02476 998229
http://www.thegeekguys.co.uk

Staying safe on public WI-FI

By following the steps below should keep you more secure on public Wi-Fi:

1 Use A VPN

A VPN (virtual private network) will encrypt your traffic so that a hacker can't see your browser traffic at all. If you are going to do online banking or research something sensitive then you should definitely do this. However, if you are only going to browse the news then it won't be necessary.

2 Visit Secure Websites

If you are going to browse the website and cannot access VPN then make sure you visit websites that have a secure 'https' rather than http. This is safer.

3 Turn Off Wi-Fi When Not in Use.

It is wise to disable your Wi-Fi when you are finished working on your smartphone or laptop. Otherwise these devices can often be joining networks without your knowledge. Sometimes these networks are traps because of the name that has been used i.e. Free Wi-Fi. Your phone may think that it has been connected to it before when it never has.

4 Turn off File Sharing and Airdrop Options

By having your file share enabled in public space is like having your front door at home left open, anyone can come and look around. But instead of your house it is your computer. Your computer probably has some sort of file sharing options that assume that you are on a trusted network with other trusted computers. Make sure that file sharing has been switched off and enable the systems built-in Firewall. Also avoid having too many internets connected apps and services running. For Mac users set Airdrop to contacts only.