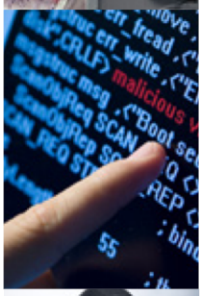
Crime prevention advice for

Wi-Fi Safety



Wi-Fi is now everywhere; whether it's at home, work or public places such as the gym, coffee shops or airports. The degree to which these are secure depends on a number of factors and where these are located. If they are at home or work they are likely to be more secure than using public Wi-Fi. With all forms of Wi-Fi however there is some degree of risk:

Home/Work

- If your Home or Work internet is not secure it could mean that others have access to your internet allowance/connection, slow down your connection, or even worse, access the (sensitive) information which you are also accessing and steal this.

Securing your wireless network:

- Ensure your network is password protected
- Change the default password
- Check the encryption level of the router – WPA2 as minimum

Public Wi-Fi

- The risk with Public Wi-Fi comes with the fact that many do not require a password to access them and if they do, you do not know who else is using the connection.

Risks

- Anyone could be connected to the router at the same time as you, watching what you do.
- A criminal may set up a spoof hotspot which you connect to thinking it is a legitimate Wi-Fi connection when in fact all your traffic is going through their computer for them to read.

Safely using Public Wi-Fi

- Do not send personal information over Public Wi-Fi unless you know it is a secure webpage.
- Use reputable hotspots where possible.
- Businesses who want to access their corporate network should use a Virtual Private Network (VPN).

Remember:

- Business information can also be stolen by shoulder surfing.
- Don't leave devices unattended.
- Use anti-virus, firewall, passwords and update these regularly.