CYBALT

Public Wi-Fi Safety: Why It Is So Vulnerable to Attack?

CYBALT

Public Wi-Fi Safety: Why It Is So Vulnerable to Attack?

In this digital world, there are so many places where we are vulnerable to cyber criminals' attacks. Mostly at the top of the list is when we are using public Wi-Fi. Public Wi-Fi networks in the world are widely and readily available in airports, parks, restaurants, coffee shops, libraries and hotels; people frequently connect to them without thinking twice.

Wi-Fi allows your devices to establish a network connection with each other without a wired connection, and in a specific area of coverage. Public Wi-Fi is a service provided by a restaurant, coffee shop or any public place that offers internet access in free of cost or sometime with minimum charges. Public Wi-Fi is incredibly vulnerable to cyberattacks, as this connection mode streamlines easy access to your sensitive information.

Here free of cost sounds good, hence everyone likes this. Free means it may be not too much secure and also sometime no need to authenticate to establish a network connection, Remember that free Wi-Fi provides a good opportunity for Bad guys to access your confidential information and once he get this confidential information then he can do lot of things with it.

The average free public Wi-Fi connection isn’t secure. Just because you may need a password to log in, it doesn’t mean your online activities are encrypted. Public Wi-Fi can leave you vulnerable for different reasons. One reason has to do with the encryption protocol used by some wireless networks.

The less security the Wi-Fi hotspot has, the easier it is for an attacker to connect and eavesdrop on users, distribute malware and steal sensitive information. Techniques such as snooping, sniffing, phishing and MITM are common within such scenarios. The attacks can lead to consumers being defrauded, for example by stealing credit card data information. They can also lead to leaking consumer private data, photos and conversations to cybercriminals for them to resell or reuse for malicious actions.

What are the risks of using public Wi-Fi?

- Packet sniffing or eavesdropping
- Malware infection
- Data breach
- Identity theft
- MitM attacks
- Unencrypted networks

Security best practices for Public Wi-Fi

- Do not use old and outdated devices and browsers that may be vulnerable and not properly updated to connect to Public Wi-Fi networks
- Do not leave your Wifi or Bluetooth connection ON, when you are not using it.

- Do not allow your Wi-Fi to auto-connect to networks
- Avoid using an open Wi-Fi network that is not password protected.
- Do not access websites that hold your sensitive information, such as financial or health care while connected to a public WI-FI.
- Avoid using public / shared terminals for accessing any websites that require input of any sensitive information.
- While using public / shared terminals make sure you logout from each portal that you have logged into. Clear your browsing history and delete the web cache before you leave the terminal.
- To stay safe on a public Wi-Fi network, use a Virtual Private Network (VPN) app.
- Enabling the firewall can save your laptop from suspicious data packets. Put simply, a firewall analyses the data traffic and protects your device from unauthorized access.
- Ensure that only HTTPS-enabled sites are visited.
- When you're through with an account, log out. Please do not leave your accounts signed in when they are idle.
- Enable Two-Factor Authentication
- Tell your staff about the risks of public Wi-Fi.

Conclusion:

It is very important to understand that Public Wi-Fi isn't secure and can be a gateway for hackers to access your device, data. Let us ensure we are aware of the overall risks and apply possible proactive steps to secure ourselves better.