



What you can do to minimize your exposure to viruses.

1. Be wary on what your clicking on. The latest viruses are coming in through the user clicking on something that looks legitimate. For example; one user saw a video of Michael Jackson. When clicking on the video it directed the user to “install this video player to view the video”. The user then clicked on the download and unknowingly installed a virus.

Here is what you can do: If your computer tells you to install something. Look at what it is you “need to install” if says you need shockwave or adobe check to see if you already have it in your programs list.

2. Eliminate the “cutesy”. A lot of people like to have a good look and feel to their computer. But be wary cutesy comes with a price. Much of the free software that people download to change the appearance of your mouse or desktop etc can be installing malicious software on your computer without your knowledge. We ALL do not spend time reading that user agreement that we all click “I accept” so that we can install the software.

Here is what you can do: Changing your wallpaper is a part of windows. You can do this without harming the computer. You can also at least create restore points on your computer before installing software that your unsure of.

3. Watch what your downloading. If your someone who does a lot of downloading, you may not know if the source is legitimate or not. Always be wary of what your downloading and ask your self if downloading something your unsure of is worth compromising your computer.

Here is what you can do: Do a quick search on Google for websites or software that you think may be harmful to your computer.

4. Never ever ever pay for something that tells you that it will remove your “infections” and asks you to pay with your credit card. Many of these scams are out to get your money for the infections that they put in your computer.

Here is what you can do: If you already paid for it call your bank right away and cancel your card. If your not sure if its something legit again, do a quick search online.

5. Just because an email is coming from a trusted source does NOT mean the email is safe, especially emails with attachments.

Here is what you can do: Most antivirus programs have email scanners with them. Use a program that supports your email scanner for example; outlook, windows mail or thunderbird and enable your email scanner settings. Be wary of attachments and contact the sender to verify they are legit.

6. Websites with advertisements are not checking the codes of the ads to verify that there is not spam in the ad’s source code.

Here is what you can do: Don’t leave your WebPages open if you aren’t at the computer. This will limit your exposure to rotating banner advertisements.