# Wireless Network Security

The biggest mistake people make when setting up their wireless network is overlooking the importance of the security features. If the security features on your wireless network are not activated properly, you will be at risk from invasions, attacks and viruses. In the hurry to get connected many people overlook simple steps to ensuring the network is protected. Often the process of configuring security settings on a WLAN computer is slow and complicated. However, these features are required for a reason and that is to protect your computer from potential problems.

Most WLAN setups include accessing an external page in order to activate the access point or router. These pages are protected by a login and password and the user will be required to input information such as network address and account details. Problems occur when the owner does not change the default login and password. For skilled hackers details like login names and passwords are easy to obtain. When setting up your WLAN always change your login and password immediately.

All wireless networks are connected with a default Service Set Identifier (SSID) this is a signal broadcast online at repeated intervals. The feature was originally designed for businesses so that WLAN clients could come and go more efficiently. In the home this feature is redundant and exposes the network to unwanted visitors. Your network administrator can disable this feature to tighten security and prevent leakages.

Another potential security risk is the position of your router or access point. While small leakages outside the home are fine, the further the signal reaches the higher the chance for exploitation. Install your access point or router near the center of the house rather than by windows. This will minimize the signals reach outside the home.

Hackers can break into your network anytime unless the computer is off. When you are not using your WLAN turn off all the connecting devices, this will ensure your computer is safe and not transmitting leakages. It may not be practical for you to do this all the time but you should consider shutting down completely if you are away for extended periods.

The most effective way to avoid common problems associated with WLAN is to follow the security instructions and set up to the letter. It might take a little longer to get hooked up but it is essential for the security of your computer.