Public Wi-Fi Dangers

You have something really important to tell your friend. Maybe it's a personal secret, a private family matter, sensitive work details, you name it. One thing's for sure: you definitely don't want strangers hearing about it. Would you take your friend and stand in the middle of a crowded café and yell your secret out? Or would you talk to your friend in a quieter place away from eavesdropping strangers? Most probably you'd choose the second option. But what if I told you that you've always been choosing the first option all along without even realizing it?

Welcome to the hidden dangers of Public Wi-Fi. In this module, we'll cover why public Wi-Fi is dangerous, the dangers of using public Wi-Fi, and how to protect yourself from them.

1- **Man-In-The-Middle Attack**

Sweet, free internet access in my favorite café, what could go wrong? Everything. Logging into your Facebook account on public Wi-Fi? Congratulations, you're handing out your email & password to a hacker on a silver platter. But how is that possible? Simply put, you were a victim of a Man-In-The-Middle attack.

An MiTM attack is an online attack where the hacker secretly sits between you and the application you're trying to use. It's like trying to tell your friend something but instead of speaking with them directly, you whisper it to a stranger which then tells your friend. That “stranger” is not trustworthy, but they hear everything you say and tell. Now imagine, instead of them delivering the exact message you want to deliver, they change it. For example, you want to tell your friend “I love pizza”, that “random person” would then deliver the message as “I hate pizza”, which totally changes the original meaning of the message, and neither you nor your friend have any idea that the message was tampered with!

That′s how an MiTM attack works: the hacker can listen in, steal your private information, or even change what′s being sent without you or the app knowing anything went wrong. Sounds scary, doesn′t it?

2- Malware Distribution

Ever heard of a computer “virus”? It′s that bad application that harms your computer; you probably know about it. A computer virus is a type of malware. Malware is a malicious program that has the sole purpose of damaging your device, it could slow your device down, steal data from your device, and the list goes on.

Thanks to public Wi-Fi, a hacker can easily install malware on your device! Hackers trick users that are connected to public Wi-Fi into downloading malware. For instance, they can send a pop-up ad to your device urging you to install a “critical software update”. Once you install it, malware instantly starts damaging your device.

One of the most dangerous types of malware is Ransomware. Simply explained, ransomware locks ALL of your files and demands money to unlock them back! Imagine you’re in a hurry to submit an assignment and you can’t finish it because of a ransomware, I wouldn’t wish that feeling on my enemy.

3- Session Hijacking

You’re scrolling through your Facebook feed as normal, only to find out you have sent a weird message to several people asking for money to be sent to a wallet registered to a phone number that’s not yours, how is that possible? Nobody even touched your computer except yourself! That’s what session hijacking is: the hacker hijacked your Facebook session and used it to send these weird messages to your friends. The scariest part? They didn’t even need your email and password; they were already in by using your logged-in session. Of course, that can be applied on various websites other than Facebook, imagine your bank account! They could use that session to send money to themselves! Public Wi-Fi could really cost your bank money, frightening.

Our advice is to never use public Wi-Fi, but sometimes we’re obliged to use it. Before hopping on public Wi-Fi, here’s how you can stay safe and avoid the dangers of it as much as possible:

1- **Use a Virtual Private Network (VPN):** A VPN is crucial when connecting to public Wi-Fi. A VPN is used to encrypt your internet connection and the data being sent and received. In other words, it makes it almost impossible for hackers to intercept your data and read it, such as credentials or even messages you're sending to your friends!

2- **Enable 2FA:** 2FA, or Two-Factor Authentication, adds an extra layer of security to your accounts. Even if an attacker got your email and password through public Wi-Fi, with 2FA enabled, they still can't access your account. 2FA requires you to insert an OTP (One-Time passcode) sent to your phone number or email in order to get into your account.

3- **Avoid Accessing Sensitive Information:** When on public Wi-Fi, avoid using websites that requires you to submit your credentials or provide you sensitive information such as bank details. That way, even if a hacker spies on your activity, they wouldn't find anything useful.

4- **Have up-to-date trustworthy antivirus installed:** Antiviruses are like bodyguards that protect your device against various types of threats that could harm your computer. By having them installed, hackers would have a hard time trying to hack you!