

## Re: Winvnc hack! [25 KB]

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2002-10/10477.html>

---

**From:** Karl Levinson [x y] mvp ([levinson\\_k@excite.com](mailto:levinson_k@excite.com))

**Date:** 10/29/02

From: "Karl Levinson [x y] mvp" <[levinson\\_k@excite.com](mailto:levinson_k@excite.com)>

Date: Tue, 29 Oct 2002 17:04:51 -0500

"Roberto" <[monserrock@hotmail.com](mailto:monserrock@hotmail.com)> wrote in message  
news:OXEIIB5fCHA.1104@tkmsftngp11...

> *Hello, can anyone tell me a way to see how my system was hacked.*

Rebooted

> *machine and noticed that winvnc was running. Checked the files and saw it*

> *had been installed and all associations removed, except for the executable*

> *which they tried to hide. Killed all connections and removed. Found a  
hack*

> *article on how this happened, tested myself on another box and was  
amazingly*

> *easy to do. How can I see where it came from and protect myself from this*

> *type of attack. Thanks!*

You won't be able to tell where this came from unless 1) you already have a firewall or router installed that logs source IP address, or 2) the hack came in from a service such as IIS that logs IP address. Check your IIS logs for entries that mention .EXE or % and that also have a code 200 or 502 and you may very well see exactly what commands were used.

To protect yourself from this sort of attack, you may seriously want to consider formatting and reinstalling Windows and everything else. The reason for this is that it is impossible to be 100% sure that you've found and removed all the back doors that the hacker may have added onto your system.

Most likely the hack occurred because you were missing Microsoft patches, hadn't configured your computer securely and also left services running such as IIS.

=====

How can I tell if I've been hacked?

A: This can be a complicated procedure and usually requires both prior experience with forensic investigations and knowledge of what the computer looked like [which files existed, which ports were open, etc.] or what a

similar computer looks like before being compromised.

Also, the procedures you follow may vary depending on your security needs. For example, performing some of the procedures below may modify the files on your computer so that it is not admissible as evidence in court. Other procedures below could alert a hacker to the fact that you are looking for her, causing her to delete evidence or retaliate against you in some way.

If this is a business computer, your company should seriously consider hiring a security consultant or contacting the appropriate local law enforcement agency, both for the initial forensic response and also to improve your security to avoid future intrusions.

Keep in mind during the investigation that this might NOT be a hacker intrusion and might instead be regular network activity or a worm. Books such as Incident Response, Hacker's Challenge and/or Hacking Exposed 3rd Edition may offer you more information on how to investigate intrusions.

You may consider performing the actions below:

1. Unplugging the network cable is one possible way to try to prevent further damage.
2. Use Fport or Vision from [www.foundstone.com/knowledge](http://www.foundstone.com/knowledge) or pslist / pstools from [www.sysinternals.com](http://www.sysinternals.com) to look at the open ports on your computer and the program or executable using that port. Some firewall software such as [www.sygate.com](http://www.sygate.com) will also tell you this information.

You can also use the NETSTAT -A command that comes with Windows to look at open ports; however, this will not identify which program is using the port.

If you're unsure about the purpose of a particular port or program, try searching an Internet search engine such as [www.google.com](http://www.google.com) for the name of the port or program, or try right-clicking on the file in question to see the properties. Or, you could even try to telnet to that port e.g. by typing TELNET LOCALHOST PORTNUMBER or TELNET COMPUTERTNAME PORTNUMBER [example, TELNET LOCALHOST 82 ] and press the Enter key a few times to see if any informative messages appear.

3. Consider using a file change checker, such as the unsupported free tool Languard File Integrity Checker at [www.gfi.com/languard/lantools-fic.htm](http://www.gfi.com/languard/lantools-fic.htm). Recently changed files on your system can sometimes indicate an intrusion. You could also find and list the files on your hard drives that have been modified in the past 3 days by clicking on Start, Search [or Find], Files or Folders, and setting the appropriate date [though note that this may change the "Last Accessed" date stamp on some of these files]. "The Forensic Toolkit" from [www.foundstone.com/knowledge](http://www.foundstone.com/knowledge) includes command-line tools to list files without modifying the date.

4. Inspect the programs that launch when Windows starts on your computer, by using MSCONFIG or Startup Cop. Suspicious programs starting when Windows

starts can indicate a successful intrusion. [These can also indicate less serious events such as a virus or worm infection or even the installation of a freeware or ad-ware program such as an MP3 music file-sharing program.] See the section in this FAQ entitled "I think there may be a suspicious program, Trojan, ad-ware, "porn dialer," etc. starting up on my computer when Windows starts" for more information on how to do this.

5. Check the logs on your computer, especially your Internet router or firewall logs, the IIS web and ftp server logs and Windows security event log. [This is probably the first thing to do if IIS web services are running on the computer.] Some of these logs may not exist if you have not already enabled them.

Many common hacks are first seen in the IIS web server logs. Any line in your web server log that contains % or .EXE and which also contains a 200 or 502 error code is cause for further investigation. If you are familiar with DOS commands, you may be able to see exactly what commands the intruder tried to execute. Keep in mind that every web server on the Internet will have suspicious looking entries from worms like Nimda, though these are not necessarily signs of a successful intrusion.

For more information on deciphering web server logs, see the section in this FAQ entitled "I keep seeing strange things in my IIS web server logs, like 'NNNNNNNNN' or 'GET /scripts/root.exe' Have I been hacked?"

6. Consider using a Trojan scanner. Antivirus programs generally detect some but not all of the most common Trojans and hacker tools. Some people choose to use a Trojan scanner in addition to antivirus.

For more information on where and how to locate and use free and not-free Trojan scanner software, see the section in this FAQ entitled "Which antivirus should I choose? Which antivirus is the best?"

7. Consider installing an antivirus program that is configured to automatically download updates daily.

For more information on where and how to locate and use free and not-free antivirus software, see the section in this FAQ entitled "Which antivirus should I choose? Which antivirus is the best?"

8. Consider running a port scanner [and/or a vulnerability scanner] to look for security flaws and configuration errors on your computers. For example, you might also run a port scanner against your computers to look for open ports. A particular open port might indicate the way a hack occurred and/or might give you a way to identify other infected computers. Begin with Vision, Fport and/or SuperScan from [www.foundstone.com/knowledge](http://www.foundstone.com/knowledge), MBSA from [www.microsoft.com/download](http://www.microsoft.com/download) and/or Languard Network Scanner from [www.gfi.com](http://www.gfi.com)

See the section in this FAQ entitled "How can I scan my computer or firewall to look for open ports or confirm that my machine is secure?" for more information.

9. Consider enabling or installing a firewall and/or a sniffer [either software or hardware based] to monitor and look for unusual network traffic. There are a number of free firewalls available on the Internet which can show network transmissions to and from your computer, such as [www.sygate.com](http://www.sygate.com), or you could use the Network Monitor which comes with Windows 2000 / XP / NT / .NET, or Ethereal at [www.ethereal.com](http://www.ethereal.com), or Windump at <http://windump.polito.it>

For more information on how and where to locate free and not-free firewall software and hardware, see the section in this FAQ entitled "Which firewall should I choose? Which firewall is the best?"

10. The third party web sites and tools below may also be helpful:

[www.sysinternals.com](http://www.sysinternals.com)

For example, some of the helpful free tools on this site include Filemon, Regmon and Process Explorer which all display activity on your computer you might not otherwise be able to see. These tools show which files, registry keys, .DLLs and other objects are currently being accessed and by which process.

Pstools is a group of tools including pslist, which lists detailed information about processes, and psloggedon, which displays who is logged onto your computer currently.

[www.foundstone.com/knowledge](http://www.foundstone.com/knowledge)

In addition to the Vision / Fport tools, one of the free tools on this site is NTLlast, a security event log analysis tool that helps identify who has gained access to the system, using the NT security event logs [assuming auditing has previously been turned on].

Also, the Forensic Toolkit is a collection of tools including:

- \* Afind, which lists recently accessed files without changing the date stamp on the file;
- \* Hfind, which scans the disk for hidden files;
- \* Sfind, which scans the disk for files hidden in data streams.

[www.incident-response.org/IRCR.htm](http://www.incident-response.org/IRCR.htm)

Incident Response Collection Report (IRCR) is a collection of forensic tools that automates many of the tasks a forensics expert might perform.

If you have trouble understanding the results of any of these tools, you can post your results along with your question to an appropriate Usenet newsgroup. Note that the Microsoft newsgroups may not be the place to get the best answers to your questions, though you can try and see what happens.

[Thanks to Susan Bradley, Rob Lee and others]

=====

How can I re-secure my computer or server after being hacked?

If your computer or server has been compromised, it is highly recommended that you follow this procedure to secure your computer:

1. Hire someone with security experience to investigate your computer and confirm that it has been hacked, learn how it was hacked, collect evidence, confirm that your other computers have not been hacked, etc.;
2. Back up your data files;
3. Format the hard drives;
4. Reinstall Windows and all other software onto the computer;
5. Do not put the computer back on the network or the Internet until the previous steps are completed [since un-secured computers on the Internet can be hacked within 15 minutes].
6. Follow the further instructions for securing your computer by reading the section in this FAQ entitled "How can I harden my computer or server to secure it from hackers?"

This procedure [formatting and reinstalling] is recommended because it is difficult to be certain that you have found and removed all changes the intruder made to your computer. If the hacker added a login ID, changed a password, installed remote control software, etc. onto your computer, the hacker or other hackers could easily get back into your computer.

If you wish, you can take the chance and just try your best to remove everything you can find, but then you may still be at risk. Instructions for how to manually re-secure your system without formatting and reinstalling everything can be complex and are beyond the scope of this FAQ. However, some general tips are given in the section in this FAQ entitled "How can I tell if I've been hacked?"

BEFORE you format and reinstall Windows, it may be a good idea to have someone investigate the computer to look for clues as to how the computer was compromised and by whom. This information can help you to:

1. Confirm that you really were hacked, possibly saving you from needlessly formatting and reinstalling Windows on your computer;
2. Find other machines on your network that were also hacked;
3. Learn what mistakes were made that allowed the computer to be compromised and avoid making those mistakes in the future.

Instructions for how to determine whether or not you've been hacked are complex and are beyond the scope of this FAQ. However, some general tips are given in the section in this FAQ entitled "How can I tell if I've been hacked?"

Note that unless you are already experienced in forensics, any actions you take on your computer will probably reduce your ability to use your computer as evidence in a court of law, and could provoke the hacker into retaliating

against you in some way. [On the other hand, your chances of being able to find and prosecute the hacker are slim, unless you are a business, or a government entity, or can prove substantial financial loss as a result of the hacking. If you fall into one of these categories, you should contact a local law enforcement agency, such as the local FBI office in your city if you are in the U.S.]

=====

How can I harden my computer or server to secure it from hackers?

A: [Note that if you have already been hacked, this section will not help you re-secure your computer. In this case, you should first read the section in this FAQ entitled "How can I re-secure my computer or server after being hacked?"]

Here is the short answer:

1. Do not put the computer onto the network or the Internet until after the computer has been hardened using the instructions below [or at least not before a firewall and antivirus have been installed].
2. Use firewall software and hardware and antivirus software that is configured to download updates every day;
3. Follow the instructions for hardening Windows and IIS at [www.microsoft.com/technet/security](http://www.microsoft.com/technet/security) ;
4. Install all service packs and security fixes from Microsoft and otherwise for all Microsoft software on your computer [Windows, IIS, Office, Internet Explorer, Windows Media Player, etc.] from [www.microsoft.com/technet/security](http://www.microsoft.com/technet/security) ;
5. [Ongoing] Download MBSA from [www.microsoft.com/download](http://www.microsoft.com/download) and run it now and also at regular intervals to look for vulnerabilities in your settings, new patches that are missing, etc. Also, check your antivirus to confirm that the last successful update was less than 14 days ago.

These steps will make your computer fairly secure, but may still leave some holes. Keep reading below for additional information you should be aware of:

A successful hacker, virus or worm intrusion into one of your computers can drain your free disk space, slow down your Internet connection, compromise your credit card numbers, damage your personal documents, allow intruders to access other machines on your network that DO contain important files, and/or leave you legally liable for other government or business computers on the Internet that are hacked by an intruder using your computer. This is why you should consider securing ALL the computer systems in your home or network, even if you think there is nothing important on the computer or it is "just a test computer."

All Windows users should seriously consider all of the procedures below to help prevent intrusions on their computers:

1. Do not put the computer onto the network or the Internet until after the computer has been hardened using the instructions below. [Un-secured computers can be hacked in just 15 minutes or less after being put onto the Internet.] Depending on your environment, it may be acceptable to put your computer on the Internet after installing a firewall and antivirus software with the latest updates.

2. Seriously consider enabling or installing firewall software and/or firewall hardware. There are a number of free firewalls available, including the ICF feature that comes with Windows XP [unless XP is joined to a Windows domain], and/or other third-party firewalls available on the Internet.

For more information on how and where to locate free and not-free firewall software and hardware, see the section in this FAQ entitled "Which firewall should I choose? Which firewall is the best?"

3. Seriously consider installing an antivirus program and configure it to automatically download updates daily.

For more information on where and how to locate and use free and not-free antivirus software, see the section in this FAQ entitled "Which antivirus should I choose? Which antivirus is the best?"

4. Follow the instructions for hardening Windows 2000 and also IIS [if IIS is installed] at [www.microsoft.com/technet/security](http://www.microsoft.com/technet/security) [For Windows 2000 / NT, hardening IIS usually includes installing IISlockdown including URLScan. For computers with FTP service installed, it usually includes removing the Posix subsystem and removing write permission from the anonymous user account, among other things.]

5. Download and install all the service packs and security patches from [www.microsoft.com/technet/security](http://www.microsoft.com/technet/security) for all the Microsoft and non-Microsoft software installed on your computer, especially Microsoft Windows, Office, Internet Explorer, Outlook Express, Windows Media Player and IIS [if IIS is installed].

Note that Windows 2000, XP, .NET and NT users should also download patches for Indexing Services a.k.a. Index Server. Do not assume that Index Server patches are included with any IIS comprehensive service pack rollup you may already have installed, because they are not.

[If you want a shortcut to do this faster, you could try this:

- \* Download and install the latest Windows service pack from [www.microsoft.com/technet/security](http://www.microsoft.com/technet/security);
- \* Reboot and visit <http://windowsupdate.microsoft.com> to receive additional patches;
- \* Reboot, download and run MBSA [Microsoft Baseline Security Analyzer] or HFNETCHK from [www.microsoft.com/download](http://www.microsoft.com/download) to discover other missing patches;
- \* Manually download from [www.microsoft.com/technet/security](http://www.microsoft.com/technet/security) and install any patches that were found to be missing, as well as patches for any server

products that may not be included in Windows Update and MBSA/HFNETCHK, such as possibly SQL Server, ISA Server, etc.

\* NOTE however that Windows Update, MBSA and HFNETCHK do NOT necessarily list all Microsoft patches or search all Microsoft products, so you could be missing some patches if you rely just on these tools.]

6. [ONGOING] Re-run the MBSA tool from [www.microsoft.com/download](http://www.microsoft.com/download) every 60 days or sooner to look for missing patches, and confirm that your antivirus program received an update in the past 10 days or less.

If you want or need even more security [or are particularly paranoid or at risk], you can consider some of the additional steps below. Some of the tools below may be more security than you need, unless you are running a server such as IIS web or FTP services.

\* Download and install MyNetWatchman or Dshield. These are free programs that work with your firewall software or hardware to automatically report hacking attempts to the hacker's ISP. You get to see information about whether that IP address has been used to scan or hack other computers, or whether it might be targeting just your computer. You also get to see whether the ISP has responded or taken action against the offending user. This is highly recommended. You can get this software at one of the links below:

[www.mynetwatchman.com](http://www.mynetwatchman.com)

[www.dshield.org](http://www.dshield.org)

\* Sign up for the Microsoft security mailing list at [www.microsoft.com/technet/security](http://www.microsoft.com/technet/security) to receive emails with a link to new critical security patches as they are released, and install them ASAP.

\* Use Fport or Vision from [www.foundstone.com/knowledge](http://www.foundstone.com/knowledge) or pslist / pstools from [www.sysinternals.com](http://www.sysinternals.com) to look at the open ports on your computer and the program or executable using that port. Some firewall software such as [www.sygate.com](http://www.sygate.com) will also tell you this information.

You can also use the NETSTAT -A command that comes with Windows to look at open ports; however, this will not identify which program is using the port.

[You may want to run a command such as FPORT >> C:\OPENPORTS.TXT or PSLIST >> C:\OPENPORTS.TXT or NETSTAT -A >> C:\OPENPORTS.TXT This command will create a "baseline" text file named c:\openports.txt that can be compared later with the results of the command to tell you whether additional ports are now open, a possible sign of intrusion.]

\* Consider running one or more vulnerability scanners to look for security flaws and configuration errors on your computers. Vulnerability scanners should be run after you have installed and hardened a new computer or server, and also run at regular intervals to confirm that your computers are still secure. You might also run a port scanner against your computers as well to look for open ports.

See the section in this FAQ entitled "How can I scan my computer or firewall to look for open ports or confirm that my machine is secure?" for more information.

\* Consider searching for and following additional checklists for hardening Windows 2000 by searching an Internet search engine such as [www.google.com](http://www.google.com) for words such as "harden OR hardening windows-2000" [e.g. [www.google.com/search?q=harden+OR+hardening+windows-2000](http://www.google.com/search?q=harden+OR+hardening+windows-2000) ]. Several such checklists are available at <http://nsa1.www.conxion.com/win2k/download.htm> a.k.a. <http://www.nsa.gov>, as well as [www.labmice.net/security](http://www.labmice.net/security), <http://rr.sans.org>, etc.

\* Uninstall any unnecessary Windows components [e.g. click on Start, Settings, Control Panel, Add/Remove Programs, Add/Remove Windows Components]. Pay particular attention to Indexing Service, Internet Information Services (IIS), Management and Monitoring Tools, Message Queuing Services, Networking Services, Other Networking File and Print Services, Outlook Express, and Windows Media Player. If you are not sure whether something is unnecessary, try searching [www.google.com](http://www.google.com) or posting a question to the appropriate Microsoft security newsgroup.

\* Disable any unnecessary Windows services [e.g. click on Start, Settings, Control Panel, Administrative Tools, Services]. If you are not sure whether something is unnecessary, try searching [www.google.com](http://www.google.com) or posting a question to the appropriate Microsoft security newsgroup.

\* Consider using a Trojan scanner. Antivirus programs generally detect some but not all of the most common Trojans and hacker tools. Some people choose to use a Trojan scanner in addition to antivirus.

For more information on where and how to locate and use free and not-free Trojan scanner software, see the section in this FAQ entitled "Which antivirus should I choose? Which antivirus is the best?"

\* Enable logging. Most logging is disabled by default, and usually this is not discovered until after an intrusion, when the logs are needed.

Enable logging of your IIS web server, FTP server, etc. For sites with a small number of hits, consider changing logs to rotate monthly instead of daily to allow easier searching of logs.

Enable logging on your Internet router, switch or firewall. [Because these devices usually do not have much storage space for saving logs, doing this may involve installing free syslog software onto your computer to be able to capture the logs.]

Enable auditing of security events on your Windows system, including logon successes and/or failures and NTFS auditing of files and registry keys. For more information, see the section in this FAQ entitled "How can I enable auditing / logging on my computer / server?"

Change the Windows event log settings to be appropriate for your environment. Consider increasing the maximum log size to retain more information. Be careful not to log too much, or you might find that your logs contain only a few minutes or hours worth of data.

Check the logs to be sure logs are really being captured.

\* Consider using a file change checker, such as the unsupported free tool Languard File Integrity Checker at [www.gfi.com/languard/lantools-fic.htm](http://www.gfi.com/languard/lantools-fic.htm). Files changing on your system can sometimes indicate a hacker intrusion.

\* Consider using a Windows event log monitor. Some types of intrusions leave entries in one of the logs on your computer. [On an especially vulnerable or secure system, you should be sure that you've configured logging to detect events such as intrusions.] Some network monitors such as [www.ipsentry.com](http://www.ipsentry.com) can send a message to your email/screen/pager if a server or service stops responding, an event or error appears in a Windows log, etc. Windows log monitors can be found by searching an Internet search engine or your favorite software web site, or by using the links below:

[www.ipsentry.com](http://www.ipsentry.com) [around \$100 US]  
[www.sunbelt-software.com](http://www.sunbelt-software.com)  
[www.webattack.com](http://www.webattack.com)  
[www.wilders.org](http://www.wilders.org)  
[www.download.com](http://www.download.com)  
[www.tucows.com](http://www.tucows.com)  
[www.google.com/search?q=windows+event+log-monitor](http://www.google.com/search?q=windows+event+log-monitor)

\* Consider using EFS file encryption [under Windows 2000 / XP / .NET] or third-party utilities to encrypt the files on your computer may be something to consider. Some of these utilities can encrypt your entire hard drive including Windows, whereas other tools just encrypt some of your data files and are not suitable for encrypting or preventing access to Windows.

Note that using any form of encryption can slow down your computer's performance. Also, you must be extremely careful to back up and protect your encryption key and any passwords. If the encryption keys are not backed up, users can lose their encrypted files forever when Windows is reinstalled, Windows encounters a problem so that Windows no longer starts up, etc.

For more information on EFS file encryption on Windows 2000 / XP / .NET, see the section in this FAQ entitled "I used Windows 2000 / XP EFS file encryption to encrypt some files. Now, I can't read the files. How can I unencrypt them or recover the key?"

Third party encryption software can be found at the following locations:

[www.pgp.com](http://www.pgp.com)  
[www.scramdisk.clara.net](http://www.scramdisk.clara.net)  
[www.e4m.net](http://www.e4m.net)

www.jetico.com ["BestCrypt"]  
www.download.com  
www.tucows.com  
www.google.com

=====

Which antivirus should I choose? Which antivirus is the best?

A: Here is the short answer: be sure you are using an antivirus program with the latest updates for the week. If you are and the virus was not removed, you should search for removal information and/or a removal tool and/or a support group at one or more of the following web sites:

- \* The web page of your antivirus vendor
- \* [www.sarc.com](http://www.sarc.com)
- \* [www.google.com](http://www.google.com)

However, there are additional issues you should be aware of. Keep reading below for more information:

The best way to deal with any virus on any computer or server is ALWAYS to install and use an antivirus program that is updated with the latest updates for that week [or day].

Some antivirus manufacturers may release mini-tools that will remove a particular virus or worm, such as a Nimda virus removal tool. However, these single-virus removal tools generally do nothing to protect you from becoming re-infected when you receive another infected email or file five minutes after you ran the tool. Antivirus software is necessary to prevent against re-infection and damage to your computer files.

Just running an antivirus program is not enough. You should make sure that your antivirus program can be configured to download updates every day [or every week] automatically via the Internet, and open the program from time to time to ensure that it is still receiving updates.

NOTE however that if an antivirus scanner or Trojan scanner finds a Trojan installed and running on your computer, it could be a sign of a hacker intrusion, in which case you will want to consider taking additional steps before removing the Trojan. For more information, see the section in this FAQ entitled "How can I tell if I've been hacked?"

If you have a particular file name and wish to find out whether or not it is a virus [or a worm, a Trojan, a hoax, etc.], you can try searching an Internet search engine such as [www.google.com](http://www.google.com) for that file name. However, it is still best to install and use an antivirus scanner. Looking up a particular file name is NOT a reliable way to determine whether or not the file is a virus.

Deleting a file from your system is never the first way or the best way to try to remove a virus from your computer.

Which antivirus software is best for you will vary depending on your computer systems, your security requirements and your personal preferences.

Antivirus programs may be purchased from Internet web sites, from your local computer store, and even from stores like Target and Wal-Mart. Antivirus software can be found using the links below:

[www.symantec.com](http://www.symantec.com) [Norton Antivirus]  
[www.grisoft.com](http://www.grisoft.com) [AVG Antivirus [including a free version]]  
[www.f-prot.com/products](http://www.f-prot.com/products) [free DOS version]  
[www.f-secure.com](http://www.f-secure.com) [F-Secure]  
[www.trendmicro.com](http://www.trendmicro.com) [Trend Micro]  
[www.wilders.org](http://www.wilders.org)  
[www.download.com](http://www.download.com)  
[www.tucows.com](http://www.tucows.com)

[Most of the antivirus products will also work on Windows Server products or have a version for Windows Server.]

There are also a number of web sites that will scan your computer for viruses for free. However, using these web sites will do nothing to protect you against future re-infection and damage to your computer files. Some of these web sites include:

<http://security2.norton.com> [Norton free one-time web-based scanner]  
<http://housecall.antivirus.com> [Trend Micro free one-time web-based scanner]

Just running an antivirus program is not enough. You should make sure that your antivirus program can be configured to download updates every day [or every week] automatically via the Internet, and open the program from time to time to ensure that it is still receiving updates.

Antivirus software is like prescription drugs or psychologists; the first one you get might not work right for you. If one antivirus program fails to install or causes your computer to perform slowly, you could contact the manufacturer, or you could uninstall it and try another antivirus program.

Note that you may need to set your antivirus program to ignore certain folders, such as the folder containing your firewall software. Failing to do so can cause speed problems or false alarms on your computer.

You generally only want to install and run no more than one antivirus program on your computer at a time. Running two memory-resident, on-access antivirus programs simultaneously can cause false alarms or cause other problems.

If you are running antivirus with the latest updates and are STILL having problems removing the virus, you should:

- \* Note the name of the virus being reported by your antivirus program;
- \* Visit the web site for your antivirus manufacturer and click on "Support," so that you can:
  - + Look up the virus name in the virus information database for info and follow any instructions found there;
  - + Search the support web page for your antivirus; and/or
  - + Post a question in the support group for your antivirus.

For example, if you are using Norton Antivirus, you should visit the following web sites:

[www.sarc.com](http://www.sarc.com) – NAV virus database  
[www.sarc.com/techsupp](http://www.sarc.com/techsupp) – free NAV support discussion groups

Be wary of any email ever that:

- \* Tells you to delete a file from your computer as the first or only way to remove a particular virus;
- \* Tells you to forward the email to everyone you know;
- \* Tells you that a particular virus cannot be stopped by antivirus.
- \* Tells you that a particular virus has been confirmed by a large company or government entity, such as Microsoft, IBM, the Department of Defense, etc.

Emails such as the ones described above are usually hoaxes [even if the warning email is from a friend that you trust]. Stop and confirm or have someone confirm the authenticity of any warning email before forwarding it to anyone. You can often confirm or deny the existence of a particular virus by searching for the virus name at an Internet search engine or virus manufacturer's web page, such as:

[www.google.com](http://www.google.com)  
[www.sarc.com](http://www.sarc.com) – Norton Antivirus  
[www.f-secure.com/virus-info](http://www.f-secure.com/virus-info) – F-Secure

#### TROJAN SCANNERS:

It is also a good idea to consider using a Trojan scanner \*in addition to\* antivirus software. Trojans and hacker tools can cause many of the same symptoms that viruses and worms do, but antivirus programs generally do not detect all of the most common Trojans and hacker tools. Some Trojan scanners can be found by searching an Internet search engine or your favorite software web site, or by using the links below:

[www.pestpatrol.com](http://www.pestpatrol.com) [includes a free mini-scanner]  
[www.lockdowncorp.com](http://www.lockdowncorp.com)  
[www.wilders.org](http://www.wilders.org)  
[www.download.com](http://www.download.com)  
[www.tucows.com](http://www.tucows.com)  
[www.sunbelt-software.com](http://www.sunbelt-software.com)  
[www.google.com/search?q=trojan-scanner](http://www.google.com/search?q=trojan-scanner)

When looking for Trojans, you should also consider using a tool to look for open ports, such as Vision or Fport from [www.foundstone.com/knowledge](http://www.foundstone.com/knowledge) or Pstools / Pslist from [www.sysinternals.com](http://www.sysinternals.com)

=====

Which firewall should I choose? Which firewall is the best?

A: The answer to this question varies depending on your computer systems, your security requirements and your personal preferences. Below are some firewalls and other forms of firewall-like packet filtering:

#### NO MATTER WHICH FIREWALL YOU CHOOSE...

No matter which firewall you choose, you should seriously consider downloading and installing MyNetWatchman or Dshield. These are free programs that work with your firewall software or hardware to automatically report hacking attempts to the hacker's ISP. You get to see information about whether that IP address has been used to scan or hack other computers, or whether it might be targeting just your computer. You also get to see whether the ISP has responded or taken action against the offending user. You can get this software at one of the links below:

[www.mynetwatchman.com](http://www.mynetwatchman.com)  
[www.dshield.org](http://www.dshield.org)

Also, no matter which firewall you choose, the lists below of port numbers for common software services may be helpful when configuring your firewall or when trying to monitor the firewall logs for signs of intrusion:

[www.iana.org/assignments/port-numbers](http://www.iana.org/assignments/port-numbers)  
[www.iisfaq.com/default.asp?View=P106](http://www.iisfaq.com/default.asp?View=P106)

#### FIREWALL SOFTWARE:

[www.sygate.com](http://www.sygate.com) [free for non-commercial use, also works like a sniffer]  
[www.kerio.com](http://www.kerio.com) [free for non-commercial use]  
[www.agnitum.com](http://www.agnitum.com) [free for non-commercial use]  
[www.zonealarm.com](http://www.zonealarm.com) [free for non-commercial use, also blocks pop-ups]  
[www.iss.net](http://www.iss.net) [Black Ice]  
[www.symantec.com](http://www.symantec.com) [Norton]  
[www.webattack.com](http://www.webattack.com)  
[www.download.com](http://www.download.com)  
[www.tucows.com](http://www.tucows.com)  
[Windows XP users can also consider using the ICF firewall that comes with XP, more info below]

#### FIREWALL DEVICES [HOME / SOHO]:

[www.linksys.com](http://www.linksys.com) [starts around \$70 US]  
[www.netgear.com](http://www.netgear.com) [starts around \$70 US]  
<http://search.ebay.com/search/search.dll?query=firewall> [prices on new and used firewalls]

FIREWALL DEVICES [PROFESSIONAL / ENTERPRISE]:

[www.netscreen.com](http://www.netscreen.com)

[www.netgear.com](http://www.netgear.com)

[www.intrusion.com](http://www.intrusion.com)

[www.cisco.com](http://www.cisco.com)

[www.nortelnetworks.com/products/family/contivity.html](http://www.nortelnetworks.com/products/family/contivity.html)

[www.nokia.com/securitysolutions](http://www.nokia.com/securitysolutions)

[www.microsoft.com/isa](http://www.microsoft.com/isa)

<http://search.ebay.com/search/search.dll?query=firewall> [prices on new and used firewalls]

LINUX / BSD FIREWALLS:

<http://www.ipcop.org> [install to hard drive, friendly GUI]

<http://www.smoothwall.org> [install to hard drive, friendly GUI]

<http://www.devil-linux.org> [boot CD firewall]

<http://gibraltar.at> [boot CD firewall]

<http://www.sentryfirewall.com> [boot CD firewall]

<http://www.thinman.com/eLSD> [boot CD firewall]

<http://www.closedbsd.org> [boot floppy firewall]

<http://thewall.sf.net> [boot floppy firewall]

INTRUSION DETECTION:

<http://www.snort.org> [free, has a version for Windows]

<http://www.trinux.org> [free, runs from a boot floppy disk or CD]

<http://www.iss.net>

Linux / BSD firewalls can be run on an old spare 486 PC to protect your network, and the software is often free of charge. Some of the firewalls above are supposedly intended to be easy enough for small offices and home users with no previous Linux experience to use. Linux firewalls are one inexpensive way to be able to add advanced firewall features that may be very expensive to add to commercial firewalls. [Features such as bandwidth usage reporting, QoS bandwidth limiting, intrusion detection, alerts in real-time to your email or pager, a third network interface to create a DMZ, identical spare backup firewalls for fault tolerance and scalability, etc. are generally free.] Unlike some commercial firewalls, 24x7 on-site technical support for Linux / BSD firewalls can be purchased from a number of companies in most cities.

Intrusion detection is software or hardware that generally monitors the data transmissions on your network in order to add better alerting, analysis and detection of intrusions [without necessarily blocking those intrusions]. Note that with most IDS systems, you must tune the default rules and settings, or else you will receive too many false alarms.

Linux firewalls and intrusion detection are not likely to be the best way to protect just one home computer or laptop [unless you are an expert computer user or computer hobbyist]. These tools are probably more useful to network administrators.

ICF – WINDOWS XP INTERNET CONNECTION FIREWALL –

If you are using a Windows XP computer at home and do not log into a Windows domain, you can enable the free ICF – Internet Connection Firewall – that comes with Windows XP. The ICF firewall is generally well respected and secure for home users.

You can enable or configure ICF either by clicking on Start, Settings, Control Panel, double-click Networking and Internet Connections, click Network Connections, right-click the connection on which you would like to enable ICF, and then click Properties, Advanced and select "Protect my computer or network."

See the articles below for more information:

How to enable or disable ICF –

<http://support.microsoft.com/default.aspx?scid=kb:en-us:Q283673>

More information on ICF and how to configure ICF –

<http://support.microsoft.com/default.aspx?scid=kb:en-us:Q320855>

<http://support.microsoft.com/default.aspx?scid=kb:en-us:Q298804>

<http://support.microsoft.com/default.aspx?scid=kb:en-us:Q308127>