Best Practices for Securing a Computer and Preventing Malware Infections 11/13/2014

1. **The computer user plays a major role in his or her online security along with anti-virus programs**. Awareness of the software on your computer, how to use your anti-virus program and reading notices before you click are good habits to have as a computer user.

2. **Keep Automatic Updates running and accept all downloads of updates and patches** for Windows and Apple operating systems. All Microsoft Office programs for Windows and Mac should be updated as those patches are released as well. There is almost always a security aspect to an update.

3. **Accept updates and install them for all non-Microsoft and non-Apple programs** such as Hewlett Packard, Adobe Flash and Reader, Oracle (Java) and all other major software and hardware companies. Keeping their software update programs active and accepting updates will play a major role in keeping you safe online.

4. **Use Stronger Passwords.** A consistent theme in Internet security articles is the use of weak passwords or no passwords at all at computer and email logon screens. While Windows, Android and Apple computers and devices do not demand a password be used to log in to their computers, all email programs demand a password of increasing complexity.

a. A weak password includes your child's name, pet's name, phone number, street address, number sequences like 1234567890 or the word "password."
b. Strong passwords are at least ten to fourteen characters and include no actual words or acronyms associated with the user. A proper password should contain at least one upper case letter, at least one lower case letter, at least one number and an acceptable symbol such as "$" (dollar sign) or "!" (Exclamation point).
c. The password xBxfre6o$?x uses the letter "o" to represent a zero, the "$" symbol represents an "s" and the "?" is added to make the password longer and stronger. Perhaps the password is guessable if the hacker knew the person really well, but probably not.
d. Create and use several email addresses with unique passwords for different types of accounts

5. **Use a top of the line Anti-virus/Anti-malware program** like BitDefender, Kaspersky or Norton's anti-virus security. Run scheduled daily and weekly scans to find and remove malware. Security software must be run in an Always On mode automatically scanning email and Internet traffic on your computers. If you think there might be an undiscovered infection, run a manual scan.

6. **If the email offer sounds too good to be true**, it surely isn't true, especially if you have to give money or open up your bank account to participate in the offer. Remember that being a little paranoid is just fine.

7. **Backup your important data.** Every good security plan includes a backup copy of all important data files including photos, school papers, financial records, taxes and other digital documents. All backups should be stored on external media such as hard drives or thumb drives and flash drives.

   External hard drives with copies of all important data are the first backup line of protection. There are many backup programs, but two services that are free include Windows' Backup and Restore program and Apple's Time Machine app. Each are included in their respective operating systems and easy to use to save important data files. However, Time Machine can completely restore a Mac computer including the computer's operating system and installed programs.

   Cloud Backup services by LiveDrive and Carbonite should be considered as an insurance backup copy in case of catastrophic damage to business facilities or thefts of computers and backup devices.

   No security backup plan is complete without attempting to make a test restore of some of your most important "backed up data." Don't make the mistake of assuming your data is backed up. Restore some of your data to prove you and making worthwhile data backups.

Article created by Dick Smith, Training Director for Computer Concepts, LLC, 757-870-8703