BRANDPROTECT EXECUTIVE THREAT BRIEF

brandprotect™

July 2015 | Briefing 7

THE PERILS OF PUBLIC WIFI

STAY SAFE ON PUBLIC NETWORKS

In today's 24/7 world, whether you are in the car, on the road, on vacation, out to lunch or dinner or even, increasingly, on a plane, connectivity is assumed. Often getting on the "network" is the first priority when you arrive at a new place. But **using a public WiFi network carries some risk**. The very same qualities that make public WiFi so convenient also make it dangerous. Basically, when you connect to the WiFi network, you may be providing the network with access to much of the information that is on your device. When you communicate over the network, others can be listening in….

In addition to eavesdropping, advanced cyber criminals can use their rogue hot spot to connect to your machine and **download spy software to your device**. This malicious package will capture your activity and communicate it to the bad guys when you are connected to the Internet. This kind of attack is a major security risk for businesses, because when you bring your device into your office, you are providing the criminals with priceless information about your corporate networks and data.

Fortunately, it is **relatively easy to reduce threat of being compromised** by WiFi threats. By taking a few simple actions, you'll make your information harder for criminals to intercept, and harder for criminals to use. Follow these five steps to safety and you'll sleep easier.

5 SIMPLE WAYS TO REDUCE YOUR RISK

CLOSING THE WIFI DOOR

A virtual private network (VPN) connection offers a very high level of security for people who must access networks and servers remotely. **VPN connections feature strongly encrypted communications**, which makes your information instantly much less desirable for most hackers. VPN should be easy to use, almost all business have VPN options set up for remote workers. If you are not using VPN to connect to your office network, find out more about what your office offers.

USE SSL CONNECTIONS

The Secure Sockets Layer (SSL) is a widely used communications technology that **encrypts general Internet browsing**. When you are online, look at the URLs of the sites you are using. If they begin with http:// consider them to unsecure. If they begin with https:// they are using the SSL technology to secure your communications. Almost all shopping and banking sites have now implemented SSL.

Most modern browsers automatically prioritize an https:// connection over an http:// connection. However, you should still glance at the address bar in your browser when you are about to enter password or other sensitive information into a log-in or other online form. If you are not in an https:// session, you could be revealing your content to eavesdroppers.

DON'T SHARE! DON'T TRUST!

Sharing is an advanced feature of modern operation systems. When Sharing is enabled, other computers connected to the same network can gain access to information and files that you have saved on your machine. Usually this information must be in specially designated folders. Most times, when you log into a new network for the first time you will be asked characterize the network. The exact question will vary but it will usually be something like: Trust This Network? (answer "NO") or what kind of network is this Secure or Public (answer "Public") Remember, **in a public network, why would you want to share anything?!**

MAN IN THE MIDDLE ATTACKS

A man in the middle attack (MITM) is one of the most common WiFi schemes. In one common variation, the cyber-attacker creates their own hot spot in a public area, say a public plaza near a business center. They give it a believable name, like "Plaza Public WiFi" and wait for people to connect. As the people connect, the attacker logs all the data that passes through the malicious hot spot. Much of that data will be encrypted (and ignored) but some of the communications will be unencrypted. Those unencrypted communications are the loot the criminal is looking to capture. They will be mined for personal data, user names, passwords, account numbers, etc.

NOT USING WIFI? TURN IT OFF!

When WiFi is turned on – even if you are not logged into a network – your computer or smart device is scanning for available networks. In some cases, your computer or device may automatically connect to the unsecure hotspot network, **If you're don't need network access**, for example if you are working on a document or presentation, **turn your WiFi off**.

STAY PROTECTED

No matter how hard you try to stay secure, it's likely that sometimes you will be forced to rely on less reliable networks. As a result, you run the risk of uploading a malicious virus, adware, ransomware or other kind of malware. To protect you from harm, **make sure you have an antivirus, antispyware, antimalware solution** installed and running on your machine. This way, any new files on that are uploaded to your machine (including email attachments, files introduced from an external drive, or direct downloads) will be scanned for safety.

Wifi Check List

Do:

- ✓ Use your personal cell phone connection via secure tethering
- ✓ Use VPN to connect to work or other networks whenever possible
- ✓ Use the more secure "HTTPS" option when connecting to websites
- ✓ Consider ALL outside networks "PUBLIC"
- ✓ Disable "Automatically Connect to WiFi" options
- ✓ Turn off WiFi when you are not using it

Don't:

- ✗ Use unsecured public WiFi
- ✗ "Trust" public networks

NEW WIFI OPTIONS MAY SIMPLIFY YOUR FUTURE

Telecom carriers have long offered public hotspots to those willing to pay a small fee. Now companies like Skype, Google and Microsoft have launched or are launching large scale WiFi networks. If you travel a lot, these offerings may make sense. They should offer you a **much greater measure of trust and security** than an open public network.

brandprotect™

www.brandprotect.com
sales@brandprotect.com | 1.866.721.3725

For enterprises concerned about their business exposure to increasing online risk, BrandProtect™ provides a complete suite of world class Internet threat detection services to monitor the entire social Internet spectrum and mitigate business risk arising from fraudulent or unauthorized online activity. BrandProtect helps security, risk management, and marketing organizations at leading financial services institutions, large-scale retailers, insurance providers, telecoms, pharmaceuticals and more, protect their brand value and business bottom line.