The Security Risks of Public Wi-Fi (And Why You Should Never Use It Without a VPN) – Matt Powell

Public Wi-Fi is very convenient. Say you're in a country that you are not native to, and your phone's service no longer works. Hop onto some public Wi-Fi and you're good to go. But are you really*? The answer is no.* While public Wi-Fi does have its purpose, it also poses a risk to anyone and everyone who uses it. Public Wi-Fi is convenience technology, and like all convenience technology, leads to complacency; which is the first step towards becoming a cybercrime victim.

Here are the security risks that come with public Wi-Fi.

2. Man-in-the-Middle attacks

When you use a computer or smart device, data is sent to and from said computer or device, to a website or app. And sometimes, men in the middle (hence the name) pilfer data as it makes its way to and from point A and B.

As stated in our above point, most businesses have terrible cybersecurity and you have non-existent protection when you use public Wi-Fi. Men in the middle take advantage of this and victimize countless innocent users.

Another trick that men in the middle use to get the data of unsuspecting victims is to use their own Wi-Fi to trap people. They will name their own Wi-Fi connection the same as a common name used by a business such as a hotel or coffee shop, and people will connect to these networks not knowing that these are the Wi-Fi networks of hackers. How can you tell if a Wi-Fi network is legit or not? More often than not, you likely won't be able to.

3. In regards to public Wi-Fi, sharing is NOT caring

Most people probably don't realize that they have file sharing turned on with their devices. Well, you may want to check to see if you do and turn it off, since hackers take advantage of this.

Having file sharing on when using public Wi-Fi is like opening up your door to hackers. Any sensitive information that you have no problem being out in the open when you are at home, is now out in the open in public. You do not want that. Be sure to turn file sharing off.

4. Automatic Wi-Fi connection can lead to connecting to a hacker's network

If you look at your smartphone or computer's Wi-Fi section, you may notice that your device automatically looks for Wi-Fi networks that it can connect to. And as you may have guessed, hackers would love for you to connect to their network so they can steal your data. Again, we stress that convenience leads to complacency. Humans are smarter than the tech we utilize, which is how victims end up connecting to ad hoc networks without even knowing it. If your device automatically connects to open Wi-Fi, turn this function off immediately.

Tips to protect yourself when using Public Wi-Fi

1. Always use a VPN

Whether you're at home using your own Internet service, or at Starbucks using their public Wi-Fi, always use a VPN. The Internet is getting far too dangerous and invasive to go without using one.

2. Keep your Internet usage as harmless as possible

Don't use public Wi-Fi to handle any sensitive information or business transactions. If you're using public Wi-Fi, try to do things that won't really put you at any risk, like watching cat videos on YouTube. Avoid inputting any usernames or passwords if you can.