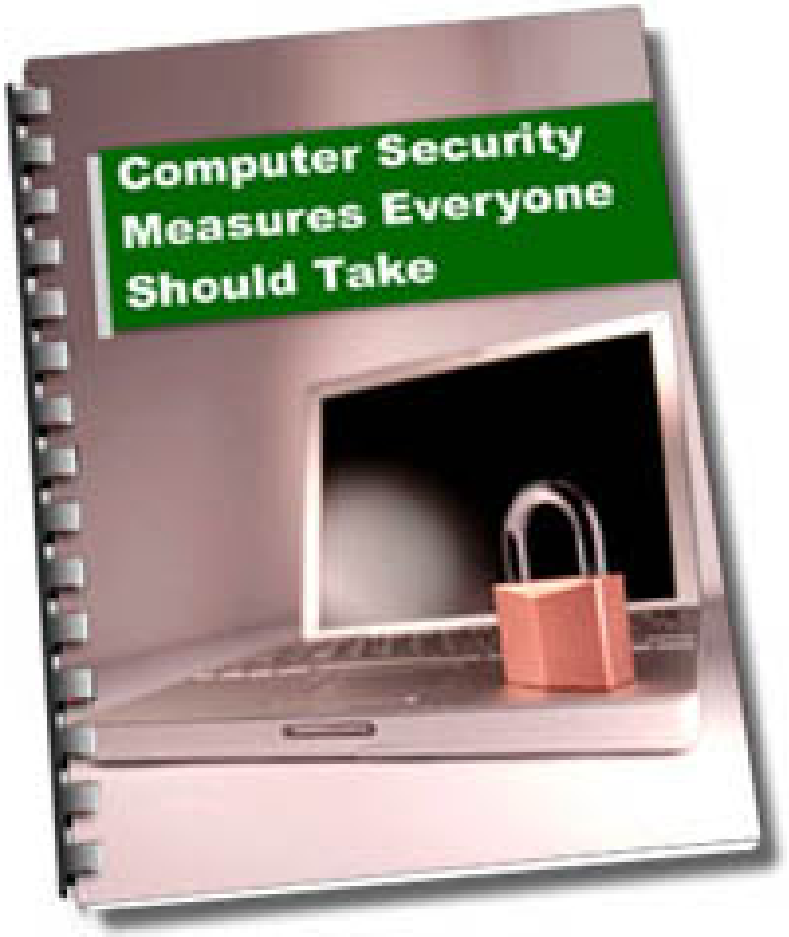
This Report Brought To You By:

Anna Williams

Websites and Webhosting

Visit Us At: http://www.websitesandwebhosting.com

Get Your FREE Butterfly Reports Account Now - http://ButterflyReports.com/axz/affiliate.php?id=18024



1. Securing Your Computer System

Today, more and more people are using their computers for everything from communication to online banking and investing to shopping. As we do these things on a more regular basis, we open ourselves up to potential hackers, attackers and crackers. While some may be looking to phish your personal information and identity for resale, others simply just want to use your computer as a platform from which to attack other unknowing targets. Below are a few easy, cost-effective steps you can take to make your computer more secure.

1. Always make backups of important information and store in a safe place separate from your computer.

2. Update and patch your operating system, web browser and software frequently. If you have a Windows operating system, start by going to www.windowsupdate.microsoft.com and running the update wizard. This program will help you find the latest patches for your Windows computer. Also go to www.officeupdate.microsoft.com to locate possible patches for your Office programs.

Get Your FREE Butterfly Reports Account Now - http://ButterflyReports.com/axz/affiliate.php?id=18024

3. Install a firewall. Without a good firewall, viruses, worms, Trojans, malware and adware can all easily access your computer from the Internet. Consideration should be given to the benefits and differences between hardware and software based firewall programs.

4. Review your browser and email settings for optimum security. Why should you do this? Active-X and JavaScript are often used by hackers to plant malicious programs into your computers. While cookies are relatively harmless in terms of security concerns, they do still track your movements on the Internet to build a profile of you. At a minimum set your security setting for the “internet zone” to High, and your “trusted sites zone” to Medium Low.

5. Install antivirus software and set for automatic updates so that you receive the most current versions.

6. Do not open unknown email attachments. It is simply not enough that you may recognize the address from which it originates because many viruses can spread from a familiar address.

7. Do not run programs from unknown origins. Also, do not send these types of programs to friends and coworkers because they contain funny or amusing stories or jokes. They may contain a Trojans horse waiting to infect a computer.

8. Disable hidden filename extensions. By default, the Windows operating system is set to “hide file extensions for known file types”. Disable this option so that file extensions display in Windows. Some file extensions will, by default, continue to remain hidden, but you are more likely to see any unusual file extensions that do not belong.

9. Turn off your computer and disconnect from the network when not using the computer. A hacker can not attack your computer when you are disconnected from the network or the computer is off.

10. Consider making a boot disk on a floppy disk in case your computer is damaged or compromised by a malicious program. Obviously, you need to take this step before you experience a hostile breach of your system.

RECOMMENDED PRODUCTS:

Win-Spy Monitoring Software

Monitor Your Home Pc Or Any Pc Within Network.

Noadware.net - Spyware/Adware Remover

Remove your Adaware and Spyware with this amazing piece of software.

2. Trojan Horse: Greek Myth or Computer Nemesis?

We have all heard the term Trojan Horse, but what exactly is it? A Trojan Horse is a destructive program that masquerades as a harmless application. Unlike viruses, Trojan Horses do not replicate themselves, but they can be just as destructive. One of the most dangerous examples of a Trojan is a program that promises to rid your computer of viruses but instead introduces viruses into your computer.

The Trojan can be tricky. Who hasn't been online and had an advertisement pop up claiming to be able to rid your computer of some nasty virus? Or, even more frightening, you receive an email that claims to be alerting you to a new virus that can threaten your computer. The sender promises to quickly eradicate, or protect, your computer from viruses if you simply download their "free", attached software into your computer. You may be skeptical but the software looks legitimate and the company sounds reputable. You proceed to take them up on their offer and download the software. In doing so, you have just potentially exposed yourself to a massive headache and your computer to a laundry list of ailments.

When a Trojan is activated, numerous things can happen. Some Trojans are more annoying than malicious. Some of the less annoying Trojans may choose to change your desktop settings or add silly desktop icons. The more serious Trojans can erase or overwrite data on your computer, corrupt files, spread other malware such as viruses, spy on the user of a computer and secretly report data like browsing habits to other people, log keystrokes to steal information such as passwords and credit card numbers, phish for bank account details (which can be used for criminal activities), and even install a backdoor into your computer system so that they can come and go as they please.

To increase your odds of not encountering a Trojan, follow these guidelines.

1. Remain diligent

Trojans can infect your computer through rogue websites, instant messaging, and emails with attachments. Do not download anything into your computer unless you are 100 percent sure of its sender or source.

2. Ensure that your operating system is always up-to-date. If you are running a Microsoft Windows operating system, this is essential.

3. Install reliable anti-virus software. It is also important that you download any updates frequently to catch all new Trojan Horses, viruses, and worms. Be sure that the anti-virus program that you choose can also scan e-mails and files downloaded through the internet.

4. Consider installing a firewall. A firewall is a system that prevents unauthorized use and access to your computer. A firewall is not going to eliminate your computer virus problems, but when used in conjunction with regular operating system updates and

Get Your FREE Butterfly Reports Account Now - http://ButterflyReports.com/axz/affiliate.php?id=18024

reliable anti-virus software, it can provide additional security and protection for your computer.

Nothing can guarantee the security of your computer 100 percent. However, you can continue to improve your computer's security and decrease the possibility of infection by consistently following these guidelines.

RECOMMENDED PRODUCTS:

XoftSpySE

Free Scan With Amazing Conversion Rates. Google, Overture, & Custom Conversion Tracking. Dedicated Support For Our Affiliates!

AdwareAlert.com: 2008 Vista Certified

Another very good piece of software that will remove your Adware.

3. Finding the Security Suite that meets your needs

Before proceeding to read this article, it is important that we state something up front. It is essential for the reader to understand and appreciate that there is no such thing as a secure operating system or web browser. While the use of security suites and other complementing products can significantly reduce your risks, they are not magic wands that you can wave to eliminate 100% of your risk. Any product claiming they can do this should be viewed with great skepticism.

With that being said, let’s talk computer security and security suites. There are numerous ways in which the security of your computer can be breached. The most common threats come from worms, viruses, Trojans, phishing, hackers and crackers. Potential security breaches can come in the form of downloading unfamiliar email attachments, being monitored by spyware, maliciously attacked by malware, or probed through port scanning.

Dshield.org (www.dshield.org), a non-profit company, functions as a “dominating attach correlation engine with worldwide coverage”. In short, they work with people and companies to track, among other things, port scanning violations. Port scanning involves a person (referred to as a hacker or cracker) who attempts to break into you computer through the open ports in your system. Once an open port is located, the

individual attempts to collect your personal data or install a malware program into you computer. On average, Dshield.org logs over 1.1 billion reported attempts of port scanning each month. What is even scarier is that this is just based on their program participants. You can imagine how many more incidents are occurring each month to the general population of computer users.

If you have a Windows-based operating system and an unpatched PC, you will be attacked or infected in a little over 2 hours. When looked at in these terms, securing your computer becomes a mission.

Here are a few easy steps you can take to immediately protect your computer.

1. Don’t run unfamiliar programs on your computer.

It sounds like common sense, but many of the most prominent attacks have involved spyware and email attachment worms such as Bagle and Netsky. If you don’t recognize the sender, don’t download its attachments.

2. Don’t allow unrestricted physical access to your computer.

If you have sensitive or proprietary information on your computer, allowing other employees or family members to use your computer can lead to potential breaches in your computer’s security.

3. Don’t use weak passwords.

Use passwords which are difficult for someone to figure out. People frequently use the names of children, pets, anniversary dates, or birthdays. Because there seems to be a password needed for everything, it is not uncommon to see many people using the same password for everything. Big mistake! The use of only one password provides a hacker with easy access to a smorgasbord of personal information. If you have to write your passwords down, it is best not to leave them on a post-it, attached to the screen of your computer. You may chuckle at the absurdity, but it happens more than you think.

4. Don’t forget to regularly patch your operating system and other applications.

Many industry experts believe that most network security attacks would be stopped if computer users would just keep their computers updated with patches and security fixes. Too often, we forget to do this on a regular basis. Remember that every day, new viruses, worms and Trojans are being created and distributed. They are looking for the weaknesses in your computer system. Having outdated software is basically the same as holding the door open and inviting them in for a visit.

5. Don’t forget to make regular backups of important data

Always keep a copy of important files on removable media such as floppy/ZIP disks or recordable CD-ROM disks. Store the backups in a location separate from the computer.

Get Your FREE Butterfly Reports Account Now - http://ButterflyReports.com/axz/affiliate.php?id=18024

In most cases, Windows desktop and screen-saver passwords provides adequate protection for normal security concerns. However, if you feel more comfortable taking additional security measures consider obtaining a comprehensive security suite.

Selecting a Antivirus Software

The next question is how do you pick the best product for your needs? You start by asking yourself a series of questions. Do you need password protection for individual files, your desktop, a network, or to block someone's access to the Internet? Is your computer used only by you or do multiple users have access to the computer? How many users in total do you expect on your computer? What are your system requirements? How much do you want to spend?

Once you are able to answer these questions, you can begin to research which security suite will best meet your needs. Product reviews and user statements provide a great starting point. PCMagaine (www.pcmag.com), Zdnet.com (www.zdnet.com), and Consumer Reports (www.consumerreports.org) are just a few informative sites that offer research on various computer software products.

There are numerous security suites available on the market. Take the time to choose the one that meets your specific needs. As a starting point, we've listed a couple of the more popular programs:

1. Kaspersky Personal Security Suite

Description: A comprehensive protection program package designed to guard against worms, viruses, spyware, adware and other malicious programs. The program offers five pre-defined security levels and is convenient for mobile users. System requirements: Window 98/2000/XP; Internet Explore 5.0 or higher, Memory: minimum of 64 MB RAM, 100 MB free on hard drive.

2. Shield Deluxe 2005

Description: This program provides protection from viruses, adware, spyware, and privacy threats while using very low system resources. Additionally, the maker, PC Security Shield offers ongoing free technical support. System requirements: Windows 98 or higher, WinNT, WinXP, WinME; Internet Explorer 5.1 or higher, Memory: 32MB ram or higher, 65 MB free disk space.

RECOMMENDED PRODUCTS:

SpyWare Detection & Removal Software

This SpyWare Nuker Is Top Choice By Consumers, and sells like hot bread.

AdwareBot - Remove Adware And Spyware Now

AdwareBot Was Created By The Developers Of Anitspyware.com As A Substitue For Internet Users Suffering From Adware Infestations. The Software Also Include Spyware, Malware, Keylogger And Virus Removal Engines. A True Quality Product.

4. Protection You Can Afford

Malware. An odd sounding word created to lump all malicious software programs, including viruses, worms, trojans, spyware, adware, and other malevolent codes into one cause-your-computer-serious-hurt category.

In 2005, Computer Economics released a report on malware. The good news was that for the first time since 2002, the total worldwide financial losses from malware actually declined to a mere $14.2 billion. The bad news was that the nature of malware was changing from overt threats to more focused, covert attacks. This definitely is not great news for the average computer user just trying to keep up with the hundreds of malware programs that bombard us daily.

It’s not an easy task keeping malware out of your computer system. In order to accomplish this, you need a strong antivirus program. One such program that can deliver the goods is ZoneAlarm Internet Security Suite 6 from Zone Labs. Zone Labs is one of the most trusted brands in Internet Security for good reason. Their product, simply put, kicks serious malware gluteus maximus.

ZoneAlarm has received more review recommendations that any other Internet-security software suite because of its superb firewall and antivirus protection. It blocks pop-up ads, protects against identify theft and provides adequate spam filters that are flexible. It even beats the market leader, Norton Internet Security, which is often criticized for excessive system drag.

Its newest version includes these additional features:

• Τριπλε Δεφενσε Φιρεωαλλ το πρεϖεντ σπψωαρε φρομ σενδινγ ψουρ ινφορματιον αχροσσ τηε Ιντερνετ. Ιτ αλσο μακεσ ψουρ χομπυτερ ινϖισιβλε το ανψονε ον τηε Νετ.

• Σμαρτ Δεφενσε Αδϖισορ ωηιχη χαν αυτοματιχαλλψ αδφυστ ψουρ σεχυριτψ σεττινγσ φορ μαξιμυμ προτεχτιον αγαινστ τηε λατεστ ϖιρυσ ανδ σπψωαρε ουτβρεακσ.

• Αδϖανχεδ Ιδεντιφψ ανδ Πριϖαχψ Προτεχτιον το πρεϖεντ ψουρ περσοναλ δατα φρομ λεαϖινγ ψουρ χομπυτερ ωιτηουτ ψουρ αππροϖαλ.

The bonus for the average user who cringes at the idea of setting-up one of these systems is that the interface is easier to understand and use in comparison to most if its competitors. If you choose to venture beyond the out-of-the-box default settings, and install a more elaborate filtering, know that this will require some additional time to set up on your part.

Overall, ZoneAlarm Internet Security Suite is a user-friendly, comprehensive security solution that will have your computer safe from Internet hazards and cyber criminals within minutes of installation.

There are numerous ways you can lose the information on your computer. Your child decides to play Chopin on your keyboard, a power surge, lightening, a virus, or even simple equipment failure. Therefore, backing up the contents of your hard drive is an absolute MUST. By regularly making backup copies of your files and storing them in a separate location, you can typically get some, if not all, of your information back in the event your computer crashes.

While a regular backup to floppy, CD, or zip drive will save your files, wouldn't it be great if you could create an exact copy (a drive image) of your hard disk? That means backups of all your files, programs, and user settings. This would definitely save you time when it came to reloading. Acronis may be able to help.

Acronis True Image 9.0 is a robust disk-imaging utility software that copies the entire contents of your hard drive including data and operating system files, personalized settings, and more, onto another disk or disk partition. Its layout is easy to use and navigate. It also includes wizards which can walk you through both backing up and restoring your computer. Highlighted features include:

• Secure Zone — allows you to save data to a special hidden partition located on your hard drive which would eliminate the need to purchase an extra hard drive.

• PC Cloning — you can upgrade to a new system disk without needing to reinstall the operating system and applications, or configure user settings.

• Acronis Snap Restore - lightening-speed restore of your PC from an image. You can start working in seconds while your system is still being restored.

Acronis provides a free test-drive of its product and a 30-day money back guarantee. When you are ready to purchase, you can either download for $49.99, or if you so desire, order a boxed version for $59.99. With Acronis True Image Home 9.0, you can rest easy that your family pictures, personal documents, tax returns, resumes, and other important information will not be lost forever.

RECOMMENDED PRODUCTS:

Get Your FREE Butterfly Reports Account Now - http://ButterflyReports.com/axz/affiliate.php?id=18024

SpyNoMore Anti-Spyware

Spyware Is Making Headlines. With Over 150,000 Detection Rules, SpyNoMore Is The Answer.

Computer Secrets Unleashed

Don’t Pay A Computer Guy Hundreds Or Thousands Of Dollars! A Top I.t. Pro Breaks His Silence And Reveals The Secret Techniques To Keep Your Home Or Office Computer Screaming Fast, Free Of Spyware, Viruses & Hackers, And 100% Backed Up!

Get Your FREE Butterfly Reports Account Now - http://ButterflyReports.com/axz/affiliate.php?id=18024