CYBER CURE+
cyber security starts with us

December 8 2023

Evil elf-in-the-middle!

You can find free Wi-Fi networks in many places, from shops to airports to libraries. Free and convenient as it is, public Wi-Fi can also put businesses at risk of security breaches. Unfortunately, many public networks are not secure enough, so cybercriminals could get your private information, such as passwords, financial details, and personal data.

As a tech leader in your organisation, remind your staff of some important safety tips to follow when using business devices this holiday season.

87% of consumers globally have taken security risks on public Wi-Fi, such as accessing work and personal email, bank accounts or financial Information

2017 Norton Wi-Fi Risk Report: Summary of Global Results

Evil twin attack

An evil twin attack is where an attacker creates a fake Wi-Fi network that mimics a real one and tricks people into connecting to it. When this happens, the attacker can spy on and steal the users' data, such as their passwords, credit card numbers, or emails. The attacker can also direct the users to harmful websites or put malware on their devices.

Man-in-the-middle attack

A common way for hackers to exploit a public Wi-Fi network that is not secure is to use a man-in-the-middle attack. This lets them get between a device and the Wi-Fi connection and see the communication that goes both ways. They can do this without being noticed and steal any important data the company sends or receives over the network.

Encourage your employees to:

- Use a VPN when connecting to public Wi-Fi at places such as airports, libraries and cafes, to make sure the connections are made private
- Check for the pad lock or HTTPS in the website’s URL
- Turn off Wi-Fi auto-connect when connecting to free, public Wi-Fi
- Turn off Bluetooth and filesharing when not in use, to prevent attackers dropping malware onto devices