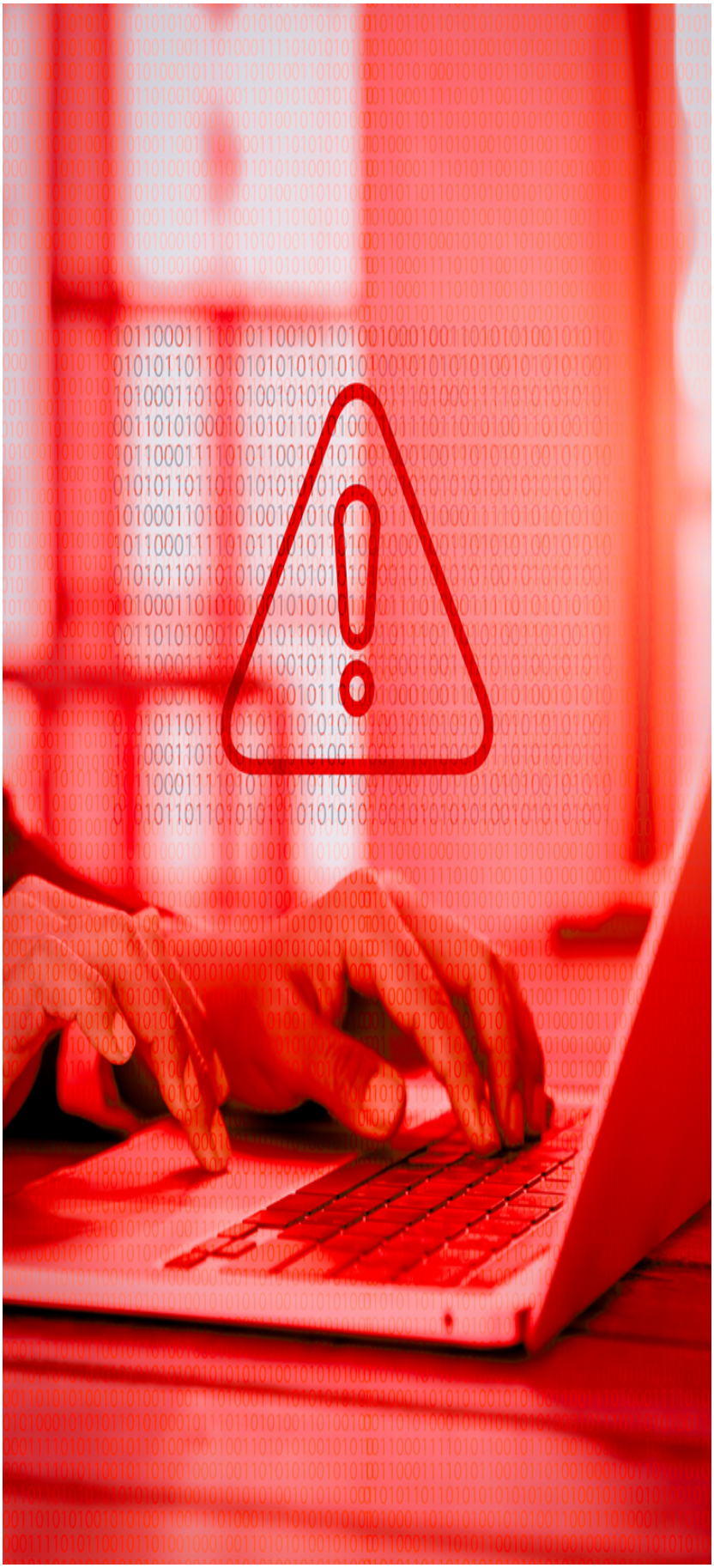
RISK & TIPS FOR PUBLIC WIFI

Introduction

Wi-Fi users are at risk from hackers but fortunately, there are safeguards against them. The recent explosion of free public Wi-Fi has been an enormous boon for working professionals. Since these free access points are available at restaurants, hotels, airports, bookstores, and even random retail outlets you are rarely more than a short trip away from access to your network and work. This freedom comes at a price though and few truly understand the public Wi-Fi risks associated with these connections. Learning how to protect yourself will ensure your important business data remains safe.



The Risks of a Public Wi-Fi

The same features that make free Wi-Fi hotspots desirable for consumers make them desirable for hackers; namely, that it requires no authentication to establish a network connection. This creates an amazing opportunity for the hacker to get unfettered access to unsecured devices on the same network.

The biggest threat with free Wi-Fi security is the ability for the hacker to position himself between you and the connection point. Instead of talking directly with the hotspot, you are sending your information to the hacker, who then relays it.

While working in this setup, the hacker has access to every piece of information you're sending out on the internet: important emails, credit card information and even security credentials to your business network. Once the hacker has that information, he can — at his leisure — access your systems as if he were you.

Hackers can also use an unsecured Wi-Fi connection to distribute malware. If you allow filesharing across a network, the hacker can easily plant infected software on your computer. Some ingenious hackers have even managed to hack the connection point itself, causing a pop-up window to appear during the connection process offering an upgrade to a piece of popular software. Clicking the window installs the malware.

As mobile Wi-Fi becomes increasingly common, you can expect internet security issues and public Wi-Fi risks to grow over time. But this doesn't mean you have to stay away from free Wi-Fi and tether yourself to a desk again. The vast majority of hackers are simply going after easy targets and taking a few precautions should keep your information safe.

Use a VPN

A Virtual Private Network (VPN) connection is a must when connecting to your business through an unsecured connection like public Wi-Fi. Even if a hacker manages to position himself in the middle of your connection, the data will be strongly encrypted. Since most hackers are after an easy target they'll likely discard stolen information rather than put it through a lengthy decryption process.

Always HTTPS

You aren't likely to have a VPN available for general internet browsing but you can still add a layer of encryption to your communication. Enable the "Always Use HTTPS" option on your web browser. HTTPS will help prevent attackers from seeing the information you submit to a website. If you reuse passwords (which you really shouldn't!), that password could get stolen and used for other websites you visit.

Its important to know that just because a website is HTTPS encrypted, that does not imply the website is safe. HTTPS only grants you the security of your connection to a website- good or bad. You'll still have to use best judgement!

Turn Off Sharing

When connecting to the internet at a public place you are unlikely to want to share anything. You can turn off sharing from the system preferences or control panel, depending on your OS, or let Windows turn it off for you by choosing the "Public" option the first time you connect to a new unsecured network.

Keep Wi-Fi Off When You Don't Need It

Even if you haven't actively connected to a network the Wi-Fi hardware in your computer is still transmitting data between any network within range. There are security measures in place to prevent this minor communication from compromising you but not all wireless routers are the same and hackers can be a pretty smart bunch. If you're just using your computer to work on a Word or Excel document keep your Wi-Fi off. As a bonus, you'll also experience a much longer battery life.

Stay Protected

Even individuals who take all the possible public Wi-Fi security precautions are going to run across issues from time to time. It's just a fact of life in this interconnected age. That's why it's imperative to keep a robust internet security solution installed and running on your machine. These solutions can constantly run a malware scan on your files and will always scan new files as they are downloaded. The top consumer security software will also offer business protection solutions. You can protect yourself while you're out and about along with your servers back at the office all at the same time.

Throughout any business travelers' life there's going to come a time when an unsecured free public Wi-Fi hotspot is the only connection available and your work simply has to get done right then. Understanding public Wi-Fi risks will ensure your important business data doesn't become just another hacking statistic.