MTBN.NET PLR Library
Category: Computers_Technology File: How_to_protect_your_Computer._Wery_useful_Tips_utf8.txt
Text and Word PLR Article Packs available at PLRImporter.Com

Title:
How to protect your Computer. Wery useful Tips

Word Count:
1348

Summary:
Computer Security Ethics and Privacy

Keywords:
computers, internet, antivirus, computer, hard disc, cd, dvd, programs

Article Body:
Today, many people rely on computers to do homework, work, and create or store useful information. Therefore, it is important for the information on the computer to be stored and kept properly. It is also extremely important for people on computers to protect their computer from data loss, misuse, and abuse. For example, it is crucial for businesses to keep information they have secure so that hackers can't access the information. Home users also need to take means to make sure that their credit card numbers are secure when they are participating in online transactions. A computer security risk is any action that could cause lost of information, software, data, processing incompatibilities, or cause damage to computer hardware, a lot of these are planned to do damage. An intentional breach in computer security is known as a computer crime which is slightly different from a cypercrime. A cybercrime is known as illegal acts based on the internet and is one of the FBI's top priorities. There are several distinct categories for people that cause cybercrimes, and they are refereed as hacker, cracker, cyberterrorist, cyberextortionist, unethical employee, script kiddie and corporate spy. The term hacker was actually known as a good word but now it has a very negative view. A hacker is defined as someone who accesses a computer or computer network unlawfully. They often claim that they do this to find leaks in the security of a network. The term cracker has never been associated with something positive this refers to someone how intentionally access a computer or computer network for evil reasons. It's basically an evil hacker. They access it with the intent of destroying, or stealing information. Both crackers and hackers are very advanced with network skills. A cyberterrorist is someone who uses a computer network or the internet to destroy computers for political reasons. It's just like a regular terrorist attack because it requires highly skilled individuals, millions of dollars to implement, and years of planning. The term cyperextortionist is someone who uses emails as an offensive force. They would

usually send a company a very threatening email stating that they will release some confidential information, exploit a security leak, or launch an attack that will harm a company's network. They will request a paid amount to not proceed sort of like black mailing in a since. An unethical employee is an employee that illegally accesses their company's network for numerous reasons. One could be the money they can get from selling top secret information, or some may be bitter and want revenge. A script kiddie is someone who is like a cracker because they may have the intentions of doing harm, but they usually lack the technical skills. They are usually silly teenagers that use prewritten hacking and cracking programs. A corporate spy has extremely high computer and network skills and is hired to break into a specific computer or computer network to steal or delete data and information. Shady companies hire these type people in a practice known as corporate espionage. They do this to gain an advantage over their competition an illegal practice. Business and home users must do their best to protect or safeguard their computers from security risks. The next part of this article will give some pointers to help protect your computer. However, one must remember that there is no one hundred percent guarantee way to protect your computer so becoming more knowledgeable about them is a must during these days. When you transfer information over a network it has a high security risk compared to information transmitted in a business network because the administrators usually take some extreme measures to help protect against security risks. Over the internet there is no powerful administrator which makes the risk a lot higher. If your not sure if your computer is vulnerable to a computer risk than you can always use some-type of online security service which is a website that checks your computer for email and Internet vulnerabilities. The company will then give some pointers on how to correct these vulnerabilities. The Computer Emergency Response Team Coordination Center is a place that can do this. The typical network attacks that puts computers at risk includes viruses, worms, spoofing, Trojan horses, and denial of service attacks. Every unprotected computer is vulnerable to a computer virus which is a potentially harming computer program that infects a computer negatively and altering the way the computer operates without the user's consent. Once the virus is in the computer it can spread throughout infecting other files and potentially damaging the operating system itself. It's similar to a bacteria virus that infects humans because it gets into the body through small openings and can spread to other parts of the body and can cause some damage. The similarity is, the best way to avoid is preparation. A computer worm is a program that repeatedly copies itself and is very similar to a computer virus. However the difference is that a virus needs o attach itself to an executable file and become a part of it. A computer worm doesn't need to do that I seems copies to itself and to other networks and eats up a lot of bandwidth. A Trojan Horse named after the famous Greek myth and is used to describe a program that secretly hides and actually looks like a legitimate program but is a fake. A

MTBN.NET PLR Library
Category: Computers_Technology File: How_to_protect_your_Computer._Wery_useful_Tips_utf8.txt
Text and Word PLR Article Packs available at PLRImporter.Com

certain action usually triggers the Trojan horse, and unlike viruses and worms they don't replicate itself. Computer viruses, worms, and Trojan horses are all classifies as malicious-logic programs which are just programs that deliberately harms a computer. Although these are the common three there are many more variations and it would be almost impossible to list them. You know when a computer is infected by a virus, worm, or Trojan horse if one or more of these acts happen:

? Screen shots of weird messages or pictures appear.
? You have less available memory then you expected
? Music or sounds plays randomly.
? Files get corrupted
? Programs are files don't work properly
? Unknown files or programs randomly appear
? System properties fluctuate

Computer viruses, worms, and Trojan horses deliver their payload or instructions through four common ways. One, when an individual runs an infected program so if you download a lot of things you should always scan the files before executing, especially executable files. Second, is when an individual runs an infected program. Third, is when an individual bots a computer with an infected drive, so that's why it's important to not leave media files in your computer when you shut it down. Fourth is when it connects an unprotected computer to a network. Today, a very common way that people get a computer virus, worm, or Trojan horse is when they open up an infected file through an email attachment. There are literally thousands of computer malicious logic programs and new one comes out by the numbers so that's why it's important to keep up to date with new ones that come out each day. Many websites keep track of this. There is no known method for completely protecting a computer or computer network from computer viruses, worms, and Trojan horses, but people can take several precautions to significantly reduce their chances of being infected by one of those malicious programs. Whenever you start a computer you should have no removable media in he drives. This goes for CD, DVD, and floppy disks. When the computer starts up it tries to execute a bot sector on the drives and even if it's unsuccessful any given various on the bot sector can infect the computer's hard disk. If you must start the computer for a particular reason, such as the hard disk fails and you are trying to reformat the drive make sure that the disk is not infected.

More about Computers and Internet on : http://bestofcomputers.blogspot.com

Find some useful TIPS about investment and financing on:
http://investmentandfinancing.blogspot.com