How to prevent spyware & malware

The best defense against spyware and other unwanted software is not to download it in the first place. Here are a few helpful tips that can protect you from downloading software you don't want:

1. Don’t click on links within pop-up windows. Pop-up windows are often a product of spyware. Clicking on the window may install spyware on your computer. Instead, close these windows by clicking on the “X” icon in the title bar and not on the “close” link within the window.

2. Choose “no” when asked unexpected questions. Be wary of unexpected dialog boxes asking whether you want to run a particular program or perform another type of task. Always select “no” or “cancel,” or close the dialog box by clicking the “X” icon in the title bar.

3. Be wary of free downloadable software. Free is not free when malware installs on your computer. Many sites offer customized toolbars or free downloads (screensavers, background images, music files, other free downloads). These sites often use spyware. Viruses can even be in pictures you download and save to your computer. Don’t download programs or images from sites you don’t trust. Another very common way of getting malware infections is the use of P2P software such as Vuze, Kazaa, Morpheus, or any type of torrent (used for downloading music, TV and movies).

4. Don’t follow email links claiming to offer anti-spyware software. Like email viruses, the links may serve the opposite purpose and actually install the spyware it claims to be eliminating. Never trust emails with links to security updates.

5. Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.

6. Use the latest browser. Microsoft Internet Explorer is the main built-in browser on most computers and it needs to be updated every few months. This can easily be done with Windows Updates.

7. Adjust your browser security settings for Internet zone to medium (or higher). If your browser security settings are set too low, you can get spyware just from visiting a web site. Make sure your browser security setting is at least at medium in order to prevent spyware from getting installed when you browse the Internet. Read: www.cert.org/tech_tips/securing_browser/ for details.

8. Be wary of opening random attachments or links even if it’s from friends or family and especially if it’s supposed to be something funny. Viruses can sometimes read a whole address book and email everyone on it. If the wording of the message doesn’t sound like your friend or family member, call or email them and ask if they really sent it. If in doubt, have an anti-virus program scan the file before you run it.

9. Don’t download special media players. Streaming media websites might seem harmless, but watching or listening to streaming media may mean downloading a special media player that could contain malware.

10. Adjust your browser preferences to limit pop-up windows and cookies. Pop-up windows are often generated by scripting or active content (client-side script: a small program that is attached to HTML documents and run (executed) on the user's browser while viewing said document.).

11. Beware of phishing schemes. A phishing scheme starts when you receive an email from a website claiming to be your bank or credit card company. You are asked to click a link and log in, but the truth is that you've just given away all of your personal information. Often, when you visit these sites, spyware, adware and viruses are automatically installed on your computer. Your lender or credit card company will often send out a real notice that lets you know that a phishing scheme is going around. The smartest thing you can do is to simply call your bank or credit card company if you receive an email saying there is a problem with your account instead of blindly following links in your email.

12. Beware of fake anti-virus software.

How do you know if there is spyware on your computer? The following symptoms may indicate that spyware is installed on your computer:

1. you are subjected to endless pop-up windows
2. you are redirected to web sites other than the one you typed into your browser
3. new, unexpected toolbars appear in your web browser
4. new, unexpected icons appear in the task tray at the bottom of your screen
5. your browser's home page suddenly changed
6. the search engine your browser opens when you click "search" has been changed
7. certain keys fail to work in your browser (e.g., the tab key doesn't work when you are moving to the next field within a form)
8. random Windows error messages begin to appear
9. your computer suddenly seems very slow when opening programs or processing tasks (saving files, etc.)

There are dozens of anti-virus and anti-spyware programs you can download for free on the Internet and a surprising number of them actually do exactly the **opposite** of what they claim. The product websites make outrageous claims that their product can protect you from a whole range of threats, when, in reality, their product installs malware on your machine. Only download antivirus programs from trusted sites or from websites that you know are completely legitimate.

George Rettich, Owner of Webspinner Computer Service. 604-217-0320

Email anytime Webspinner@me.com

Webspinner
Computer Service