Title:
Checking Computer Security

Word Count:
615

Summary:
Many people wonder whether or not their computer is secure. They fear that someone might be looking through their files, copying, altering, or erasing them. They are uneasy about the thought that someone might be monitoring their every move in cyberspace. These concerns come to mind when reminded of the problem of hackers, viruses, and other security risks that abound in the Internet. Fortunately it’s easy to prevent these problems by following a few simple tips.

Update

...

Keywords:

Article Body:
Many people wonder whether or not their computer is secure. They fear that someone might be looking through their files, copying, altering, or erasing them. They are uneasy about the thought that someone might be monitoring their every move in cyberspace. These concerns come to mind when reminded of the problem of hackers, viruses, and other security risks that abound in the Internet. Fortunately it’s easy to prevent these problems by following a few simple tips.

Update

Perhaps the most important step for computer security is to keep it updated. Install the latest critical updates and service packs from Microsoft's download center. This is made easy by configuring the system to utilize Automatic Updates, if available. If not, updates can be downloaded directly from Microsoft's download center. Currently, Service Pack 2 (SP2) is the most current Service Pack for Windows XP.

Firewall

The easiest way to increase the security level of a computer is by using a firewall. Firewalls monitor all activity that occurs on a connection between one or more computers. They act as a "wall" with one or more computers on one side, and one or more computers (usually the Internet) on the other. Information transfer by suspicious programs are immediately cut off, preventing them from entering the protected side of the firewall. This way denying access to anything coming from unauthorized and unknown sources prevents possible infection by viruses, worms, and other malicious codes.

Anti-Virus and Anti Spy-ware

Even if a computer is protected by a firewall it is still necessary to use anti-virus and anti spy-ware. This is because a firewall only prevents unauthorized outside access, and cannot distinguish between malicious and benign access. It is still possible to inadvertently make a request for information that is harmful, which the firewall views as an authorized transfer. Anti-virus and anti spy-ware provides another layer of armor for a computer, making it harder for hackers and their malicious programs to penetrate and control a computer. Some well-known anti-virus programs include Norton, Trend Micro PC-cillin, and McAffee. Anti spy-ware programs are also important as they reduce the chances of spy-ware getting into a computer. Spy-ware behaves differently than viruses, making it necessary to use different programs to catch it. Spy-ware can monitor any activity a computer infected with it performs, or even act as a gateway to download additional spy-ware or viruses. Hackers typically use spy-ware to obtain important information that must remain confidential like credit card numbers, social security numbers, and police records.

Protect Home Networks

It is possible for a computer owner to be unaware they are using a network at home. If more than one computer shares the same Internet connection or if wireless Internet access is being used, a home network is present. Securing a single computer is not much use if it is part of a network. The whole network must be protected as well to prevent malicious software from simply hopping from computer to computer to avoid attack. Different kinds of home networks face different kinds of risks. In the case of a wireless connection, anyone within the broadcast range of the network may be able to look at any data contained within the network.

Most networking devices employ their own security mechanisms. Using this in combination with security defenses installed on each computer's should provide enough protection to thwart attempts from hackers to hi-jack the network and use

the computers connected to it. Most routers function as Network Address Translators (NAT) which makes them a safe connection to the Internet.

While no measure can guarantee total immunity from attack, these steps should increase the security of a computer or network enough to protect against any typical attack.