Safety on the Internet - To Click or not to Click

In Part 1 of this series, we went over definitions and concluded that all viruses, spyware, bots, etc. are categories of **malware**. In Part 2, we learned that anti-virus programs can never protect a user from all malware, so we have to be **smart internet users**. In Part 3, we will teach you a couple of ways to avoid installing malware on your computer.

PART 3 – How we inadvertently install malware on our computers

It is getting harder for the common user to determine what is safe and what is not safe on the internet. The most important key to avoid becoming a victim of malware is to be a savvy internet user. It's the same way you avoid telephone or mail scams. Be skeptical; pause and think before you click.

Downloading Free Software

Most free software these days delivers a package that includes **add-on software we might not want**. When downloading any program, take these steps:

1. Often there are several download buttons on the download page. Be careful to choose the one that specifies just the software you want. It will NOT be flashing to draw your attention!
2. After you press the correct download button, READ each window that pops up before you click "agree" or "install" or "next."
3. Sometimes the window asks you to agree to install the add-on software. It's OK to click "disagree," you'll still be able to continue with the installation.
4. Sometimes a window includes boxes that are already checked to include added software. Be sure to uncheck these boxes if you don't want the add-on programs.
5. There will be a point where a window asks you to agree to the program's "Terms and Conditions." At this point, you MUST click "agree" to continue with the installation, but if you click "disagree," you'll still be able to go back and click "agree" so never be worried about clicking "disagree."

Unscrupulous websites

Websites that border on the illegal or are outright illegal very often have malicious software embedded in the site. The malicious software will install on your computer automatically on your visit or as soon as you click on something on the site. If you want to keep your computer clean, stay away from marginal websites. Be careful of "free" music, video, and other entertainment sites. Don't click on enticing ads or pictures.

Discount shopping browser plug-ins

Plug-ins, add-ons, or extensions are little software programs that get attached to your website browser (*Internet Explorer, Google Chrome, Firefox, Safari*) either purposely or inadvertently. Some claim to be helpful by providing coupons or showing you better prices. Most shopping add-ons come in a form of adware. Some to stay away from are *Dealio* and *Pricegong*. You may think you are getting a deal, but your browsing habits are being monitored and you will start getting annoying pop-ups showing shopping deals everywhere you go on the internet. Most of these types of add-ons can either be uninstalled in the Windows control panel or disabled in the browser settings.

Pop-up windows can indicate infection

If you have a window that pops up and starts scanning your computer, you most likely already have a virus. Malicious software is created to make the creators an economic profit. Here are some things that usually occur after an infection:

1. Your web browser is hijacked. This means that either your home page is changed, or your search engine is changed or both. When you use the internet to search for something, the virus will take over the search and send you

to pages that offer up ads related to your search but limited to the companies that paid the virus creator to hijack your browser. In other words, your use of the resources on the internet is now extremely limited and not representative of what is available to folk who don't have this virus.

2. Your computer is locked up and "held for ransom." A window will pop-up telling you that to get the virus off your computer so your computer functions again, you will need to *"pay $xx to ABC company, or call this 800 number. Click here to make payment."* **DON'T click, call, or pay**. **And never allow anyone to remotely log into or control your computer unless you already know him/her to be a reputable specialist.**

Both of these virus conditions can be remedied by a computer repair specialist. The sooner you get the virus removed, the easier and less expensive the repair will be.

In Part 4 of this article series, I will share even more ways to avoid malware.

Mark Rudiger has been troubleshooting computers for over 20 years. He owns Lake County Websites & Computer Repair which is located in Middletown. You may contact Mark by calling 707-987-1923 or emailing web@lakecountywebsites.com.
Website: www.lakecountywebsites.com