

Are you using a Wireless Router? Is it Secure?

A friend on a visit to a hotel found that they had no wireless broadband, so he got in his car, drove round for about 10 minutes until he found an unsecured network. Then spent half an hour checking his e-mail. The intent was not malicious, all be it that their actions were illegal. But if their actions had been more sinister just what could they have done?

Once on someone else's wireless network what can you do?

Well you could:

- Access files in any shared folders on the PCs in that household or office if they are connected to the broadband router, via wires or wireless and even put files onto those PCs.
- Send anything to their printers (if shared) that will print out when they turn their printer on.
- Use that broadband connection to download files, browse dubious websites, or send SPAM e-mails.
- Infect the PCs with viruses or a key logger program.

There are a number of simple steps to protect yourself when setting up a wireless router.

1. Make sure that your wireless connection is encrypted using WEP or WPA (stronger).
2. Pick an encryption pass phrase that is not easily guessed, ideally with numbers and letters.
3. Change your router login to something other than default.
4. Disable access to the router management pages via wireless connections.
5. Do not use a wireless name (SSID) that could identify yourself, your location or the make and model of your router.

By implementing the above you stop people stealing your bandwidth and accessing your personal data.