How To Secure Your Wireless Network

There is something you should realize. Working from home while using a wireless local area network (WLAN) may lead to theft of sensitive information and hacker or virus infiltration unless proper measures are taken.

People have more flexible time due to wireless network. Thanks to the invention of wireless. People can now work from home while taking care of their kids or doing house works. No more stress from traffic jam anymore. Is this great?

Well, there is something you should realize. Working from home while using a wireless local area network (WLAN) may lead to theft of sensitive information and hacker or virus infiltration unless proper measures are taken. As WLANs send information over radio waves, someone with a receiver in your area could be picking up the transmission, thus gaining access to your computer. They could load viruses on to your laptop which could be transferred to the company's network when you go back to work.

Believe it or not! Up to 75 per cent of WLAN users do not have standard security features installed, while 20 per cent are left completely open as default configurations are not secured, but made for the users to have their network up and running ASAP. It is recommended that wireless router/access point setup be always done though a wired client.

You can setup your security by follow these steps:

1. Change default administrative password on wireless router/access point to a secured password.

2. Enable at least 128-bit WEP encryption on both card and access point. Change your WEP keys periodically. If equipment does not support at least 128-bit WEP encryption, consider replacing it. Although there are security issues with WEP, it represents minimum level of security, and it should be enabled.

3. Change the default SSID on your router/access point to a hard to guess name. Setup your computer device to connect to this SSID by default.

4. Setup router/access point not to broadcast the SSID. The same SSID needs to be setup on the client side manually. This feature may not be available on all equipment.

5. Block anonymous Internet requests or pings. On each computer having wireless network card, network connection properties should be configured to allow connection to Access Point Networks Only. Computer to Computer (peer to peer) Connection should not be allowed.

Enable MAC filtering. Deny association to wireless network for unspecified MAC addresses. Mac or Physical addresses are available through your computer device network connection setup and they are physically written on network cards. When adding new wireless cards / computer to the network, their MAC addresses should be registered with the router /access point. Network router should have firewall features enabled and demilitarized zone (DMZ) feature disabled.

All computers should have a properly configured personal firewall in addition to a hardware firewall. You should also update router/access point firmware when new versions become available. Locating router/access point away from strangers is also helpful so they cannot reset the router/access point to default settings. You can even try to locate router/access point in the middle of the building rather than near windows to limit signal coverage outside the building.

There is no guarantee of a full protection of your wireless network, but following these suggested tips can definitely

lessen your risk of exposing to attackers aiming at insecure networks.

Short note about the author

George Williams maintains many websites about network security, including http://www.wirelessservicesecrets.info.
