Title:
Five Critical Steps You Should Take To Protect Your Personal Or Work Computer

Word Count:
564

Summary:
Computers have come a long way in the past few decades. This, in a way, is a double-edged sword. With computer technology as advanced as it is now, we have easy and quick access to conveniences such as shopping centers, bank statements and health records. Unfortunately, hackers can also work out how to get into supposedly private records. Hacking can be a real nuisance and cause you great financial loss or other damage.

Computer security is vital. You can reduce the likeli...

Keywords:
GoToMyPC, GoToMeeting

Article Body:
Computers have come a long way in the past few decades. This, in a way, is a double-edged sword. With computer technology as advanced as it is now, we have easy and quick access to conveniences such as shopping centers, bank statements and health records. Unfortunately, hackers can also work out how to get into supposedly private records. Hacking can be a real nuisance and cause you great financial loss or other damage.

Computer security is vital. You can reduce the likelihood of experiencing identity theft by making your computer as hacker-proof as you can. You need common sense and the right software. Here are 5 key points in making your computer as safe as possible:

1) A firewall is a good way to shield your computer. It is a type of software that checks all data that enters and exits your machine and blocks any that does not meet specified security criteria (your user-defined rules). Anti-virus and anti-spyware programs are effective after something has got into your machine but a firewall should block the bad stuff in the first place.

2) Scan every file you receive, no matter who sent it. You cannot assume it is safe to open a ‘funny video’ file from your brother or a ‘cool game’ attachment from your friend because a virus might have embedded itself without them knowing

about it. Your brother or friend might not be using good hacker-proof software themselves. It only takes a few seconds to do a security scan and this could make the difference between accepting a virus and denying it entry to your computer.

3) If you receive spam (junk email) do not click on any website links it contains. Some spammers have been known to send links to try and obtain personal information. Some of these messages are disguised as important communications from well-known online establishments, such as PayPal or Ebay, and they ask you to confirm your password or credit card number. Alternatively, they sometimes try to upload harmful software onto your machine. You can always forward a suspect email to the establishment itself to verify if it did come from them or if it is fraudulent.

4) Do not store sensitive data on your machine. If your computer does get infected with a worm, piece of spyware or virus, you know that the thieves will not get their hands on any personal information useful to them. Hackers want full names, social security numbers, home addresses, phone numbers and credit card numbers. If you do not save these things on your computer, hackers cannot get to them.

5) You need to install an anti-virus and anti-spyware program. This stops malicious code from downloading and installing on your machine while you are on the internet. This malicious code, known as worms, viruses or spyware, can destroy important files, stop your machine from functioning altogether and send sensitive data back to the identity thief. You can be faced with a huge bill to repair your computer, might lose all your data and someone might be able to clean out your bank account. It is a mistake to think you do not need protection.

The best way to prevent computer crime is to use common sense and make sure you have the best software installed on your computer. Doing this protects not only yourself but also the spread of these malicious files to your friends and business connections.