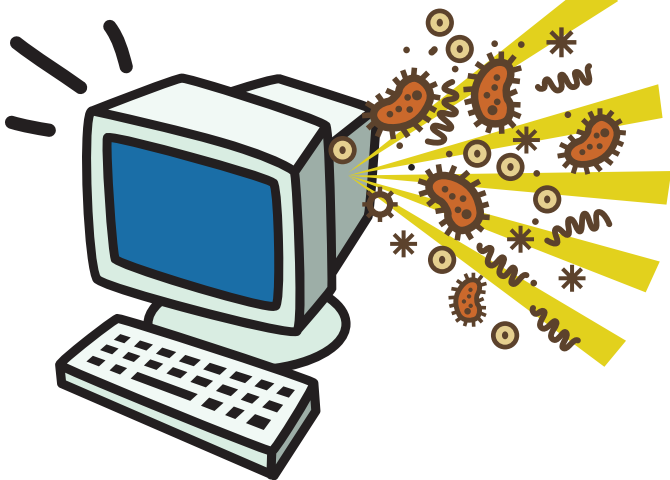


# Security: Viruses & Malware threats

Security from viruses and spyware on your PC begins with a state-of-mind. It is being aware that websites are trying to actively infect your PC with malware, adware and other threats. It is recognizing that if the site is not a known, trusted one it is potentially dangerous.

Put your into preventing infection, instead of hoping your anti-virus application will catch it once it's inside.

Remember the basics. Update



and patch your operating system often. Update your browser and the plug-ins you use, such as Java and Flash, as well.

Never click e-mail attachments from unknown sources. Be suspicious of attachments from friends.

Never install software from companies or websites you don't know and trust. Do not click a button allowing an executable (ends in ".exe"), plugin or add-on (like a toolbar) to be installed from a website you don't know to be trustworthy.

Use a software or (preferably) hardware dedicated firewall to prevent intrusion, and limit the exceptions to the firewall.

Be aware that simply entering some websites will cause your computer to become infected by worms and/or viruses. These websites do not require any interaction on your part, they exploit weaknesses found in Windows and Internet Explorer (use Firefox or Opera web browsers for a little bit more security).

For those wishing to go the extra mile, install a "sandbox" that isolates your browser, preventing infection.

With the basics covered, realize

that it is no longer safe to use a single anti-virus program, experts say. Viruses have evolved, even in the short time since we last covered this topic. They believe now there is virtually no chance you can stop the more sophisticated threats once they have had the opportunity to execute inside your system.

Some viruses can now terminate the anti-virus processes (programs) that are running on your computer, and then infect

your system at will. According to recent tests by independent organizations, the anti-virus application that is best prepared to defend itself against termination is Symantec's Norton Anti-Virus (NAV). NAV is however, susceptible to infection itself, and so is not enough. NAV also has longstanding problems with interaction- in that it causes problems with installed applications and drivers in some instances. A second, less-vulnerable application is needed.

#### • Free Anti-Virus applications

<http://www.avira.de> (Avira) Good features, annoying nag screens.

<http://free.grisoft.com> (AVG)

Includes the recommended rootkit scanner and spyware tools as well.

<http://www.avast.com> (Avast!)

Includes free cleaning tool available for download.

The preferred configuration is Norton Anti-virus also running Avira (pro edition- not free), although any two running concurrently will be better than one or none.

Rootkits are often the most dangerous of the maladies that can befall your computer, and

most anti-virus companies have released applications that can find these and get rid of them. We recommend you download and use all three of these products once (along with Avast's excellent cleaning tool), to clean your system before switching or adding anti-virus applications.

#### • Free Rootkit Tools

<http://www.f-secure.com/blacklight>

<http://www.sysinternals.com/Utilities/RootkitRevealer.html>

Microsoft's Online Alware Remover

<http://www.microsoft.com/security/malwareremove/default.msp>

(requires you to use Internet Explorer as opposed to other web browsers)

Removing rootkits first require us to know what they do and why. Rootkits work by changing Windows in order to hide another program while it is running. Most anti-virus applications cannot find rootkits or remove them. Because of the way they work, they are hidden from view by you, and your software. You need to first find and remove the rootkit, and then remove the virus or spyware it was hiding.

Sometimes removing the rootkit can cause system instability. Backup your data before you proceed. After using the rootkit

## Using a Sandbox

Now knowing that merely visiting a website can infect your machine, and that short of disabling Java and Flash and other plugins, there is virtually no defense, what do we do? First avoid websites you don't trust, that show up in searches as random URLs instead of ordinary site names. Don't visit serial number or crack download sites, avoid using P2P sharing programs. Then you can use a "sandbox".

This is essentially a program that creates a "virtual environment" for your browser to run inside of, isolating it from the main system. Not all sandboxes are created equally, however. Like anti-virus programs, new hacks and malicious code can force them to terminate (shut down) leaving you defenseless.

These are the only three sandbox programs currently recommended as resisting termination and still effectively isolating your system. They're not all free, and not necessarily easy to use. But it is worth the effort to try if you frequent websites you don't know are safe. Remember, places like MySpace, PhotoBucket and other popular media-sharing sites are often places hackers upload infected files.

[www.sandboxie.com](http://www.sandboxie.com) (\$Donationware)

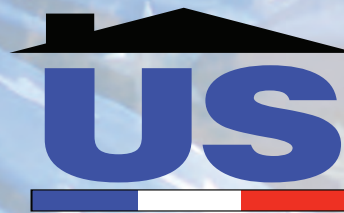
[www.softsphere.com](http://www.softsphere.com) (\$29, free 30-day trial)

[www.greenborder.com](http://www.greenborder.com) (\$30, free trial)

[www.mojopac.com](http://www.mojopac.com) (\$30, free trial)

scanners, unhook your internet, reboot your PC and run your anti-virus performing a deep, intensive scan of the entire system. Cleaning the system first will let

your additional anti-virus or spyware applications start out uninfected, and have a better chance of protecting you.



## U.S. Mortgage Group

When experience counts...

*Count on US!*

**Better Rates • Better Service • Better Loans**



**Matt Redd**



**Carrie Judas**



**Katie Harker**



**Stacey Cottrell**

573-302-4949 | 3736 Hwy 54 | PO Box 1483 | Lake Ozark, MO 65049

Toll Free 877-302-4949

[www.usmortgagegroup.net](http://www.usmortgagegroup.net)