Protect your information when using public Wi-Fi

Here are some ways you can protect your information when you are using public Wi-Fi:

- **Know who is providing the service.** Read the policies and information provided.
- **Don’t access your personal or financial information.** Always assume a public Wi-Fi network isn’t secure.
- **Log in or send personal information only to websites you know are fully encrypted.** To be secure, your entire visit to each site should be encrypted (meaning that the URL starts with https) — from the time you log in to the site until you log out. If you think you’re logged in to an encrypted site but find yourself on an unencrypted page, log out right away.
- **Don’t stay permanently signed into accounts.** When you’ve finished using an account, log out.
- **Don’t use the same password on different websites.** It could give someone who gains access to **one** of your accounts access to **many** of your accounts.
- **Use strong password.** Passwords are one of the biggest weak spots in the whole Internet security structure. A strong password is one that is unique and complex—at least 15 characters long, mixing letters, numbers and special characters.
- **Pay attention to warnings.** Many web browsers alert you before you visit a scam website or download malicious programs. Don’t ignore those warnings. Also keep your browser and security software up to date.
- **Install browser add-ons or plug-ins that can help.** For example, Force-TLS and HTTPS-Everywhere are free Firefox add-ons that force the browser to use encryption on popular websites that usually aren’t encrypted. But they still don’t protect you on all websites. Look for **https** in the URL to know a site is encrypted.
- **Keep ALL Antivirus, Antimalware, AD Blockers, Operating Systems etc Up To Date.** Internet security software cannot protect against every threat, but it will detect and remove most malware—though you should make sure it's to date. Be sure to stay current with your operating system's updates and updates to applications you use. They provide a vital layer of security.

What do we do to help keep you safe?

While using our Free WiFi Service we automatically implement services to help keep you safe while surfing the Internet, these include

Blocking Websites that fall outside of our allowed categories and do not meet the safe surfing guidelines as set out by the UK Governments Friendly Wi-Fi Service.

Automatic implementation of Googles Safe Searching rules

We block any websites or domains that are unclassified and we are unable to confirm the content type