Title:
Making Sure Your Wireless Home Network Is Secure

Word Count:
770

Summary:
As more and more people make the switch from wireless networks to secure networks in their homes, there are a whole new range of security issues to be aware of. Too often people set up their wireless network and forget about the security implications.

Keywords:
network security

Article Body:
As more and more people make the switch from wireless networks to secure networks in their homes, there are a whole new range of security issues to be aware of. Too often people set up their wireless network and forget about the security implications.

However, this can be a serious oversight as people can easily access your personal information and is a common cause of fraud. In this article we advise you on some of the steps you can take to make sure your wireless network is secure.

Almost all computers with recent operating system and wireless capabilities will have the option to turn on a built in firewall. If you are using an older operating system you may want to install a third party firewall. Although this alone will not stop third parties from accessing your network, it will act to secure each computer on the network from unwanted network requests.

Creating secure user accounts is also advisable. Weak username / password combinations are exploitable should a hacker try to gain access to your networked computer via your wireless network. Stronger passwords will generally contain mixed case alphanumeric characters. You can easily find advice on writing secure passwords on the internet.

Most wireless routers allow you to access their configuration with your web browser. Be sure to change the default username and password that allows you to administrate your router to prevent unwanted access. If you do not, almost

anyone could breach your network.

In addition, every network capable computer will have at least one MAC address that identifies it on your network. Granting access to your wireless network based on MAC addresses will filter out unwanted users and network capable devices. It is not foolproof, but it will discourage most would-be hackers.

Wireless routers also broadcast an SSID which is basically a name of the network that appears when a computer picks up its signal. By default, this will usually be the name of the manufacturer of your wireless router. Many companies identify their networks using the SSID and it can be a handy way to identify Wi-Fi hotspots when you are out and about. However, for the sake of your home network it is not really necessary so it is a good idea to stop broadcasting it entirely.

It should also be possible to encrypt the data that is sent between computers on your wireless network. However, you must ensure that all computers have the same encryption settings.

One of the main reasons that wireless home networks can have security issues is because the signal can often reach beyond the boundaries of your home. One major financial institution recently lost millions of credit card records because it did not have its wireless system properly secured.

Another method that is commonly used to secure wireless networks is static IP addressing. IP addresses are often assigned automatically on wireless networks. However, networks are much more secure if the IP addresses of all computers on a network are set by hand. This is not foolproof but will keep out casual hackers.

If possible, place your wireless router in a part of your house or apartment where the signal will not travel too far beyond the boundaries of your home. If your home overlooks a street, do not put your router too close to this part of your home. In addition, if you are going on vacation or are going to be away for an extended period of time you should turn your router off while you are gone.

Even if you do not have a wireless network in you own home, it is important to know how to keep your notebook secure when you are out and about. You should make sure that your notebook does not auto-connect to other wireless networks. By default, both Windows and Mac OSX will display a warning before connecting to unknown networks and both will allow you to identify which networks you trust for automatic connection. When you are connecting to outside networks that you do not know, make sure that your firewall is turned on.

Too many people overlook the importance of securing their wireless networks. The steps outlined above should not take long to implement. While they may not guarantee 100% security, they are likely to deter any would-be hackers.

These are just some of the steps you can take to make your home wireless network more secure. There are millions of networks out there that are very poorly protected so if you take the time to put even a few of these safeguards in place you will most likely deter any would-be hackers.