REMOVING SPYWARE, VIRUSES AND OTHER MALWARE FROM WINDOWS

For voluntary sector staff who use computers all day, system glitches can bring important work to a grinding halt. While you can often prevent trouble on Windows machines through regular maintenance (see the knowledgebase article "Good Housekeeping" for more information), sometimes trouble finds you in the form of malware — *software* designed to damage or disrupt your computer system. Malware — **mal**icious soft**ware** — includes viruses, worms, and other software installed by hackers. Spyware and*adware*, while not necessarily malicious, is similarly undesirable.
Such software can wreak all sorts of havoc on your computer. It can hog memory, cause crashes, shut down your computer, steal personal data, change your system settings, or force your computer to attack other systems.

Fortunately, keeping this junk from infecting your computer is usually not hard:

- Install antivirus software and keep it up to date
- Use a hardware or software firewall (see the knowledgebase article onFirewalls for more information).
- Keep your computer up to date with security patches (use Windows Update regularly and / or visit Microsoft's security pages.
- Don't install file-trading programs like KaZaa that carry adware and transmit viruses

But we're all busy people. Maybe you forgot to update your *virus definitions* this week. Or maybe your co-worker's teenager installed file sharing software on your computer. However it happened, your system has been invaded by malware and you need to remove it.

Removing Malware the Easy Way

Sometimes getting rid of malware is easy. Adware like Gator and SaveNow can be removed using the Add/Remove Programs control panel in Windows.

1. In Windows XP Professional click on Start > Control Panel > Add/Remove Programs
   In Windows 2000 Professional / Windows ME / Windows 98, click on Start > Settings > Control Panel > Add/Remove Programs.
2. In the list of programs, locate the software you want to remove. If you see a program you don't recognise, look it up in Google to learn what it is.
3. Select the offending program and remove it with the "Remove" button.

Programs like Lavasoft's AdAware and Spybot Search and Destroy are free to download and are specifically designed to identify and remove spyware and adware components.

Removing Malware the Hard Way

Sometimes, removing malware isn't easy at all. It resists your attempts to remove it, reappearing like magic. It seems to mock your attempts to purge it from your system. Maybe you can't even figure out where the program is or what to remove.

Don't worry -- you don't have to reinstall your system (although that works). But you do have to do a little work. If the problem is a persistent program that repairs itself as you try to remove it, odds are good you're not the first person to run into this problem. Someone has probably identified the perfect solution.

If you know the name of any component of the software, search for it on the Web (e.g. on Google or in Google's Usenet archive, and you might find information about how to remove it. But maybe you can't find an answer. How do you get rid of a program like this? This situation falls into the category of security incident response. Some program is interfering with the confidentiality, integrity, or availability of your system, and you want to recover from it.
It doesn't matter what the program is; the same steps can be used to identify and remove it. If you are recovering from an intrusion by a hacker, this article can't tell you everything you need to know. There are other steps to perform before removing the malware. You might want to leave the foreign program running in an attempt to gather intelligence on the hacker. Contacting the appropriate authorities might be a step in some situations. If you hope to prosecute the intruder, you must proceed carefully in order to avoid destroying evidence of the crime.

But let's say you have just some nasty tricky spyware or a stubborn virus on your system, and you cannot remove it by the regular techniques. Proceed with the following:

Find the process(es) and kill them

A process is a computer program that is actively running. In Windows NT, 2000, and XP, it's easy to view the list of processes. Then you can find the offending process and stop it.

1. Right-click on the taskbar and choose Task Manager from the menu that appears.
2. Click on the Processes tab to view the list of running processes
3. Click on the Image Name header to sort the list by name

4. Now the hard part. Plug the name of each process that you do not recognise into Google. Find out what they are. Come up with a list of processes that you know or suspect are related to your malware
5. Kill the processes by right-clicking on them and choosing End Process

Sometimes you can't kill the processes that way. You might get the message "Access denied." But are you going to let some spyware flack tell you what you can and can't do on your own computer? When you have administrative rights and everything? I didn't think so.

If the process cannot be killed in the Task Manager, it's time to bring out the heavy artillery.

Pskill.exe from SysInternals will blow away any process running on your system or even on a remote system you have an account on. You have to run it from the command line, but it's easy to use.

1. Download the archive of the program
2. Extract the program from the .Zip archive. You might need a decompression utility like StuffIT Expander or Winzip
3. Move the program, pskill.exe, to your C: drive
4. Open a command window: Click Start, then Run, type cmd and click OK
5. In the command window type C:pskill.exe and the name of the process you wish to kill, then press enter. For example, if you wanted to kill the process for Microsoft Word, you would type:
   C:pskill.exe winword.exe
   In this example, Pskill would respond with:
   Process winword.exe killed

Stop the program from running on start up

OK, so the program isn't running anymore. But how do you keep these processes from returning like decomposing corpses from Evil Dead? Somewhere on your system, a component of the spyware is set to automatically run when you start up your computer. But where is it? Is it in the registry? Is it in the start up folder? Or *boot*.ini?
It could be any of a number of places. Fortunately, Sysinternals comes to your rescue once again.

Autoruns.exe is an applet that displays most of the places where a program can be automatically set to run in Windows. When you find the malware, delete it. Be careful not to delete a program just because it has a cryptic name. Do your best to confirm that the file or *registry* entry is actually part of your problem, or you might accidentally end up removing a valid portion of your system.

Clean up the mess

Now that the process is dead and it isn't set to start up automatically, you're all set. You can go further and look for registry entries or try to remove all the components, but once the malware isn't running, and you stop it from starting up again, the program is defeated. All that remains is to clean up as best you can.

Next Steps

It's time for a little reflection. If you actually had to respond to an incident like this, consider what made your system vulnerable in the first place. Was it something you did? Was it something you didn't do? Identify your vulnerabilities so you can take corrective action to ensure your future experiences with malware are limited. Again, the actions described in this article can be used to assist in various malware scenarios, including when a server has been hacked and an intruder may have left a program running.

Source : http://www.ictknowledgebase.org.uk/removingmalware