TIPS & ADVICE

Risks of Using Public Wi-Fi

Today many, if not most, people carry some form of Internet-enabled device with them, whether it is a phone, laptop, tablet or some other technology. To get online, and avoid extra expenses by using a cellular connection, many opt to use free Wi-Fi Internet connections which are often widely available.

However, there are many potential risks involved in using public Wi-Fi. Users are often not aware of exactly whose network they are joining, what data they are sharing or how they may be subject to a cyber attack.

Whose network you are joining?

Anyone can set up a wireless hotspot and name it as they wish.
By setting their own network name (Service Set Identifier or SSID) to a common or commercially used SSID, someone running a rogue hotspot can attract connections from users who think they are joining a legitimate network.
Some devices will automatically join networks with familiar SSIDs.

Which networks are safe?

It is safest to assume that no public Wi-Fi is secure. Airports are particularly risky locations due to the high concentration of targets that may not have access to a domestic cellular network and may have an urgent need to get online.
Need often outweighs any perceived risk.

What are you agreeing to?

If you are asked to accept terms and conditions, ensure you read exactly what you are agreeing to. You may be agreeing to share more with your Wi-Fi supplier than you think.

What data are you sharing?

Any encrypted data sent through a Wi-Fi network can be monitored and collected. You may be potentially giving away information such as passwords, email content and web searches.

Risks and Attacks

ROGUE WI-FI NETWORKS. An attacker sets up a honeypot in the form of a free Wi-Fi hotspot in order to harvest valuable data. The attacker's hotspot becomes the conduit for all data exchanged over the network.

MAN-IN-THE-MIDDLE (MITM) ATTACKS. An attacker compromises a Wi-Fi hotspot in order to insert himself into the communications between the victim and the hotspot, to intercept and modify the data in transit.

PACKET SNIFFING. An attacker monitors and intercepts unencrypted data as it travels across an unprotected network.

ANYONE CAN BE AN ATTACKER. The tools required to carry out such an attack can often be easily obtained, therefore an attacker requires little technical experience or skill to carry out his criminal activities.

DATA IS A VALUABLE COMMODITY. Attackers can monetise many types of stolen data and therefore they seek information such as online banking credentials, Bitcoin wallets and other sensitive data that can be used in identity fraud.

Safety Considerations

DOS

Use a virtual private network (VPN) to keep your data encrypted in transit. They are quick and easy to use while providing you with privacy and safety.

Enable your firewall.

Turn off file sharing.

Look out for HTTPS in your browser bar - this indicates that SSL encryption is active and your communication is more likely to be secure.

Turn off the automatic connection feature within the Wi-Fi settings to prevent your device from connecting to public or open Wi-Fi networks without your consent.

DON'TS

Assume that a Wi-Fi network with a trustworthy SSID is genuine.

Share sensitive or personal data over a public Wi-Fi network unless you are sure the connection is secure. i.e. encrypted via HTTPS or a VPN.

Keep your software patched and updated.

Use anti-virus software and ensure it is up-to-date.

Created by Europol