Classic Computers

970-874-9210

BEST PRACTICES FOR HOME COMPUTER SECURITY

Always remember to have TWO copies of all your data. That is one copy in your computer and one outside your computer. If you use a cloud service (Carbonite, DropBox, and the like) you need to consistently check to make sure that you can access your data and that the program is backing up everything you want. Do not back up your entire hard drive. Programs have to be reinstalled. If you have a financial program, use the built in backup ability to back up your data outside your computer and also backup to your Documents folder, that way your cloud service program will also make a second backup of your financial data.

Microsoft, Dell, HP, etc. will not call you to tell you your computer has a virus. These corporations do not care if you have a virus. The calls are always scams. If you are contacted via a phone call tell the caller that you do not own a computer. This will encourage them to not call back. Make sure everyone in your household tells them the same thing, that you do not own a computer.

Never give anyone remote access to your computer unless you know exactly who they are. A common scam when they get remote access is to plant hidden programs that can do any number of unwanted things, now or in the future. Theses scammers will show you the "Event Log" in your computer, to show you all the errors your computer is generating. It is very common for the "Event Log" to have a few random errors and it is usually nothing to worry about. Scammers use it as a scare tactic so that you will let them "fix" your computer.

Never give your credit card number over the phone. If you feel you have been compromised contact your credit card company and your bank. Follow their instructions.

BEST PRACTICES FOR THE INTERNET

Never click on ads. If you're interested in something type the address in the address bar of your browser (Amazon, Sears, Wal Mart. etc).

If you get a pop-up box from a web site, CLOSE THE BROWSER!! Do not click anywhere within the pop-up box. Do not click the X on the pop-up. Any place within the pop-up can be an executable.

If a pop-up tells you that you need a newer version of java or flash, close the browser, open it again, go straight to the source of the requested update. If you already have the latest version these web sites will say so.

Java – www.java.com Please uncheck the boxes for “Ask”.

Flash – www.adobe.com Under “Menu”. Uncheck the box for “Chrome”

Always read each screen to make sure you can de-select additional programs that you do not want. You can the go back to the site that asked for the update. If it still has a pop-up telling you to update, close the browser. Chances are that web site is infected with a virus. Do not go back to that web site for a couple of weeks at least. Their administrators will discover the infection and fix it on their end.

Other common web sites to download from are:

Firefox – www.mozilla.org

Chrome – www.google.com/chrome

Open Office – www.openoffice.org

Microsoft Security Essentials – www.Microsoft.com under Downloads.

DO NOT CALL 800 NUMBERS THAT POP UP ON YOUR SCREEN!

A good way to get a virus is downloading something that you would normally have to pay for. Music and movies are the two most common. Downloading programs that would normally not be free is another common way to get a virus. It is also illegal to download copyrighted material and you can be prosecuted.

Do not click on links on Facebook or in emails. You can read the article or view the video, but again, go straight to the source. Open a new tab and go to the website for the article or for the video.

Do not try and fix your computer using Google or any other search program. If you do not know legit sources you can infect your computer. Most of the time Google or Bing searches do more harm than good and also make the computer harder to fix when you do have it fixed.

There are 4,000 new viruses every month. There are no perfect virus programs. The only guaranteed way to never get a virus is to never turn a computer on. Since that’s not practical, these are some ways to lessen the risk.

Other things you can do is update and run full system scans with your virus and malware programs once a month or sooner if you are suspicious. Allow your computer to do the Microsoft updates. These are usually automatic, however, some people change their update settings and they should do them manually weekly.

Change your passwords twice a year or sooner if you think you have been compromised.