WHAT YOU NEED TO KNOW

Using Public Wi-Fi Hotspots

One of the great advantages of mobile devices such as tablets, laptops and smartphones is that we can use them to access the internet from just about anywhere. And many of us connect through public Wi-Fi hotspots in places like cafes, bars, airport lounges and hotels.

Some of these allow unsecured access which makes it especially easy for hackers to do things like infect your device, access your files, or steal your usernames and passwords.

Here are some things you can do to help protect yourself.

If possible, instead of using a public Wi-Fi connection, use a mobile data service such as 4G.

If you do connect through public Wi-Fi, make sure it’s to the correct network as hackers can set up bogus ones to fool us. If you’re not sure which one to use, ask a member of staff.

Configure your device so that it doesn’t connect you to an unknown Wi-Fi network without prompting you first.

You could also consider using a virtual private network or VPN service. These are becoming more common as they encrypt your data which makes it harder for criminals to access your information.

And if you notice anything suspicious, let the management know.

It’s a good idea to keep your operating system and applications up-to-date, but avoid updating when connected to a public Wi-Fi hotspot.

And remember that email, social media, online shopping, and banking services are just some of the applications which are likely to put you at risk as personal information is being sent over the connection.

Here are the main tips

- Use mobile data (4G) when possible
- Connect to an authentic network
- Consider using a VPN
- Report anything suspicious
- Update through a secure network e.g. at home
- Be especially careful with personal information