PUBLIC WIFI

None of us likes being detached from the internet, especially when its free! Public Wi-Fi can be a curse as well as a blessing. It is a potential gold mine of information from which attackers can gain information about you or your devices.

The security of public Wi-Fi should never be trusted.

You have no idea who else will be on the network with you.

Turn off your Wi-Fi when not in use.

When your Wi-Fi is enabled on your phone or laptop, it will constantly be broadcasting information about wireless networks to which it has previously connected. Using this information, it is possible to track where a device has been. It is also possible for an attacker to sneakily connect to your devices by impersonating any of the networks to which you have previously connected, e.g. your home Wi-Fi. From this, an attacker could now monitor any internet communication from your phone or laptop: email, instant messaging and downloads.

Don't access sensitive data

Do not access any sensitive information (like online banking or work emails) on public Wi-Fi. If an attacker can gain access to the same wireless network as you, it is easy for them to then view a large majority of websites you visit; they could also redirect you to other - more malicious - sites.

Consider using a VPN

A "Virtual Private Network" (VPN) can also be used for extra protection on public Wi-Fi and mobile data networks. A VPN creates an information tunnel between your device and the VPN server, which then forwards your data to the websites you wish to visit. This means that everything you access over the internet will be encrypted and secured from public Wi-Fi; even if the site doesn't use HTTPS.

VPN providers charge for this service, however there are comparison charts available to find the best deal. Ensure, when looking for a VPN service, not to use the free alternatives, as they could do more harm than good.

What if I must use public Wi-Fi?

If using public Wi-Fi is an absolute must, ensure websites have a padlock at the address bar. This sends everything encrypted over a protocol known as HTTPS (where the S stands for "secure") and makes it much harder for an attacker to read on your end. Remember also to check the URL for each website you visit to ensure you are on the correct, official sites.

The Cyber Resilience Centre for Greater Manchester