How to safely use free Wi-Fi

Public Wi-Fi is a convenient way to check Facebook, browse the Internet or do some online shopping on the go without putting a dent in your cellular data plan. Use this free app to find Wi-Fi anywhere you go. Unfortunately, if a hacker is on the same network, it gives them a good chance of snooping on what you're doing or even taking over your accounts.

Aside from hackers, the government and Internet service providers can also monitor your connection to see where you go, and, if they want, what you do. If you aren't a fan of that, and few people are, there is a way you can keep these parties out of your business.

The state of Internet security

Before I talk about that, however, let's do a quick review of the security measure that's already in place. Any finance, medical or shopping site that's even a little security conscious is going to provide you with an encrypted connection.

The encryption scrambles your traffic so hackers can't get your passwords or other information. You can tell encryption is running on a site when the Web address in your browser starts with "https://".

Aside from the types of sites I already mentioned, Facebook, Google and other major tech sites have adopted always-on encryption as well. However, not every site you encounter will, and some only provide partial encryption.

That means they might not encrypt the connection until you log in, which gives hackers a possible opening to steal your password. Or they only encrypt your login information and leave things like email messages exposed to traffic snoops.

Fortunately, more sites are moving to full-time encryption. Netflix is going to enable it over the next year, and even news sites are turning it on, with the largest one so far being The Washington Post. Mozilla, the developer of the popular Firefox browser, is even making plans to stop supporting unencrypted websites entirely in the future.

Of course, you don't have to wait for that level of security. You can fully encrypt your connection today and prevent hackers or anyone else from snooping on you.

VPN basics

To encrypt your connection, you can use a virtual private network. In the business world, VPNs let off-site employees create an encrypted connection with the company network so they can work safely.

Windows and Mac both have VPN features built in just for this purpose. However, for the average home user or traveler, these aren't very helpful because you need a network to connect to. That's where a third-party VPN service comes in handy.

A VPN service lets you create an encrypted connection with one of its servers, and you use that server to browse the Internet. The connection is encrypted through the server, so the VPN can't see your traffic either. OK, it's a bit more complicated than that behind the scenes, but that's the result.

To start, you need to choose a program or service to use. There are dozens that offer a mix of security features, privacy options, server locations and other considerations.

Note: If you're searching for VPNs, you'll see VPN services and "proxy" services. A proxy service can disguise your computer's identity, but it doesn't necessarily encrypt your connection. Always go with a VPN for security.

For the average user, it's important to make sure the service has U.S.-based servers, know how much bandwidth you can use per session or month, and to know that it doesn't keep logs of your activity. Paid services will require some personal information and payment information, naturally, but you can find one that minimizes what it needs to know.