Updated: 02/03/2017

Computer Security

Computers are used for Internet banking, investments, tracking business and personal finances, health care information, employee records and business correspondence. This information can be misused for identity theft, actual theft and other nefarious schemes.

Computers in your home where physical access is limited to the immediate family often do not require user accounts that are password protected. If others are able to access your computer, make sure you have a password protected logon for your account. A computer located in a business environment must be protected by a user account logon.

The following list is good practice needed to safeguard your valuable information:

1. **Keep your system up to date.** Enable the Microsoft automatic updates. It is important to do these updates since they fix software problems that might allow someone to infect or take over your computer. If you see the yellow security shield in the System Tray in the lower right hand corner of your monitor, be sure to click on it and let the update install.

2. **Do NOT click on links.** Links appear on web pages and in email. The links appear in the form of blue underlined words, OK buttons, Submit buttons, or images and ads. These links are links to web pages on other computers. When you click on a link, you are giving your browser permission to go there. Once you do this, it is possible for the other computer to do bad things to your machine.

3. **Be very careful with all email.** Email will often contain malicious links and attachments.

    a. **Never click on an attachment** unless you know it came from a trusted source. Even friends can accidently send you a virus if their computer happens to be infected.

    b. **Be aware of forged emails** - A common scam is sending you an email that appears to come from someone you know. The email may have the return address and name of someone you know. Look to see if it contains links or an attachment or if the subject or content is unusual. **Do not click on links or open the attachment.**

4. **Ransomware** is malware that encrypts all of the data on your computer. The criminal then demands a ransom for the key that will allow you to decrypt your data. Often the price will be hundreds of dollars. Once this happens the only way you can recover without paying is if you have a recent offline backup of all your data.

5. **Social Engineering** – A cybercriminal will call you on the phone and claim to be from the company who made your computer, or IBM, or Google or any easily recognized company. They will claim to have detected a problem on your computer and offer to fix it. In the process, they talk you into giving them control of your computer and they fix the problem. They also install malware to infect or control your computer. **Do not accept help from someone who calls you, you really don't know who they really are.**

6. **Run an antivirus program** "Microsoft Security Essentials". Microsoft Security Essentials is built into Win 7 and Microsoft Defender is built into Win 10. These are free applications that will automatically be updated. Make sure whatever A/V program you use that it is set to automatic update. Make sure your computer's firewall is enabled. This can be done from the Control Panel Security tab in Windows and is normally switched on by default. If you have another A/V program, make sure it updates automatically. You may have to buy a subscription from the vendor to enable updating. You should only have one A/V enabled on your computer.

7. **Beware of "Pop-ups".** These are windows that "pop-up" on your desktop. Often, they are advertisements that offer free software. Downloading and installing an application from and untrusted site can infect your computer. Some Pop-ups will warn you that your computer is infected or has a problem and ask if they can scan your computer to fix the problem. **Do Not Click OK because it is malware trying to infect your computer**.

8. **Don't go to dangerous web pages**. On many of these sites when you download a file, for example a music file from a peer to peer music sharing site you may also get several harmful programs. These can be anything from browser hijackers to pop-up advertising.

   Examples of suspect sites are:

   a. Music sharing sites
   b. Casino and game sites
   c. Porn sites
   d. Free software downloads sites. (Source Forge, CNet, and others are safe sites but it is still buyer beware.)
   e. Don't click on web page links to download something unless you know it is safe.

9. **Choose Internet shopping sites carefully.** When you go out to shop or dine or some other activity, you avoid "seedy" places. You instinctively avoid places or people that look suspicious or dangerous. You need to think about the Internet in the same way. Name sites like Penney's, Sears, Amazon, or government sites are safe and secure. Sites that have a brick and mortar location that can be found on Google are safer than Internet only sites. Sites you are not familiar with are much more of a risk. You can often search for a business on Google and find information about their trustworthiness.

10. **Make sure you are using an SSL connection to make payments on the Internet** Most sites such as banks or online stores will establish a SSL connection when you are making payments or doing banking. Most browsers will display a gold key or green address bar when connected to an SSL site. To make sure, look at the URL in the address bar, the URL should begin with https://. The "s" tells you that you are using a secure, encrypted link. This means your information is encrypted before it leaves your computer and does not get decrypted until it is at the destination.

11. **Backup your data.** All the documents, pictures and videos you keep on your computer are stored on a hard disk. Hard disks can get corrupted or physically malfunction to the point where your information can be lost. Malware infecting your computer can make it impossible to save any of your data. When this happens, you may lose priceless family pictures, music collections, financial records and other things that are important. You must provide a way to back up your computer.

    It is a good idea to follow a 3-2-1 plan. You need three backups stored on two different media with at least one backup stored off site. The Windows operating system does have backup software. You can buy a USB hard disk that can be attached to the computer and all your valuable data can be copied to this external disk. You can copy pictures and data to DVDs using your DVD writer. Either of these can be kept in a safe deposit box or at another location. If you have a fire or burglary, your data can then be restored on the new computer.

    You can also back up automatically to the "cloud" by using a service such as Carbonite. For about $60 a year, you can make sure all of your data is automatically backed up to an encrypted store on their servers. If ever it is needed, you can then restore the data to a new computer.

12. **DO NOT provide account or personal information over the Internet** unless you know you are on a safe site. No bank or company will send you this kind of request! (A criminal will send you an email that looks like it is from your bank, or credit card Company. It will have official logos and look very legitimate. It will typically say something about a problem they had and that they would like you to click on a link enclosed in the email and go to their site to verify some information. The information turns out to be your account number, password, etc. The site will look exactly like a real site. If you give them your information, **they will probably steal from your account immediately**.) If you get an email from your bank, broker or credit card site that

requires your input, it is good practice to not use any links in the email. Use your browser to navigate to the site and login as you normally would. Best way is to call them on the telephone and find out what is needed. Don't call phone numbers provided by an email.

13. **Use good Passwords** (See short password tutorial below.)

    a. If you keep password or account information on your computer, try to keep it in an encrypted file. It is probably better to write it down and put the list in a safe place until you need it. Don't write down the passwords and tape it to your computer. Freeware programs exist such as KeePass and LastPass that will keep you passwords in an encrypted store. LastPass can be used from any computer and provides a simple way to remember your passwords and to simplify logons.

    b. Do not use very simple and obvious passwords. Ideally your password will be more than 12 characters long, contain upper case, lower case, numbers, and at least one special character.

    c. Do not use a password that can be looked up in a dictionary. Do not use simple pattern passwords such as "Qwerty" or "123456". Hackers have lists of hundreds of commonly used passwords such as "monkey", "Secret" and others. They will first run down a list of several hundred common passwords and the do a dictionary attack because these methods are simple and often successful. A password such as this "Example….60060" would be very difficult to find. "Example" is not a dictionary word since it is combined with other letters. The dots or other special characters are "padding" to make it longer and the number is some number that you will remember such as your childhood telephone number. Be creative! See "What is a Good Password" below.

    d. Do not use the same password on everything. If someone gets the password, all of your accounts will be open to them. It is a good idea to use different passwords for important accounts such as Internet banking.

14. **Beware of friends, relatives and acquaintances who know how to fix your computer.** Most people are over confident about their computer skills especially when they are working on someone else's computer.

    If you must tinker with your computer set a restore point and make a full back up of your system. Most backup programs will allow you to save an image of your hard disk to an external drive. This image can be used to restore your computer to the condition it was in when you made the backup.

15. **It is also a good idea to have a router on your home system.** A router (wireless or not) can be installed between your modem and your home network. Many of the newer modems provided by carriers have built in routers. Use the WAP encryption on the router with a good password. A NAT router hides your computers from the outside world and since it is kind of a dumb hardware device, it is difficult for someone to hack it.

16. **Many computer problems are often caused by users installing new software.** Make sure you understand the system requirements before you elect to install new software. You can find this information printed on the software packaging or on the web site where you go to download the software. Your computer must have the required hardware, sufficient disk space, and enough memory to satisfy the resources required by the new software.

17. **Do not upgrade your Operating System.** Upgrading the operating system can result in significant problems. Operating systems (OS) usually require a certain level of computer hardware resources. If the computer does not meet these requirements, the computer may become inoperable after the upgrade is loaded. Usually the installation of a new OS will wipe out all of the old applications and the data in the computer. It also reinstalls all of the drivers needed to operate your hardware. Sometimes the new OS may not have a driver required by your hardware and the system will fail to operate. Upgrading the OS should only be done by a qualified technician.

Updated: 02/03/2017

What is a Good Password?

In order to understand what constitutes a good password, you need to understand a little about how the bad guys attempt to discover your password.

A very common method that is used to guess passwords is to use a list of common passwords. It is readily available on the Internet to anyone who wants it. Below is the top ten off the list.

123456
password
12345
12345678
qwerty
123456789
1234
baseball
dragon
football

As you can see, these passwords exhibit little creativity or originality. Hackers can use lists of hundreds of common passwords to try to guess your password. They do not have to manually try each password; they can create short computer programs that will systematically go through the list until they hit one that works.

Hackers also use the dictionary to guess passwords. A fast computer can run through a big dictionary and use each word to try to guess your password. If your password is a word that can be found in a dictionary or a common name, they will quickly find it.

If you want to be more creative (more secure) you need to think about how hard it would be for someone to use a computer program to guess your password. A password that consists of only one number between zero and ten only has ten possibilities to test. If the password has two numbers the possible combinations becomes ten times ten or one hundred possible combinations.

To calculate how many combinations exist in a password you first add up the number of possibilities for each character in the password.

For example:

If you use only numbers, you have ten possible choices for each character in the password. If you use only lower case alpha characters you have 26 choices for each character.
If you use upper and lower case alpha characters you have 52 possibilities.
If you use upper and lower case alpha characters and numbers you have 62 possibilities. If you also include a special character such as a #@%:, there are 94 possibilities.

To find out the total possible combinations for a given password you take the total possible combinations for a single character and multiply it by itself by the number of times equal to the length of your password.

If you have a three character password using lower case alpha characters and numbers the total number of combinations is 62*62*62 = 238,328. Now this may seem like a large number of combinations but computers are fast. A modern home computer could crank through all of those combinations within an hour or two. If your password consisted of ten characters the number of combinations would be about 62 raised to the 10^{th} power which is a very large number. It is a large

enough it becomes impractical for a really powerful computer to process in less than many decades. Use passwords that are at least ten characters long that consist of numbers, upper and lower case and some special characters. How do you remember such a long password? The secret is to use a “pass phrase” instead.

Pick a simple phrase you can remember, for example: TheSkyIsBlue and then add in some numbers that you will remember TheSkyIsBlue##60148. The number can be an old address or zip code or telephone number that you can easily remember. Since all the words are run together, the word cannot be found in a dictionary and the use of numbers and upper and lower case letters and a special character makes the password a very strong password.

It is also a good idea to not use the same password on all accounts. Use one password for all of the “low risk” accounts such as Facebook, Blogger, etc. Use a second or third password for high risk accounts such as Internet banking or investing.

A few simple precautions and the use of a strong password will go a long way to keeping your Internet experience secure.