WIRELESS NETWORKS SECURITY ISSUES

All flavours of the 802.11 standard are susceptible to a number of security vulnerabilities.

As wireless networks use radio waves, anyone with the right equipment and know-how could tap into your network from outside your building (or from another office within a shared building). It is possible to *encrypt* data travelling across a wireless network using a technology called Wired Equivalent Privacy (*WEP*). However this and other security settings are often disabled by default on wireless equipment. Added to this, WEP itself is not completely secure.Look out for newer products which use a system called WiFi Protected Access (*WPA*). WPA promises much improved security over WEP. However, it is possible to undermine the added security afforded by WPA if it is not set up correctly. For example it is important to use a good choice of password and security keys to reduce this possibility. It is possible to upgrade some current wireless Network Cards to incorporate WPA - see your manufacturers site for details.
WEP and WPA may provide adequate security for home wireless networks when used in conjunction with other security measures. For office wireless networks, additional measures will need to be taken to ensure security. Virtual Private Network (VPN) technology used in conjunction with wireless networking may provide a solution (see the knowledgebase article Virtual Private Networks for more on this). Basic precautions that should be taken to prevent casual access to a wireless LAN include:

- Enable Wired Equivalent Privacy (WEP) at the highest setting - whilst this does not guarantee security it's worth having.

- Use WPA if available in preference to WEP.
- Set up access points to allow access to known network cards only (each network card can be identified by a number called a MAC address)
- Change the default SSID (Service Set ID or network name) and encryption keys. The SSID is the name by which an access point indentifies itself. Using the default SSID suggests to hackers that the rest of your setup is default, making your network a likely candidate for intrusion attempts.
- Turn off broadcasting of the SSID. This makes it much harder for people to find your network, but you must tell your users what the SSID is so they can connect.
- Using a firewall to protect all connected PC's (see the knowledgebase for more on firewalls)
- Install antivirus software on all networked computers, and keep it updated.
- Set up network drives and folders with different access rights for different users - password protect files and folders if necessary.
- Put your wireless access point in the middle of the building, to minimise leakage outside.

For more on general computer security issues see the knowledgebase article Safe and sound - keeping your computers and data secure.

Source: http://www.ictknowledgebase.org.uk/wirelessnetworks