EXCLUSIVE REPORT

COMPUTER SECURITY CRACKDOWN

Protecting Your Computer System From Security Threats

Computer Security Crackdown

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.

With the rise of digital technology, and high speed Internet, it's a safe assumption to make that most people are constantly connected to the Internet. Often times computer users leave themselves WIDE open for attack from a cybercriminal.

If you're unprepared, and you are taken by surprise – this could be the beginning of a long series of attacks and the risk of having your personal information and accounts compromised as well.

Fortunately it’s easy to prevent these problems by following a few simple tips.

Keep Your Security Software Updated

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, Windows XP is no longer supported with updates for Microsoft. The most up to date you can get with Windows security nowadays is with Windows 10. They have recently announced that Microsoft will stop supporting updates for even Windows 7 as well in the very near future.

When it comes to Microsoft security, if you're running anything older than Windows 10, your best course of action is to ensure that you have anti-virus and anti-malware software included. You should also always make certain that this software is up to date with the most recent security patches for worms and viruses.

It's also very important to have a firewall in place to protect your computer from outbound attacks and other malicious cyber-criminals. In the next section we will discuss the firewall more in depth.

Implementing A 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.

A lot of operating systems have built in firewall defenses now so that you technically don't need any outbound or additional software in order to protect yourself.

However, at the same time, many of the anti-virus and security suite software bundles come with a passive firewall integrated, and you can either choose to enable this or disable it. When this is enabled, be aware that some of these are very aggressive in how protective they are over every application that opens on your computer. Because of this, you often need to add a number of “exceptions” for software that you frequently use.

Firewall's are actually quite important, which is why most operating systems have them automatically built-in. If you were to look at the traffic that pings and checks your network everyday for opening in your security, you would be amazed (and probably horrified as well).

Anti-Virus and Anti-Spyware

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.

Spyware behaves differently than viruses, making it necessary to use different programs to catch it. Spyware 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.

Conclusion

Securing yourself and your computer from digital attacks is a lot easier than it may seem.

More often than not, companies and even “pop ups” will warn you of attacks, and try to pressure you into installing this kind of protection software or that kind. It's important that you do your due-diligence any time you see a product or software that you are recommended or that you intend to use.

On the other hand, following the tips in this guide, you should now have a better understanding of the cyber and digital world and it's potential threats. You should also now be able to determine your next move, as in which kind of security aspects you need to improve upon to keep yourself safe.

All-in-all, don't be the person that believes they could never be under attack. You would be baffled at the amount of hackers out there scanning for openings in your network.

Follow the details and information in this guide, and get yourself secure today!