

Tips for Internet Security

Many people are leery of using the Internet because they are afraid of getting a virus on their computer, becoming victims of identity theft, or a host of other problems. The truth of the matter is that using the Internet is just like driving a car: if you are acting responsibly, you'll be fine. Let's go through a few tips that will help you feel more secure in using the Internet.

1) Virus/Spyware Protection

You absolutely have to have virus protection. Let me repeat that, just to make sure you understand. **YOU HAVE TO HAVE VIRUS PROTECTION.** It doesn't cost that much to purchase virus protection, and you'll be glad you did the next time a 'major virus threat' comes down the pipe. I recommend either Grisoft AVG or Avast!, both of which can be downloaded as a free trial before you have to buy them. **Do not use more than one virus protection program.** This will cause major conflicts on your computer. If you want to have more protection than what anti-virus software offers, you might want to install a spyware prevention program. I recommend Spybot—Search & Destroy, which is provided for free though donations are welcomed.

You may find these programs at the following websites.

<http://www.avg.com/download-trial>

http://download.cnet.com/Avast-Home-Edition/3000-2239_4-10019223.html?tag=mncol

<http://www.safer-networking.org/en/mirrors/index.html>

2) Trust No One!

Sometimes, the biggest threat to your Internet security is you. Too many users are too trusting, which leads them to give out highly critical information. This is one area of life where having trust issues might be helpful. Be careful whom you give your information to. Online shopping is fine, and it's most often secure. Most reputable companies offer some sort of guarantee (i.e. VeriSign, PayPal, etc) to certify that transactions made through them are safe.

The basic principal is this: if it feels like it could be dangerous, it probably is. Do some research. Check with the FTC, BBB, and Google to see what's being said about the company and whether or not it's safe to deal with.

Online shopping isn't the only area where the worst can happen. Too many people are taken in by e-mail scams. Read this carefully: **The U.S. Government will not contact you via e-mail. There is no Nigerian prince trying to smuggle millions of dollars into the country. Your long-lost, distant uncle did not die in London, and the executor of his estate is not trying to send you your inheritance. Your bank does not need you to remind them of your account or PIN number.** This listing of scenarios might seem silly, but this is just a sample of some of the most popular e-mail scams that people **do fall for** each year. If you receive an e-mail that you think might possibly be real, contact the company for verification.

If you're still really concerned about identity theft or unsecure online financial transactions, you might want to invest in identity theft insurance, which you can find more information about from the link below.

<http://www.zanderins.com/idtheft/idtheft.aspx>

3) Secure Passwords = Security

Most e-mail and commercial sites now require what are considered strong passwords, and you should make sure that what you use is considered strong. Microsoft.com offers a great article on this subject, which you can find at the first link provided below. The second link leads to an online Password Protector that Microsoft offers for free.

<http://www.microsoft.com/protect/yourself/password/create.msp>

<http://www.microsoft.com/protect/yourself/password/checker.msp>

4) Don't Be Afraid to Ask for Help

Technical support exists for a reason. The problem is that it often costs more than it should. Google, a search engine, can provide numerous articles and websites, which deal with common computer issues. You might also check your phone book for local computer stores that offer reasonably priced technical assistance. Many chain stores offer tech support; however, many of their 'technicians' are simply following a checklist of issues that has been prepared ahead of time. Rarely are they properly trained to offer tech support beyond their checklist, yet they almost always are more costly than they should be.

5) Turn Your Computer Off

It sounds so basic, but so many people become victims of malicious software simply because they left their computer on and the Internet flowing into it with no one watching. So, to add another layer of protection, turn your computer off.