



Article published on March 5th 2012 | [Computer](#)

Computers have become integral part of modern lifestyle. It has become a basic necessity and a life without computer is unimaginable. Computers have invaded into every section of life and have made lives simpler and better. You do not need to stand in long queues for appointments as communication has become lightning fast. On one click of mouse you can perform tasks that took considerable time and efforts a couple of decades ago. People world-wide are connected with each other and can communicate directly using internet.

This connectivity can be by means of cables or by wireless connections. In wireless connection the service provider gives you access to internet without using cables. You have freedom to move freely and use internet in a limited area. But this type of connection is prone to hackers who can get access to your personal information by invading your wireless connection space. Here are some steps to ensure wireless security.

• **Change The System ID:** Wireless equipment comes with a default system ID called SSID (Service Set Identifier) which is easily traceable by hackers. Change this ID and give it a secure and peculiar name. Your new password should not be obvious like your name or last name. Some digits and symbols should be used to ensure safety.

• **Encrypt Your Data:** At times you have to send some confidential data to someone and you do not want anyone else to get access to this information. This is where encryption comes into play. WPA (Wi-Fi protected access) and WEP (Wired Equivalent Privacy) encrypt your data and only your intended recipient can open it. Although there are still chances that wireless hackers invade your network, encryption can keep your data safe from casual wireless hacking.

• **Disable Identifier Broadcasting:** Disable identifier broadcasting from your device. It sends an open invitation to hackers and they can invade your personal information easily. Look up in your device manual for the procedure to disable broadcasting.

• **Change Administrator Password:** All hardware and software come with default passwords which are easily cracked by hackers. Change the default password with a not so easily guessable password. A lot of people do not take this simple step and fall prey to hackers.

• **Manage Traffic:** give access to only desired people who you want to connect to. You can configure your router with the help of hardware manual. It provides an extra shield to your data as it restricts unwanted people to get access.

• **Anti-virus Software:** A large variety of anti-virus software™s are available in the market. Subscribe to any good one and keep it updated. Updated software™s are important because new viruses are discovered every now and then and software companies upgrade their antivirus software to counter them.

Hackers are always looking for a chance to get access to your private information. While some of them do it for fun others may use it to rob you of your money. Keep yourself updated with new advances in the field of network security to counter the moves of hackers.

Article Source:

<http://www.articleside.com/computer-articles/beginners-guide-to-keep-wireless-connection-safe.htm> -

[Article Side](#)

[Elissa Joyce](#) - About Author:

Hackers can do serious damage if you do not take proper a [Wireless security](#) measures. For further assistance you can visit [trainace.com](#)

Article Keywords:

wireless hacking, wireless security

You can find more [free articles](#) on [Article Side](#). Sign up today and share your knowledge to the community! It is completely FREE!