WiFiSecurityTips

As we hope most people already know, when using public wifi hotspots you need to understand how to browse securely. Here are a few tips in how to be more security aware, and how to do some things more securely. Remember, unsecured wifi traffic can be sniffed with anyone with even a tiny amount of knowledge.

Note: As always with security, if you really need to keep something private, you need to do your own research about how to do it properly. These are only general tips and pointers to useful information elsewhere.

Using a VPN

VPN = Virtual Private Network. This is software you can run on your laptop to encrypt all or most network traffic from your laptop to a host server on the internet, which keeps your data secure from attackers on an open wifi channel.

Many employers provide VPNs if they allow workers to work at home; however be sure to check the documentation, since some employer-provided VPNs only encrypt traffic sent to the employer's networks, not everywhere.

There are a wide variety of paid and even free VPN providers and programs. They vary in price and ease of setup, but are definitely worth looking into if you're concerned about security when using open wifi hotspots.

Browsing Securely using SSL / https:

Seeing the http*s*:// at the start of the web address and the little lock in your browser shows that you're connecting to a website securely. That typically means that the information sent between your computer and the server at the other end of the URL is secure - however you do need to ensure you're actually getting to the right computer on the other end. In particular, if you get any certificate warnings or security alerts for websites you regularly visit while you're browsing over an open wifi channel, you should be suspicious (and click "No" unless you really know what the message means).

Blogging Securely

The best way to blog securely is to ensure your blogging site supports https for all it's connections. Depending on your blog's webhost and your blogging package, this is often easy to setup.

If you can't post to your blog over https, then consider saving a draft locally until you get to a secure network.

Emailing Securely

Again, you need to ensure you use SSL for getting mail from your POP or IMAP mail server, and for sending SMTP mail. Ensure in your client you check on SSL or security settings in your client.

This often also changes the port that your client connects to the server via. Unsecure POP uses port 25; secure POP should use port 995. Secure IMAP should use port 993. Secure SMTP should use port 465, although you also need to check your mail client's setup to ensure it's doing it securely.

For webmail accounts, ensure your webmail host uses https: for their website, or contact their support desk.

Using Social Networking Sites Securely

Most major social networking sites offer https: connections for their login process, meaning your password for logging into your account is reasonably secure. However they vary in their support for securely browsing within their websites. In some cases, if the social network sets cookies on your computer to allow you to stay logged in for a period of time, it's possible that an attacker could sniff the cookie over an open wifi hotspot and either temporarily access part of your social networking account, or possibly even change the password on your social networking account.

For most secure results, either ensure you can always use https:, or check with your social network's support group to see how to browse their site securely.