Wireless Routers for Homes; are they Even Safe to Use?

by Eccuni

Article published on December 23rd 2011 | Internet

Many are wondering if wireless routers they use in their homes are safe to use and if there are any risk if other people uses their internet connection. Indeed, wireless routers may offer free internet to some, but because of this fact, some people with dark intentions in mind can exploit this opportunity.

Hijacking Connection

Computer forensics says that someone can use your wireless internet connection to attack other computer networks. Hackers would prefer to use others internet connection, instead of theirs when they attack a particular target. Although, hackers can mask their connection, details and location, but it is much safer for them to use other's internet connection. That way, the hacker will not be blamed for the attack he made, thus making him anonymous.

Attack the Computer and the Network

Despite the fact that there are new types of computers and operating systems, some people are still using ancient computers and operating systems on their homes, much worse, they have no decent protection against virus and malware. These types of computers are the easiest to penetrate. Once these computers are penetrated via the wireless network, hackers can then secretly install a Trojan. It can be used to transmit important information of the target, such as credit car information, banking information and etc. Hackers can use this information for their advantages unknown to their victims.

The Zombie Computer

If zombies are scary, then a zombie computer would be scarier to digital computer forensics and security experts. The hijacked connection will be used to perform a specific attack on a specific time. A computer turned zombie can be used repeatedly by a hacker, through the installation of software. The software installed can be used to coordinate attack, if there are more zombies the hacker controls then that could be more dangerous.

Data Storage

There are instances when hackers will need a place to hide the data they have stolen. And what is the most suitable storage place to use? It's a computer with wireless connection. The data is masked perfectly that only graduates of computer forensic course can detect them. The data is hidden well that it is not visible to the desktop's user and the disk space will seem not used. Knowing how this happened will be very troubling.

The Bandwidth

Hackers will even use the bandwidth or connection of the one owning wireless connection to upload or download huge amounts of computer data. These types of files can be in Gigabytes and could lead to additional bills for that person's internet connection.

Violates Privacy

No person with healthy state of mind would like someone activating their microphone just to listen to

the conversations inside the house. Or activate the camera to see what is inside the house. If hackers are planning to hack a company, then hacking the privacy of certain officials would surely help their cause.

How to Protect The System

It is important to protect the wireless system against hackers. First thing to do is configure the firewall of the operating system, so that there are some levels of protection. It is also possible to purchase firewalls to supplement or replace the current firewall of the system. Although they are hard to configure, there are manuals that would provide a step-by-step guide in how one could configure their firewall.

The second thing to do is install the latest antivirus software; an antivirus software that has anti-hacking capabilities. It is important to know how to effectively use the software, since there are other things aside from protection anti-virus software can offer. There are many good anti-viruses in the market, such as Kapersky, Norton and others.

Turn off the router or the internet connection when the computer is not used. If there is a need to store important information like details in bank accounts, passwords or any other private information, store it on other secure media or in a secure external drive that will make the data encrypted so that the hacker cannot retrieve it. Sometimes routers will provide security features and encryption, thus it is much better to know how to make use of this. Of course, the hardware will provide manuals that will guide their users on how to activate and configure the security features of the router. It might be confusing at start, but it is worth it.

Article Source:
http://www.articleside.com/internet-articles/wireless-routers-for-homes-are-they-even-safe-to-use.htm - Article Side

Eccuni - About Author:

The International Council of E-Commerce Consultants (EC-Council) is a member-based organization that certifies individuals in cybersecurity and e-commerce. It is the owner and developer of 20 security certifications. EC-Council has trained over 90,000 security professionals and certified more than 40,000 members. These certifications are recognized worldwide and have received endorsements from various government agencies. They also offer trainings in computer forensics.

More information about EC-Council is available at www.eccouncil.org, a Computer forensics, a digital computer forensics, a computer forensic course

Article Keywords:
Wireless Routers, computer forensics, computer forensic course, digital computer forensics, wireless internet, hackers, anonymous, virus, malware, Trojan, credit card, banking information, victims, security experts, firewall, antivirus software, anti-hack

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