Computer Safety in the Modern Age

Computers are wonderful tools. They allow us to display and sort information in new ways and present that information quickly and easily to many people. By using the internet we can connect office and home computers to vast sources of information and to each other. With these connections come a few responsibilities.

Viruses

Viruses are programs that are written to make your computer do things that you don't want it to do. They can be as simple as making a message appear on your screen to something as sinister as erasing all of the data from your computer. There have even been viruses written that allow the writer to use your computer to attack websites. This causes your computer to run slowly and also slows down the website for those that are attempting to view it.

It is important that every computer that you use has anti-virus software running on it. Some computer systems are more vulnerable than others but all computers need to have anti-virus software. Two major vendors which are both popular are Symantec and McAfee. Such software costs approximately $60 at this time. It's possible to find it cheaper via mail order. The important thing is to buy a package and install it on your system immediately.

Set the software up so that it checks for updated virus definition files and installs them if necessary. Virus definition files are what the software uses to determine if something coming to your computer is a virus or not. There are dozens of viruses released weekly so Symantec and McAfee update their virus definitions on a regular basis. If you installed anti-virus software a year ago and have never updated the definitions, you may as well not have it installed at all as the virus variations are countless.

The final step is to check the software once a month to make sure it is running correctly. Also, you will want to make sure that it's updating the definitions when it's supposed to. If it's not running or the definitions are old, restart the software, update the definitions, and then check it again in a couple of days. If the software is disabled again, take your computer to a professional to have it cleaned. Some viruses first attack anti-virus software and disable it. That allows the follow-up virus to attack the system.

It's also important to note that viruses can forge the sender name. For example: Jim's computer gets a virus. Jim has George and Heather's email address in his address book. The virus then sends a message to George, and make's it look like it came from Heather. So if you get a message from someone that contains a virus, it doesn't mean that they sent it.

Spyware

Spyware is software that gets installed on your system and then tracks what you do. Some spyware monitors web sites that you visit and then sends that information to the company that wrote the spyware. They sell that information to advertisers and then create pop-up messages on your system.

Spyware can take many forms, such as search bars, date & time monitors, etc. Don't install them. Make your favorite search engine a favorite and get to it that way. It also doesn't matter if your time is off by a little bit. Set it and don't worry about it. You also need to make sure that you pay attention to what you are doing when browsing the web. One way that spyware gets installed is via pop-ups. I have seen pop-ups worded in a confusing manner. For example, it may say click yes to not install the software. You read it quick and then click no and the software gets installed.

If you suspect that your machine has been infected with Spyware, there are a number of free or low cost removal tools. One that I use often is Spybot Search and Destroy. You can download it from **http://www.safer-networking.org/en/index.html**.

One good way to protect yourself from spyware is to make sure that you never use your computer with administrator rights. All modern operating systems allow you to create multiple users and

give them different rights on the system. Create an administrator user that you will use only when you want to install software and a user account for all other use. The user account should not have the right to install software. Of course you will also want to create an account that your kids or grandkids use. You don't want them erasing or moving your files.

Urban Legends and Email Hoaxes

There are a number of emails circulating that talk about lost kids or gathering postcards for someone that's dying. There is even one that says that Coke was originally green. These emails sound real and they ask you to pass them along to everyone that you know. Before you pass them along, visit **http://www.snopes.com/**, as it is an excellent reference for urban legends. You wouldn't believe everything that you read in the paper, so don't believe everything that you read in an email.

Another type of email that is gaining in popularity are those that appear to be from your bank. This is known as Phishing. These messages contain the bank logo and talk about security concerns. They ask you to click a link in the email and update your information right away. When you click the link, you are taken to a site that appears to be the bank, but it's not. On the site is a form that asks you for your name, address, account number, password, social security number, etc. When you fill the form out and hit submit, you are giving information to people that are attempting to steal your identity. So, if you get an email like that, open your web browser and go to the bank or brokerage firm site and see if they are looking for updated information. Don't click the link in the email!

Conclusion

Before you read the next article on the internet, check your virus software. Do you have current software installed? Are the virus definitions current? If not, you're computing on borrowed time.