What is Public Wi-Fi?

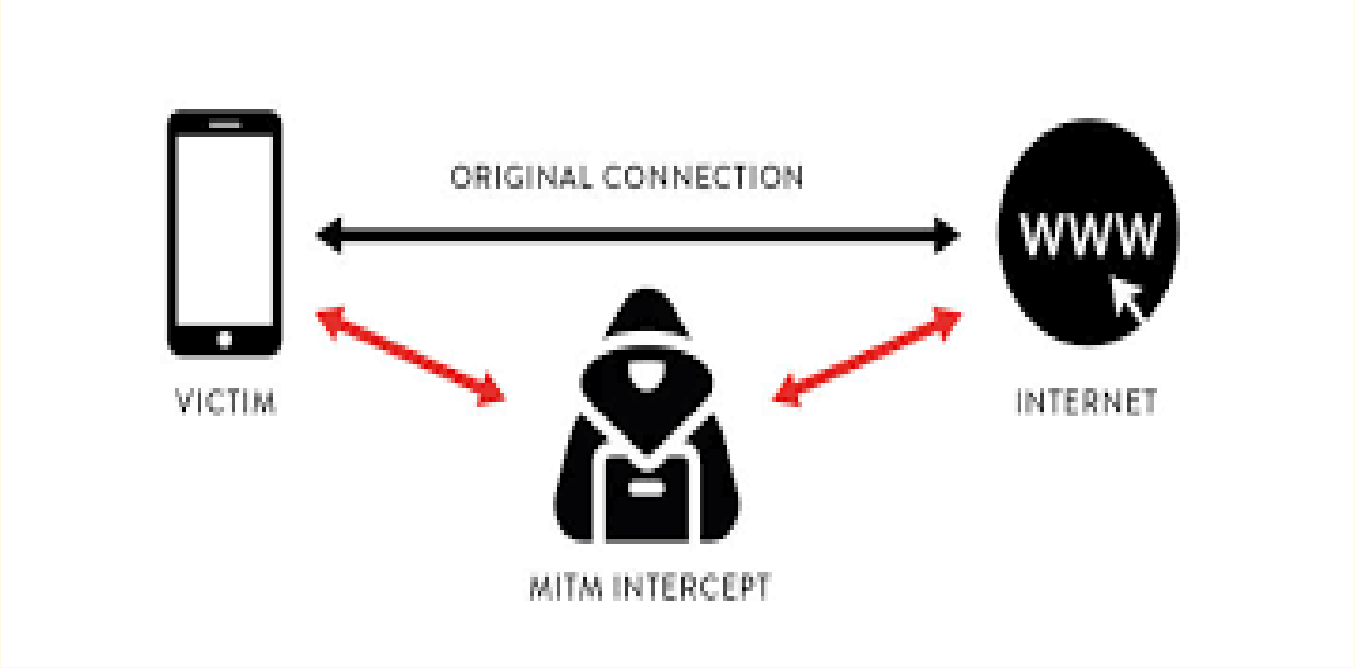
Public Wi-Fi can be found in popular public places like airports, coffee shops, malls, restaurants, and hotels etc and it allows you to access the Internet for free. These “hotspots” are so widespread and common that people frequently connect to them without thinking twice. Although it sounds harmless to log on and check your social media account or browse, everyday activities that require a login like reading e-mail or checking your bank account could be risky business on public Wi-Fi.

1. Unencrypted networks

Clear text transmission of data over unsecured Wi-Fi channels leaves other kinds of information open to interception, modification, and theft. This would include corporate data, intellectual property, images, media files, and the content of unencrypted email or instant messages.

2. Snooping and Sniffing

Wi-Fi snooping and sniffing is what it sounds like. This technique can allow the attackers to access everything that you are doing online from viewing whole webpages you have visited (including any information you may have filled out while visiting that webpage) to being able to capture your login credentials, and even hijack your accounts .



3. Malicious hotspots

These “rogue access points” trick victims into connecting to what they think is a legitimate network because the name sounds reputable. Say you’re staying at the Goodnight Inn and want to connect to the hotel’s Wi-Fi. You may think you’re selecting the correct one when you click on “GoodNyte Inn,” but you haven’t. Instead, you’ve just connected to a rogue hotspot set up by cybercriminals who can now view your sensitive information

Disable auto Wi-Fi connect. If your phone automatically joins surrounding networks, you can disable this function in your settings. Avoid linking to unknown or unrecognized networks.

Turn off Wi-Fi when done. Your computer or phone can still transmit data even when you are not using it. Be sure to disable your Wi-Fi from the network when you are finished using it.

Avoid financial transactions. You must not use public Wi-Fi, don't conduct a sensitive transaction such as banking, shopping, or any kind of activity that requires your social security or credit card numbers or password use. Wait until you get to a secured home network to conduct personal business.

Look for the HTTPS. Fake or unsecured websites will not have the HTTPS in their address. Also, look for the little lock icon in the address bar to confirm a secure connection.