Security tips for public Wi-Fi

With most people carrying around smart devices, whether it's a smartphone or tablet, having access to Wi-Fi is almost a necessity. And if your device's mobile or data plan isn't generous, coming upon public Wi-Fi while you're out and about can be a life-saver. But just how risky is using public Wi-Fi?

Should I really be worried about public Wi-Fi?

When using public Wi-Fi, your device (and thereby your personal information) is vulnerable because it is possible that someone else can access it. There are two ways someone can gain access to your information while using public Wi-Fi: (1) access to your device and the content on your device, and (2) access to the information you are sending/receiving when connecting online (which may include websites you visited and sometimes your username/passwords).

Access to your device

Whenever you connect to a public Wi-Fi, you are connected to a network, along with all the other devices connecting to that network. Depending on the settings on your laptop or tablet, it could allow someone else using that same network to see your device and even access to your files. The settings that allow this access are "discovery" and "file and print sharing." Check your laptops and turn off these settings when logging onto public Wi-Fi. If you have a MacBook, iPhone or iPad, turn off Airdrop or change the setting so that only contacts can connect.

Although not as common, another way someone could gain access to your device is if a malicious individual (a hacker) scans for open ports to see if they can hack your device. A port allows your device to send and receive data when you connect to the internet and is a normal process. Generally, a port opens only when you are connecting to the internet (send an email, visit a website). You can increase your device security by making sure the firewall is turned on and by running anti-virus software on your devices.

Access to your internet traffic data

Another method hackers can use to gain information about you is to intercept your internet traffic data, such as websites you visit and login credentials (username and passwords). Generally, the hacker will need to be connected to the same public Wi-Fi and is purposefully intercepting other users' internet traffic. Depending on their sophistication, skill, and goal, the hacker may merely be eavesdropping (watching your internet traffic) or they could change your data in transit, sending you to fake websites or websites with malware.

Some hackers may create fake Wi-Fi hotpots where they can monitor and see the internet traffic of everyone who connects to that fake hotspot. They will be able to see usernames, passwords, and other sensitive information.

© 2017 WESNET

What can I do to increase my security?

Use a VPN (virtual private network). If you are worried about someone intercepting your information, a VPN to encrypt your internet traffic. A VPN works by encrypting your internet traffic and sending it to an alternate server somewhere else on the internet. Once the encrypted information has reached that alternate server, it is decrypted and sent to its final destination. The VPN disguises both web content and destination as it passes over the public Wi-Fi, and makes it look as if the requests are from that alternate server, keeping your IP address and location anonymous.

VPNs can be helpful even when you're on a password protected Wi-Fi network, since hackers can still hack those networks and potentially eavesdrop on your communication. There are VPNs for computers/laptops, tablets, and mobile devices.

Turn on the firewall on your laptops. Most all laptops have firewalls built in, but some don't have them turned on by default. A firewall will protect your laptop from someone who is trying to hack it through its open connections. To check if your laptop's firewall is on, check the firewall settings under the Control Panel (for Windows operating system) or System Preferences/Security & Privacy (for Mac).

Turn off file sharing, printer sharing, and discovery on your laptops. If your laptop is connected to the same network (the public Wi-Fi), it could allow someone who's also connected to the same network to see and access files on your computer if you have these settings turned on. You can turn off these settings under the Control Panel (for Windows operating system) or Systems Preferences (for Mac).

Use HTTPS. Most websites offer HTTPS, which you can tell by the addition of the letter "s" at the end of HTTP. Sites using an HTTPS connection is best when using an open/public Wi-Fi Network as it will encrypt the information being shared between your browser and the website you're communicating with. Keep in mind that HTTPS only encrypts the content, not the destination; meaning that if a hacker was eavesdropping, they will see that you visited Facebook, but will not see your username or password. Most web browsers allow you to add an extension that will automatically connect you to an HTTPS connection where one exists. HTTPS Everywhere has links to most popular web browsers' HTTPS extension.

Run anti-virus/malware software. The most harm that hackers can do is to infect your device (laptops, tablets, mobile) with viruses and malware. If your device is vulnerable, and you've connected to an open network (such as a public Wi-Fi), hackers can infect it with malware. Run anti-virus, anti-spyware software on your devices. Anti-virus software will scan your device and files you download for malware, and if it detects any, it will prevent the malware from installing.

Update the security software on your devices. Sometimes, hackers can exploit security vulnerabilities of your devices, and this can include how your device connects to the internet. Whenever security vulnerabilities are discovered, companies will often create security updates to patch them. This means that when your device, software, or apps prompt you to update the software, make sure you do so. Keep in mind that some older devices (such as some Android

© 2017 WESNET

mobile devices) or operating systems may no longer be supported with security updates. In which case, follow the other advice in this article or upgrade to a new device or operating system.

Be careful with public Wi-Fi hotspots without passwords. While some people may decide not to use public Wi-Fi for fear that hackers might access their device and information, some may decide that the benefit of having access to public Wi-Fi outweighs the risk. In which case, some public Wi-Fi might be safer than others. Be cautious of Wi-Fi hotspots that don't have a password. Without a password, anyone can hop on, which makes these networks easy targets for hackers. Also, be cautious of Wi-Fi hotspots in large places where many people are logging in, such as airports. The large number of people connected to one network can be an attractive target for hackers.

Turn off Wi-Fi. If you are not using Wi-Fi, a good practice is to turn it off. You can always turn it back on when you need it. Another good practice is to "forget the network" after you've finished using the public Wi-Fi. This way, your device doesn't stay connected, making it vulnerable to hackers.

Don't access sensitive accounts. If you must use public Wi-Fi, try not to access sensitive accounts such as your bank, email, or accounts that contain personal and sensitive information. Wait until you're on a more secure connection before you check those accounts.

Follow good laptop, mobile, and internet practices. The best protection is to follow good security practices while on your laptop or mobile device, or online. Check out WESNET's other resources for those tips and advice.

Use a privacy screen. And finally, don't forget about that nosy neighbour looking over your shoulder. He doesn't need hacking skills to know what websites you're visiting and what you're typing into your screen. Use a privacy screen over your laptop, tablet, or mobile device so someone can't see the screen unless they're looking straight at it.

Could my abuser hack my device while I'm on public Wi-Fi?

One of the big concerns for many survivors is whether their abuser could hack their devices while they are on public Wi-Fi. In general, someone can gain access to your device or eavesdrop on your internet traffic via public Wi-Fi if they are on the same network or is within proximity to you, and have the "hacking" skills, tools, and information about the Wi-Fi network to do so. If they are not on the same public Wi-Fi, the chances of them being able to remotely hack that network to find out your information is low.

If your abuser already has remote monitoring access to your devices, it doesn't matter where you connect – via public Wi-Fi, your home Wi-Fi, or your mobile data. They will be able to monitor your device. If that's the case, read WESNET's other handouts on laptop and mobile spyware.

© 2017 WESNET