as your

protected home network.

- **Use sites that start with “https”**—Sites that begin with “https” instead of just “http” use encryption to protect the information you send. Look for this level of security on sites where you plan to enter login and other personal information.
- **Use comprehensive security software**—Software such as the McAfee LiveSafe™ service can help protect all your computers and devices from viruses or malware. In addition, make sure to turn on your computer’s built-in firewall, which monitors incoming and outgoing connections. This makes it more difficult for an attacker to gain access to your machine.