How to use public Wi-Fi securely

With the use of laptops and other mobile devices for work now commonplace, we have come to expect that we can work anywhere and access the systems and data we need from outside our usual work environment (perhaps an office) just as easily as when we are within it.

There is a general availability of free Wi-Fi wherever we are, whether that's on the train, in a café, public library or hotel. Some of these Wi-Fi networks require us to register to be able to use them but some just let us connect straight away (open networks). Even those that do require registration, don't always verify that you have a valid email address, i.e. they don't send you a verification code to submit before you can connect.

Why should I worry?

Should you be concerned about the security of these free networks? Unfortunately, the answer is yes. These Public Wi-Fi networks can potentially be used by cybercriminals to gain access to your personal information. They can do this in a number of ways, but typically they will all involve monitoring the network traffic and picking up the information you send, whether that's your account information, password or private conversations.

How do they do it?

Here are just a few of the ways hackers can take advantage of Public Wi-fi:

- ***Man-in-the-middle (MITM).*** The cybercriminal sets up a "secret agent" device between your laptop, tablet or smartphone and the Wi-Fi device. This allows them to 'eavesdrop' on what you are doing and they could even potentially redirect you to a fake site that will trick you into entering your security details.
- ***Evil Twin attack***. These are networks that pretend to be something else. Cybercriminals could create fake Wi-Fi networks to fool you into connecting, such as "Costa - Customer" without knowing that a hacker might be running it.
- ***Malware injection***. Silently installing malware onto your computer. This can then damage your system or provide hackers a backdoor to your files.

How can you protect yourself?

The two main ways are to piggy-back off your phone (tethering or mobile hotspot) or to use an application to secure your information (Virtual Private Network or VPN).

- **Mobile hotspot or tethering.** This is when you connect your laptop to your phone either with a cable (tethering) or through Wi-Fi (mobile hotspot). This will use the data included with your phone package (so could potentially result in an additional charge for extra data used) and uses a lot of power so can quickly drain your mobile battery. It's a good idea to have a charging cable with you just in case.

  See below for instructions to set up a mobile hotspot:
  - Android phones
  - Apple phones

- **Virtual Private Network or VPN**. A programme on your laptop that you connect to, which secures information in transit so that cybercriminals can't see what you are doing. We recommend you consider this option if you regularly work using public Wi-Fi.

How does a VPN work?

Virtual Private Networks (VPN's) reroute your data though a secure private network, managed by the VPN provider, and the data is encrypted between your device and decrypted when it leaves the VPN and arrives at your destination website.

Encryption is a way of scrambling data so that only authorised parties can understand the information. It uses a key to scramble it on your device and then to unscramble it at the other end. This means that should cybercriminals have access to the information you are sending, they won't be able to understand what it is, as it will be just random characters. Without access to the key, they won't be able to unscramble it.

Where do you get a VPN?

VPN software is available either from specialist VPN providers or is included with some Antivirus Security bundles. Generally standalone VPN's offer more functionality, some of which may not be required. Also be aware that some Antivirus VPN's, and some free/lost cost Standalone VPN's, limit the daily or monthly usage.

Costs provided are correct as of March 2023.

VPN Providers:

- NordVPN https://nordvpn.com/
  £3 per month (2yr contract), up to 6 devices at the same time, per account

- ExpressVPN https://www.expressvpn.com/
  £5.70 per month (1yr contract) up to 5 devices per account.

Antivirus Security Suite with VPN included:

Some examples of Security Suites that include a VPN as part of the package. Please check the features included with any security suite before purchase, as features can change from version to version.

- **Bitdefender Total Security**
  £35 first year from Bitdefender, 5 Devices. VPN limited to 200MB per day.
  Beware this product auto-renews at the full price of £80 per year.

- **Norton 360 Deluxe**
  £30 first year direct from Norton, 5 devices.
  Beware this product auto-renews at the full price of £85 per year.

- **Avast One**
  £27.99 first year from Avast, 5 Devices.
  Beware this product auto-renews at the full price of £80 per year.

The costs for Antivirus Security Suites above are when purchased direct from the provider. However, various discounts on Antivirus Security software are available from online resellers such as Amazon – for example you can typically find Norton 360 Deluxe £14, Avast One 10-devices at £17, Bitdefender Total Security at £20. It is also possible to not renew direct but to purchase a new product licence and apply that to your devices, but please be aware that you may need to reinstall the product for the new licence which will take added time.

Antivirus Security software is also available from Charity Digital Exchange, for qualifying non-profits – usually if you are a registered charity. Please check the product features before purchasing as only some of the available anti-virus bundles include a VPN, for example Norton 360 Deluxe does, but Norton Small Business does not.

How do you use a VPN?

How you use each VPN will depend on the software you are using, but typically you just need to start it and it should then connect and secure your connection across the available public Wi-Fi.

Some providers will offer an automatic connection when a public or unsecured Wi-Fi connection is detected and also provide a ‘kill switch’ to automatically disconnect the Wi-Fi if the VPN software disconnects or fails, which could otherwise potentially leave you unprotected.

With each product you should be able to configure which server or region to use (probably UK), and the auto-connect and ‘kill switch’ options.

To use a standalone VPN like NordVPN, you will need to first install the program. Then to use it - open the program and connect. You should be able to configure auto-connect options, so that the program would detect an unsecured connection and protect it as above.

For Antivirus Security bundles, you should see the VPN option in the control panel or dashboard. You should be able to manually switch it on and it will connect to the default VPN server and region.

And finally

Please note that when using a VPN, your internet speed will be slower than without a VPN. This is due to the encryption process and the speed of the servers that you are going through. The speed reduction will vary from provider to provider and it may be worth starting a trial to see which provider you are happy with, before committing to a contract, particularly if you plan to be working regularly from venues with unsecured public Wi-Fi.