Security Tips for Free Wi-Fi

SecurIT360
The physics of securing IT

Is free Wi-Fi really free? What do you think?

Mobile computing is a very risky way we use and share information and expose our equipment to attack or loss.

Remember that no matter where you use Wi-Fi, there are risks associated. It is critical to use caution when deciding to connect to a public or free wi-fi link. The same features that make free WiFi hotspots convenient for consumers make them convenient for hackers.

Once you connect to unsecured public Wi-Fi, all your internet traffic is vulnerable to interception and eavesdropping.

For Example:

- Passwords
- User ID's
- Online Banking Credentials
- SMS text messages
- Private Facebook Chats
- Personal pictures and videos sent over SMS
- Skype conversations
- E-mail content

The weakest portion of your wireless connection is that short distance between your computer or mobile device and the Wireless Access Point just like the one you use at home.

It is called **the last yard**.

If you need to use public or free Wi-Fi, you must take steps to protect yourself.

Use a VPN (virtual private network)

A VPN creates a "private tunnel" that encrypts any data that passes over the wifi connection. This can prevent a cybercriminal from intercepting your data. Make sure the VPN is enabled before you leave home. It's so EASY! There are free VPN clients available of you don't already have one in mind.

Make sure that your e-mail client settings only allow you to download e-mail *after* you are connected to the VPN.

Verify that the Wi-Fi Link is legitimate

If you want to use Starbucks' Wi-Fi for example, you need to know exactly which link to select. Ask what the exact name of the Wi-Fi network name and verify that the name you select matches exactly. For example, **StarbucksCustWifi** may be a legitimate Wi-Fi link. However, Starbux1, could be wi-fi hotspot broadcast from a nearby vehicle which is set up solely to capture the data of an unsuspecting user.

Avoid Sites That Store Personal Information

If you must use public W-Fi, try to avoid accessing web sites which store and use personal information. These would include-

- Social Media Sites
- Online Banking Sites
- Online Shopping Sites

Avoid any site which would require a credit card number or social security number. If you're not sure if a site collects personal info, check their PRIVACY POLICY! It's usually linked somewhere from their website.

Use Your Cell Phone "Hotspot" Instead

Your cell phone may have an option for you to connect your laptop to the internet via your cell phone. If you do need to access internet sites like those listed above, your cell phone and mobile provider will provide a more secure connection. After all, you're paying for it!

dburns@securit360.com

Security Tips for Free Wi-Fi

SecurIT360
The physics of securing IT

Always Use a Strong Password

A strong password, or a "pass-phrase" is an absolute necessity. Your password should be at least 12 characters and complex enough that an observer would not be able to "shoulder surf" and figure it out.

Keep Your Updates Up to Date

Make sure your laptop has the latest software updates installed before you leave home. These include the latest security updates for your device. Other than anti-virus software, these updates should never be performed on a public / free network.

Make sure that your device has both anti-virus and anti-malware software installed.

Always Keep Your Devices in Your Possession

It is very tempting to ask someone else to "watch your bag" at an airport, restaurant, etc. You cannot afford to do this. The person next to you could be a cyber-criminal, or just someone who may have other than admirable intentions. Always keep your laptop, cell phone or tablet where you can protect them!

Set Your Settings

Simply turning settings on or off as appropriate can help protect you from the risk of cyber theft.

- Keep Wi-Fi turned off unless needed
- Set your screen saver to activate after 5 minutes
- Disable internet connection sharing on your laptop
- Turn off Bluetooth to avoid "drive-by" attacks

Remember:

Develop a "cyber-defense" mindset and protect yourself!

If you would like to learn more about Cyber Security and how to protect your company, contact -

David Burns
Account Manager, SecurIT360
dburns@securit360.com
205.787.1250