

## Protect Yourself Against Malicious Internet Spyware and Trojans

Even with the advent of the new powerful OS like Windows Vista and Apple Leopard, people must be very cautious when visiting malicious websites. You could think that only surfing, without downloading or opening suspicious email attachments, would be a safe activity. You are wrong, very wrong. Nowadays, the internet criminals have invented all sort of things to try to steal your personal info (credit card or bank details, physical address, identity) for their illegal activities.

One of them is the use of ActiveX or Javascript embedded in the page, in practice by just opening the page in your browser, if you're not very careful, you can automatically download, install and execute very dangerous programs called "trojans" that reside on your pc and start everytime you boot your computer, sending your information over the net to specific email address or computer connected to the network.

So beside using a good antivirus, is always good to follow this guideline: avoid completely visiting unknown or suspicious website, look at Google's advice in search results (they have added a text saying "this website can harm your computer") and add plugins to your browser to block the execution of ActiveX and Javascript elements in the webpages, unless you give them authorization.

Both Firefox and Internet Explorer have in the options menu the possibility to disable execution of Java or ActiveX component, and I recommend you turn those off unless you know it's a trusted site.

On Apple Macintosh computers the risks are really limited, since there is no ActiveX and in general the Apple OS is very well designed for security. As of today very few virus exist, and the only way to be infected is actually opening an executable, so the risks are very low in this regard.

Another thing to watch is the presence of a secure connection when buying anything online. You can instantly notice if you're using a safe encrypted connection just looking at the lock icon displayed on the bottom of your browser status bar.

If the icon is not present, absolutely avoid entering any personal information in the webpage, because it could be easily intercepted and used for other purposes by anyone.

Other way to check the reliability of a website is to look if in the order page is present a link to certified sites like Scanalert and Verisign. You should see clickable icons that you can use to verify the attendibility of the website you're about to make a purchase on.

Another thing to watch for is website that ask for lots of personal information: those are absolutely not required unless you're actually making a purchase. But never enter your real name address, ID, phone number and so on because you expose yourself to the so called "Identity Theft". This means that the criminals can use your personal info to commit fraudulent or illegal act in your behalf, so better be very prudent when a website asks for lot of info without any real reason.

A good way to avoid this is using Paypal, a system which lets you protect your personal info (only the email address is exposed), so if you are interested in buying something online, always check first if you can do it through the Paypal system.

Speaking of Paypal, another danger you could face is the so-called "Phishing", which means that you'll receive emails that looks exactly like Paypal (or other common online stores like eBay) asking you to enter your user/password again, but in real they are just redirecting to a fake website to steal your access info. So watch out for those, since no site will ever send you an email asking to re-enter your user and password.

In conclusion, following the simple step I've described in this article is easy to have a safe browsing experience, without any risk for you and for your family.

### About the Author

Riva Celso is an independent shareware author developing games for pc and mac computers. Among his favourite genres, there are [strategy games](#) and [rpg games](#).

Source: <http://www.tntarticles.com>