**1. Fill in the blanks with suitable words (one or two words in each gap)**

**Third party applications**

Third party applications are programs **develop/written/created/designed/ devised** to work within operating systems, but are written **by** individuals or companies other **than** the provider of the [operating system](http://www.wisegeek.com/what-is-an-operating-system.htm). For example, Microsoft® systems come packed with several software applications. Of these, any program authored by Microsoft **is** a first party application. Any program authored by a different company or **an** individual is a third party application; the same being true for Apple™ and Linux™ systems. In this equation the second party is the user.

Third party applications **can be** standalone programs or they can be small plugins that add functionality to an existing parent program. The former category is endless. On a typical system, standalone third party applications **include/have** tens of dozens of programs. [Web browsers](http://i.wisegeek.com/what-is-a-web-browser.htm) like Opera, Safari® and Firefox®; and [email](http://www.wisegeek.com/what-is-email.htm) clients like Thunderbird®, The Bat!, and Pegasus are some examples of popular standalone third party applications. **Most** anti-virus programs, firewalls, multimedia programs — virtually any program not written by Microsoft®, Apple®, or Linux, yet made to work on those systems — fall **into** this category.

In some cases, computer users of Windows® operating systems consider **it** more secure to use standalone third party applications for tasks **such as/for example/for instance** email, newsgroups, Web browsing and Internet Relay Chat (IRC). Microsoft® applications **have** traditionally **been** the target of the vast majority of hackers, viruses, Trojans and other security threats. By using a third party application, one theoretically lessens/ the degree of potential vulnerability.