Virus Safety Guide

1. Don't use the same password over and over

This may come as news to you, but whenever there is a breach in a company's database or information, emails, passwords, names and other confidential information is what usually gets posted online. You can check if your information has been posted online here, just type in your email address and it will tell you if your account is posted online somewhere.

2. Avoid visiting questionable websites

Whether you mean to or not, you may end up at a questionable website. You might click on a pop-up ad or a bad link in an e-mail. Either way these types of websites do NOT have your best intentions in mind. To avoid pop-ups or other questionable blockers, check out services such as Adlock Plus for Google Chrome or Firefox.

3. Keep software updated

One of the easiest ways for hackers to access your computer is by not updating your software. Software makers are always plugging security holes to prevent this from happening, but if you don't have the latest version, you can be more likely to become a victim.

4. Avoid downloading illegal online content

Sure it is easy to get the latest music, movies, or games online but should you? No. One, it's illegal. Two, it can really cause some serious issues. Hackers know lots of people are searching for free content like this online so they put viruses and Trojan viruses into illegal content. It is just waiting for you to download and run it.

5. Practice safe web searching

Make sure you use the real Google, Yahoo or Bing as your search engine rather than another browser. Sometimes a toolbar will change your search engine to theirs so they can make some money from advertisements.

6. Don't click unknown links in your e-mail

This one is very essential now-a-days because everyone gets a few hundred e-mail messages a day. Most of them are spam but a few of them look legit because they claim to be from your bank, courier services or some other well-known company. They are just there to get you to click a link then steal your login information.

7. Don't install junk software

Free is not always the best option. Free comes with a few extra things most of the time. Who would spend all that time making a program then just give it away? Most of the time they expect you to just hit next when installing and also install their partner advertisements and junk on to your computer.

8. Keep virus or malware scanners or software up-to-date

By not updating your scanners you are basically scanning your computer for viruses that are old. Most scanners now update their virus definitions hourly or at least daily. So it is very important to check in with your scanner at least once a week and make sure all is running smooth. Generally they have a dashboard that will let you know.

For a more comprehensive guide, visit: **http://www.wikihow.com/Avoid-Getting-a-Computer-Virus-or-Worm**

Source: http://www.angieslist.com/articles/how-avoid-computer-virus.htm