

What is Sandboxing?

Most modern viral and spyware infections are triggered by visiting poisoned web sites that have hidden malware code. Although many anti-virus software companies are now incorporating black-listing as part of their service, these lists are not updated frequently enough to be effective blocking technology against rapidly developing web threats. Because of the tenacious nature of the latest malware technology, removing infections from computer systems and networks has become more and more difficult - almost to the point that saving the hard drive contents is no longer cost effective. **It's always a better solution to prevent malware from infecting your systems in the first place, which can be accomplished using web browser-based sandboxing software.**

Sandboxing software is simply a way to wrap your internet browser within a virtual environment. Any malicious code that attempts to install on your computer will instead install itself in the virtual storage within the sandbox. When you exit your browser, the sandbox is then purged, along with any possible malware.

Sandboxie, is an example of web browser sandbox software, and is available for download at www.sandboxie.com. It can be used for free, however, the paid version has some interesting special features, including sandboxing any software that you specify, such as your e-mail program. Another example is **Buffer Zone** from www.trustware.com.

One way to visualize how sandboxing works is to think of it as wearing protective "gloves". While wearing gloves you are free to "touch" as many web sites as you wish, all without the fear of infecting your computer with any malware. When you're done using the internet, just "peel-off the gloves" and you're as clean as when you started. This is how sandboxing works - by preventing your computer from directly "touching" the internet as you surf.

As malware becomes more sophisticated, removing infections becomes more difficult, resulting in possible data loss and costly service calls. If you install and use sandbox software, you are taking a proactive step to prevent infections. Be aware however, that sandboxing is just one step in an overall approach to security. It is very important to install and maintain an effective anti-virus/anti-spyware solution, and to insure that your operating system and programs are all up to date with the latest security patches, which should include Adobe Reader, Macromedia Flash Player, and Java updates.

For more information, contact your security specialist at Genesys Micro LLC at 304-267-0433