

FACTSHEET

Securing your Wireless Network



Background

The affordability and ease-of-use of wireless networking technology has made it a popular feature in many business ICT systems, allowing flexible access to files and communications resources without needing to 'plug in' to the network.

Securing wireless networks is therefore of paramount importance. Being so 'easy to connect to' is a double-edged sword for organisations deploying a wireless network. Without appropriate safeguards, wireless networks can be maliciously abused with dire consequences for the organisation concerned.

The Potential Risks

An unsecured wireless network can be easily compromised in the following ways:

- Hackers can access any sensitive files on your entire network, in the same way as if they were sat inside your premises at a workstation.
- Malicious individuals can launch viruses, spyware and other harmful code into your ICT system.
- Rogue users can use your expensive Internet connection without your knowledge, using up the bandwidth you've paid for and possibly visiting illegal websites and conducting illegal activities while 'looking like it's you'.

Seven Steps to Protection

There are numerous straightforward and inexpensive measures you can take to secure your wireless network and enjoy its benefits without risk.

1. Configure your wireless access points to 'turn-on' the in-built encryption feature. Consult the instruction manual or contact the manufacturer online for an easy guide to doing this yourself in minutes. Most wireless access points will use 'WPA2' encryption which is strong enough to repel almost all attacks.
2. Configure your wireless access points to 'hide' or 'randomise' the ID name it uses to distinguish itself to users. Call it something that doesn't associate it to you, your business or your location. Again, this is simple to do.
3. Configure your wireless access points to a unique password. All new access points come with a default password like '1234' or 'password' that most people never change. These are well known to hackers and - when overcome - give them complete control over the device. Make sure you change the default password to a secret password containing characters and numbers, and change it regularly.
4. Ban employees from adding new access points to the network without prior management authorisation. Without this disciplined approach, your entire ICT system could be undermined by a single insecure access point.
5. Position wireless access points carefully to avoid areas outside your premises from being 'broadcasted' to. This will make it much harder for people to access your wireless network unless they are within the confines of your business. This process



can be refined by configuring the signal broadcast range/direction of individual access points.

6. Strictly control the users allowed to connect the wireless network. Avoid sharing crucial passwords and configuration information with colleagues, employees and contractors who don't need to know it. Think carefully about the ramifications of allowing guests to access your wireless network when they visit your business.
7. To fully exploit the many advanced benefits of wireless networks safely, consult a qualified ICT advisor with expertise in information/network security. They will be able to advise on a solution appropriate to your needs and budget, and how a strategy for securing your wireless network should fit alongside a broader security strategy for your entire ICT system, including anti-virus, firewall, VPN and other protection measures.