You can check out more useful publications and eSafety guides on the Hub or Moodle and around the LMC campus.
Contact Computer Services for any help with this or any other IT related issues.

If you feel unsure about your data storage or its security or need more help and advice then you can talk to your Course Tutor, Computer Services or Student Services

Online advice is also available at

www.thinkyouknow.co.uk

Lancaster & Morecambe the College

Stay Safe @ LMC

Computer Services eSafety Series

Using Wireless Networks

Lancaster & Morecambe the College

Stay Safe @ LMC

About Wireless Networks

Access to wireless networks (Wi-Fi) is becoming more commonplace and the number and types of devices (laptops, i-Pads, Mobile Phones, tablet pc's etc.) that can take advantage of this access is growing. Wireless access points are available at home and in public places like libraries, town centres, at college as well as in hotels and airports all across the world. However, there are a few things you should know about Wi-Fi networks if you choose to use them.

Wireless security

In general Wi-Fi connections are provided as **Secured** (authenticated access) or **Unsecured** (open access). You can quickly check the security status of wireless networks that have been detected by your device by looking at the wireless connections. On a Windows 7 pc you simply need to look at the signal strength icon in your task bar by left clicking on it and looking at the pop-up list of Wi-Fi networks that it has detected. The **unsecured** networks have a small yellow shield symbol next to them with a black "!" in the middle which signifies that this connection is **NOT** secure.

However, you may be still be prompted to enter login details to access an unsecured network (as you are on the Visiting Student Wi-Fi service at college) as this allows you to see secured resources whilst still protecting your network user name and password when you login.

Good Practice

- Do check if the Wi-Fi network is secure or not **BEFORE** connecting to it.
- Only use **unsecured** networks if you have to.
- Don't log into your personal accounts with your userID and password if the Wi-Fi network is NOT secure . . . . even if the web page you log into is secure, e.g. your bank's website.
- Do make sure your device is protected with Anti-virus - there are plenty of FREE versions available.
- If you suspect that someone is watching you whilst you are using a Wi-Fi connection then disconnect and try again elsewhere or later if necessary.
- Do disconnect from an unsecured Wi-Fi network when you are done with it to help prevent unauthorised access to your device.
- Do configure your device NOT to Automatically connect to unsecured Wi-Fi networks if possible so that **YOU** have the choice about what your device connects to.
- Do be aware that any unsecured Wi-Fi access is a soft target for the bad guys.
- If you suspect that your password has been discovered then change it as soon as possible.
-
- If you are unsure about anything in this topic then please ask or seek further advice.