Welcome to Securing Your Digital Footprint

Free Wifi-

Unprotected Wifi networks, particularly in public places, are most certainly a threat. This is because you are connecting to a network without knowing *who else* could be on the network. ’Free Wifi' provided by cafes, restaurants, etc., serve as excellent places for harvesting passwords.

Sending data over Wi-Fi is kind of like sending messages by smoke signal. If you're connected through an open access point,(Public Library or McDonalds) anybody who can see the smoke can read your message.

Adding encryption (require a password) to the signal would be like using a special smoke that only you can see while wearing special glasses. The problem with a public access point in a coffee shop is that they hand the glasses out to every customer who ask for it. No matter how honest the manager and employees are, you don't know if somebody took the glasses out in the parking lot so they can read everybody's signal. Source:

Some experts even advise against checking Facebook or email accounts for the same reason, because too much information can be exposed to hackers that allows them to gain access to information and steal a person's identity. Source:

The hacker will perform a Man in the Middle attack, and can now read *all plaintext passwords*, including unsecured email (email that does not use encryption), unencrypted ftp, websites without HTTPS, etc. Not to mention they can see all your Google searches, all domains that you visit (encrypted or not) and so forth.

Now they move into a more advanced attack, setting up an active proxy on his machine to perform attacks such as SSL Stripping, which would give him access to *all* sites you visit, including HTTPS. This means he now has your PayPal, Facebook and Twitter passwords.

Moving on, a hacker might target your machine directly, if you have not updated your software in a while, it is likely that he can spawn a shell with Metasploit and download *all* your files for later analysis. This includes any saved browser passwords, authentication cookies, bank statements etc.

One other thing you might face is where they spoof the wifi host. You think you are logging into Starbucks, but you are actually logging into the hackers machine, before you move on to Starbucks machine. Always check with the business to verify what the name of the network is.

Ways to identify a rogue site, if a prompt asks you to re-enter your user name and password and if the Web browser suddenly says the security certificate is invalid: immediately log off and shut down your computer. Source:

Another situation that comes up when ‘sharing’ connections. If you have a cable internet connection and all of your neighbors have a cable internet connection, any unencrypted information that is sent on your subnet is visible to every one else on that subnet. This is marginally safer, only in the idea, that the number of people that can view information is a more static group and other people can only view information via a physical connection of some type. The firewall and NAT (Network Address Translation) operation of most routers will prevent direct access to resources on your local network, but it will not protect information sent without encryption (e.g. email). Internet email should never be considered secure. If you need to share information put it in a document and encrypt (WinZip w/ AES256). Source:

1.You can do several things to help secure your computer and secure your passwords while on a public network. The first rule is have a good firewall on your computer. ZoneAlarm is free and good to use withPC’s, I would not recommend the one that Microsoft offers. Apple includes one that is quite good. Make sure you are on the highest level of security when on a shared public network.

2. if you have any shared files, check the permissions to ensure that only authorized users can access it (in particular, do not have it set to "Everyone"). Instructions for Windows. Instructions for Apple.

3. Use a good, comprehensive Internet Security software is also important to ensure no malware is running to expose the system.

4. The next thing you can do is make sure your transactions on the network are encrypted. Using a Virtual Private Network connection to a known secure proxy server is one of the best ways. Nothing you transmit on the public network would be viewable.

5. Make sure when you are finished with the freebie - you close out of everything and forget the network. Android instruction. Windows instructions. Apple OS X instructions. Apple iOS instructions.

If you can’t access a VPN the following steps are recommended:

1. Do not do any banking or credit card transactions.

2. Do not login to any site, this includes email, social media, Amazon/Ebay/Paypal.

3. Do not update your software on a free site.

4. Make sure when you are finished with the freebie - you close out of everything and forget the network. Android instruction. Windows instructions. Apple OS X instructions. Apple iOS instructions.

Free wifi hotspots can be handy, just remember whether you are on a computer, smartphone or tablet to be careful and aware. If you need to do some surfing, or check your email use your cell connection. It is more secure to local prying eyes, and will teach you brevity.