Cyber Security Awareness Foundation

PUBLIC Wi-Fi TIPS AND ADVICE

BE SAFE WHEN CONNECTING TO A PUBLIC Wi-Fi HOTSPOT

BE AWARE: Public Wi-Fi is inherently insecure — so be cautious.

REMEMBER ANY DEVICE COULD BE AT RISK: Laptops, smartphones and tablets are all susceptible to the wireless security risks.

TREAT ALL Wi-Fi LINKS WITH SUSPICION: Don't just assume that the Wi-Fi link is legitimate. It could be a bogus link that has been set up by a cybercriminal that's trying to capture valuable, personal information from unsuspecting users. Question everything — and don't connect to an unknown or or unrecognised wireless access point.

TRY TO VERIFY IT'S A LEGITIMATE WIRELESS CONNECTION: Some bogus links — that have been set up by malicious users — will have a connection name that's deliberately similar to the coffee shop, hotel or venue that's offering free Wi-Fi. If you can speak with an employee at the location that's providing the public Wi-Fi connection, ask for information about their legitimate Wi-Fi access point — such as the connection's name and IP address.

USE A VPN (VIRTUAL PRIVATE NETWORK): By using a VPN when you connect to a public Wi-Fi network, you'll effectively be using a 'private tunnel' that encrypts all of your data that passes through the network. This can help to prevent cybercriminals — that are lurking on the network — from intercepting your data.

AVOID USING SPECIFIC TYPES OF WEBSITES: It's a good idea to avoid logging into websites where there's a chance that cybercriminals could capture your identity, passwords or personal information such as social networking sites, online banking services or any websites that store your credit card information.

CONSIDER USING YOUR MOBILE PHONE: If you need to access any websites that store or require the input of any sensitive information — including social networking, online shopping and online banking sites — it may be worthwhile accessing them via your mobile phone network, instead of the public Wi-Fi connection.

PROTECT YOUR DEVICE AGAINST CYBERATTACKS: Make sure all of your devices are protected by a rigorous anti-malware and security solution — and ensure that it's updated as regularly as possible.