Computer Security

These guidelines below can help you to keep your computer from getting infected by malware:

1. **Keep your system up to date.** Enable the Microsoft automatic updates. It is important to do these updates since they are fixing software problems that might allow someone to infect or take over your computer

2. **Be very careful when clicking on links that appear on web pages or in email.** Links appear in the form of blue underlined words, **OK** or **Submit** buttons, or **images** in advertisements. Clicking on a link takes you to a page on another computer. 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 execute code to infect 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. **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.

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. **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.

7. **Beware of "Pop-ups".** These are windows that "pop-up" on your desktop when you are using the Internet and often ask you to click OK to fix your computer or to scan for a virus. **These "pop-ups" are always malware trying to infect your computer**.

8. **Choose Internet shopping sites carefully.** Name sites like Penney's, Sears, Amazon, or government sites are usually safe and secure. You can often search for a business on Google and find information about their trustworthiness. On many sites when you download a file, for example a music or video file from a peer to peer music sharing site, you may also get malware designed to infect or take over your computer.

9. **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.

10. **DO NOT click on advertisements** that offer free downloads such as screen savers.

11. **DO NOT ever 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 a credit card company. It will have official logos and look very legitimate.

12. **Use good passwords –** Passwords should be at least 12 characters long and contain upper and lower case characters and numbers. A pass phrase is easier to remember, for example, "DecemberSnow25".