



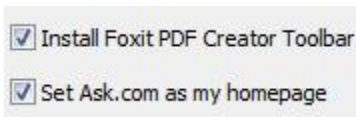
How to Avoid Viruses and Malware



Beware of any email from **unknown senders**. Beware of messages that **seem strange** or that **seem like advertisements** – even if you know the sender. Your contacts' email could be hacked. **Beware of all links** – regardless of the source.



When you are downloading a program (from a reputable website of course), beware of fake Download buttons. Sometimes on a download page, **only one of several download links are real**. Watch out for the obvious big green buttons! They're usually fake. The real link is usually more subtle.



Be cautious **when installing software or updating existing software**. Software vendors are paid to bundle their software with add-on browser toolbars and internet tracking software (adware). When going through the installation process, **read what each checkbox says** and make sure you are only installing the program you intend to.



Programs that claim to "**Speed Up Your Computer!**" or "Clean Up Your Registry" or "Scan Your Computer for Viruses and Malware!" often **do the opposite**. These programs are infamous for being trojans/viruses. Only trust reputable antivirus and antimalware programs (see below) if needed. Prevention is the best medicine for viruses.



Websites offering **free screensavers, wallpapers, icons, themes, fonts, or mouse cursors** are generally loaded with some type of malware. **Pornographic** websites often leave tracking software (which result in pop-ups) or viruses on a computer.



Keep programs like your web browser, antivirus, and operating system **up to date**. Install Java and Adobe product updates as they become available.



A good anti-virus program is important, but not all anti-virus programs are effective. If you need help, please contact us so we can recommend a highly-rated antivirus and help with installation and renewal as well.