Securing your Router & WiFi

If your router or WiFi is not secured, cyber-criminals could gain access to your home network. A hacker could access sensitive or private information, download inappropriate material, redirect you to fake websites and affect the speed of your connection.

What to do if you think your router has been compromised?

Scan your router for malware. Most anti-virus software can do this from your computer and will give advice about what to do next.

Contact your internet provider. Your internet provider may be able to provide further security support or replace the device.

Keep your router updated. Make sure to update your router to get the latest security updates.

How to protect yourself in the future?

Your router has a password to connect to the WiFi and a separate password to access the router settings (sometimes called the admin area). These both need changing from the default to something more secure. We recommend using **three random words**.

If possible, disable remote login for the router to prevent a hacker from remotely changing the settings.

If you can, also disable WPS (WiFi Protected Setup) as this can be an easy way for a hacker to access your router.

To make these changes you can access your router's settings using your computer or phone:

1. Connect to the WiFi as normal.
2. Open a web browser.
3. On the sticker on the back of your router should be either a "default access" address or the IP address of the device (this will commonly be http://192.168.0.1 but may depend on the make and model) – if neither of these are present contact your internet provider for help. Enter either of these into the address bar on your browser to go to the settings menu for your router.
4. Find the security settings menu to change the passwords – you can refer to the user guide that came with it or ask your internet provider for assistance.

Make sure that your router is kept up to date. Most routers from internet service providers do this automatically but you can search for instructions online for your make and model.

Keep your WiFi passwords safe so others cannot access or use them without your permission.

Regularly check any connected devices and investigate any you don't recognise.

METROPOLITAN POLICE