Skillmine
Technology • Consulting • Services

infosec
Miners

PUBLIC WI-FI

Public Wi-Fi can be found in popular public places like airports, coffee shops, malls, restaurants, railway stations and hotels and it allows you to access the Internet for free. These "hotspots" are so widespread and common that people frequently connect to them without even thinking of it twice.

HOW TO PROTECT YOURSELF ON PUBLIC WI-FI NETWORKS?

Once a luxury item, free public Wi-Fi has morphed into a standard service that consumers expect when patronizing everything from restaurants and retail stores to airports and hotels. Free Wi-Fi users aren't just checking Facebook or posting vacation photos to Instagram, either; all of us have sat down at a train station or in a coffee shop and seen business people tapping away on their laptops, taking advantage of public Wi-Fi to work on the go.

Numerous cyber-attacks if the network is unsecured. These includes:

01 Bogus rogue networks set up specifically by cyber criminals. These networks often have innocent-sounding names such as "Customer Public Wi-Fi" and they are unsecured.

02 Man-in-the-middle attacks where hackers commandeer a public Wi-Fi network and redirect users, often to a bogus login site where their credentials are stolen.

03 Wireless sniffer tools that locate unsecured public Wi-Fi networks, analyse their packets, and steals data, monitors network activities, or gather intel for use in a future attack against the enterprise's network.

04 Having your device infected by a worm on another user's device that travels through the public Wi-Fi network.

STAYING SAFE ON PUBLIC WI-FI:

The best way to prevent an attack on a public Wi-Fi network is to never connect to one in the first place, even if it is "secured." The WPA/WPA2 Wi-Fi standard is currently in use has multiple security flaws. Far more secure WPA3 won't start rolling out until next (later this) year, when devices supporting it are scheduled to be released. Instead of using a public Wi-Fi network, tether your laptop to your mobile phone or use one of your mobile carrier's hotspots.
If you travel a lot, it may be worth investing in an unlimited mobile data plan.

infosec
Miners

PROTECT YOURSELF USING THESE BEST PRACTICES:

Use a Virtual Private Network (VPN)

VPNs allow users to connect to servers through the secure connections. While many free or ultra-low-cost VPN services are available in market, they may not be trustworthy; it's better to pay for the peace of mind to avoid getting affected. Employers should provide their employees with VPN access to protect their companies' data when their employees are working in the field.

Use Secure Connections

Configure your browser to default to "always use HTTPS" option on websites for which you use frequently, especially those that require the login credentials.

Don't Access Anything Sensitive

Do not check your bank account or credit cards, go shopping, or access any other sites that would expose sensitive personal information using public wi-fi.

Turn Off Automatic Connectivity

Change the settings on your devices so that they do not automatically connect when they sense an open Wi-Fi network; you could end up connected to a phony rogue network. Even if you're not stuck using the public Wi-Fi networks, never leave your electronic devices unattended while in a public place, and make sure to turn off Bluetooth and file sharing capabilities.

THE RISKS OF PUBLIC WI-FI:

Man in the Middle Attack (MitM)

An MitM attack is a form of eavesdropping, in which the attacker secretly intercepts and relays messages between two parties who believe they are communicating directly with each other. This gives the attacker the ability to capture and manipulate the sensitive information in real-time.

Malware Distribution

A software vulnerability is a security hole in the operating system or software program. Hackers can exploit this weakness by writing code to target a specific vulnerability, and then inject the malware on the user device over the Internet.

Snooping and Sniffing

Cybercriminals can buy special devices to help assist them with eavesdropping on Wi-Fi signals. This allows the hackers to access everything like your online activities, capture your login credentials, and potentially hijack your accounts.

Malicious Hotspots

These "rogue access points" trick victims into connecting to what they think is a legitimate network but instead it is a rogue hotspot. Just because the name sounds reputable, that is you are at a Marriott and the name of the hotel appears, it does not mean that you are.

CONCLUSION

Even individuals who take all the possible public Wi-Fi security precautions are going to run across the issues from time to time. That's why it's important to keep a robust Internet security solution installed and running on your machine.

> **Wifi is the umbical cord of the modern world.**
>
> *-Kammpan Sharma*

SKILLMINE CYBER SECURITY TEAM

Skillmine
Technology • Consulting • Services

#46/4, Novel Tech park,
Kudlu Gate, Bangalore
Karnataka-560 068

☎ +91 9920063515
www.Skill-mine.com
info@Skill-mine.com

India | KSA | UK | USA

Stay connected