



Virus Program

What's a Virus?

A virus is a program or piece of code that causes an unexpected, usually negative, event. Viruses are often disguised as games or images with clever marketing titles such as "Me, nude".

A virus must meet two criteria:

- It must execute itself. It will often place its own code in the path of execution of another program.
 - It must replicate itself. For example, it may replace other executable files with a copy of the virus infected file. Viruses can infect desktop computers and network servers alike.
-

What's a Worm?

Computer Worms are viruses that reside in the active memory of a computer and duplicate themselves. They may send copies of themselves to other computers, such as through email or Internet Relay Chat (IRC).

What's a Trojan?

A Trojan horse program is a malicious program that pretends to be a benign application; a Trojan horse program purposefully does something the user does not expect. Trojans are not viruses since they do not replicate, but Trojan horse programs can be just as destructive.

Many people use the term to refer only to non-replicating malicious programs, thus making a distinction between Trojans and viruses.

What's a Virus Hoax?

There are a lot of viruses out there. But some aren't really out there at all. Virus hoaxes are more than mere annoyances. They may lead some users to routinely ignore all virus warning messages, leaving them vulnerable to a genuine, destructive virus.

Next time you receive an urgent virus warning message, be sure to check the list of known virus hoaxes. (we will get to it below)

Remember to never open an email attachment unless you know what it is-even if it's from someone you know and trust.

Some of the common phrases used in these hoaxes are:

- If you receive an email titled [email virus hoax name here], do not open it!
- Delete it immediately!
- It contains the [hoax name] virus.
- It will delete everything on your hard drive and [extreme and improbable danger specified here].
- This virus was announced today by [reputable organization name here].
- Forward this warning to everyone you know!

Remember that virus writers can use known hoaxes to their advantage. For example, AOL4FREE began as a hoax virus warning. Then somebody distributed a destructive trojan attached to the original hoax virus warning! The lessons are clear:

- Always remain vigilant
 - Never open a suspicious attachment
-

What is the Back Door?

This is a program that sends information back to its creator about the infected system, making it easy for that person to hack into the infected system and take control of it or read sensitive data.

What is the Blended Threat?

This is a combination of infection types in a single item. For example, a worm that infects a boot sector, deletes important files and/or opens a security back door would be a blended threat.

What is Not a Virus?

Because of the publicity viruses have received, it is easy to blame any computer problem on a virus. The following are not likely to be caused by a virus or other malicious code:

- Hardware problems. There are no viruses that can physically damage computer hardware, such as chips, boards, and monitors.
- The computer beeps at startup with no screen display. This is usually caused by a hardware problem during the boot process. Consult your computer documentation for the meaning of the beep codes.
- The computer does not register 640 K of conventional memory. This can be a sign of a virus, but it is not conclusive. Some hardware drivers such as those for the monitor or SCSI card can use some of this memory. Consult with your computer manufacturer or hardware vendor to determine if this is the case.
- You have two antivirus programs installed and one of them reports a virus. While this could be a virus, it can also be caused by one antivirus program detect the other program's signatures in memory.
- You are using Microsoft Word and Word warns you that a document contains a macro. This does not mean that the macro is a virus.
- You are not able to open a particular document. This is not necessarily an indication of a virus. Try opening another document or a backup of the document in question. If other documents open correctly, the document may be damaged.
- The label on a hard drive has changed. Every disk is allowed to have a label. You can assign a label to a disk by using the DOS Label command of from within Windows.

Finding Information on a Virus

1. Go to the McAfee homepage.
<http://us.mcafee.com/virusInfo/default.asp>
2. Click **Virus Information**.
3. At the right, under Virus Search, enter the name of the virus.
4. Click **Search**.
5. Search results appear. Click on the name of the virus to view its profile information.

Finding Information on a Hoax

1. Go to the McAfee homepage.
<http://us.mcafee.com/virusInfo/default.asp>
2. Click **Virus Information**.
3. At the left, click **Virus Hoaxes**.
4. A list of hoaxes appear. Click on the name of the hoax to view its profile information.

<http://oroville-city.com/connectors>

Uninstalling Existing Antivirus Software

1. From the taskbar, click **Start**.
 2. Click **Settings** (skip this if using Windows XP).
 3. Click **Control Panel**.
 4. Double-click **Add/Remove Programs**.
 5. Click to highlight the existing antivirus program in the list of software.
 6. Click **Add/Remove**.
 7. Follow the prompts to remove the antivirus program.
Note: If you're prompted to remove shared files, click **Yes to all**.
 8. Restart your computer.
-

Virus Hoaxes

Virus hoaxes are not viruses. They are false email warnings about viruses or other malicious software. Some hoaxes cause as much trouble as viruses by resulting in massive amounts of unnecessary email.

Most hoaxes contain one or more of the following characteristics:

- Warnings about alleged new viruses and its damaging consequences
- Demands the reader forward the warning to as many people as possible
- Pseudo-technical 'information' describing the virus
- Bogus comments from officials: FBI, software companies, and news agencies.

If you receive an e-mail message about a virus, check with a reputable source to ensure the warning is real. Visit McAfee's Virus Hoax page to learn about hoaxes and the damage they cause.

Virus Information Websites

<http://us.mcafee.com/virusInfo/default.asp?affid=101&langid=1>

Many of the viruses will have a removal tool listed with their information; the tool is called STINGER on the McAfee site.

Virus Removal Tools

<http://us.mcafee.com/virusInfo/default.asp?id=VRT>

McAfee Security provides you with a powerful set of virus removal tools, designed to automatically detect and remove viruses that infected your system. These applications are also valuable because of their size, making them easily downloadable even with a slow Internet connection. If you suspect your system to be infected with one of the following viruses, these invaluable FREE tools will allow you to repair any damages to your computer.

<http://oroville-city.com/connectors>

Additional Virus Information

Norton Anti Virus and Product Information

<http://www.symantec.com/product/>

Norton Anti Virus Downloads and Information

<http://www.symantec.com/downloads/>

Norton Anti Virus Removal Tools

<http://securityresponse.symantec.com/avcenter/tools.list.html>

Computer Associates (CA.com) virus information – **include a great free scanner.**

This site stays up to date and has a lot of information

Also there are some stand a lone cleaning tools provided.

<http://www3.ca.com/virusinfo/>

AVG Anti Virus – includes a free version (by Grisoft)

http://www.grisoft.cz/us/us_index.php

http://www.grisoft.cz/us/us_dwnl_free.php **the link to free download**

TrendMicro – offers an online free scan

<http://www.trendmicro.com/en/home/us/personal.htm>

F-Secure Security – great site for virus & wireless devices issues.

This site has a lot of up to date virus information. (non US company)

<http://www.f-secure.com/virus-info/>

Microsoft Basic Virus Information and Links

<http://support.microsoft.com/default.aspx?scid=kb;en-us;129972>

<http://www.microsoft.com/security/protect/default.asp> - protecting your OS.

For free virus-related support from Microsoft in the U.S. or Canada,
call (866) PC-SAFETY (727-2338).

How to Disable Active Scripting in Outlook Express – helps reduce virus

<http://support.microsoft.com/default.aspx?kbid=192846>

Virus Protection Features in Outlook Express 6

<http://support.microsoft.com/default.aspx?kbid=291387>

List of Major Anti Virus Vendor's Websites

Some of these sites are not designed for the home user.

<http://www.ealaddin.com>
<http://www.quickheal.com/default.htm>
<http://www.f-prot.com/products>
<http://www.f-secure.com/products>
<http://www.gfi.com>
<http://www.pandasoftware.com>
<http://symantec.com>
<http://www.trendmicro.com/en/home/us/personal.htm>
http://info.ahnlab.com/english/product/01_1.html
<http://www.avast.com/>
<http://www.authentium.com/solutions/products/commandantivirus.cfm>
<http://www3.ca.com/Solutions/Product.asp?ID=156>
http://www.dials.ru/english/dsav_toolkit/drweb32.htm
<http://www.nod32.com/home/home.htm>
http://www.grisoft.com/us/us_avg_index.php/
<http://www.globalhauri.com/html/products/products.html>
<http://www.kaspersky.com/>
<http://www.networkassociates.com/us/products/home.htm>
http://www.norman.com/products_nvc.shtml
<http://www.protectorplus.com/>
<http://www.sophos.com/products/sav/>
<http://www.sybari.com/products/>
<http://www.zeroknowledge.com/>

Mac Sites

<http://www.hyperactivesw.com/Virus2.html>
<http://www.intego.com/virusbarrier/>
<http://us.mcafee.com/root/package.asp?pkgid=100>
<http://www.nai.com/us/index.asp>
<http://www.slipstick.com/outlook/antivirus.htm>

Got Information - Know Someone Starting Virus?

Individuals with information about the MSBlast.A worm, the Sobig worm—or any other worms or viruses—should contact the FBI or the Secret Service through the online Internet Fraud Complaint Center or by calling their local FBI field office or the Interpol National Central Bureau in any of Interpol's 181 member countries.

[Internet Fraud Complaint Center \(ifccfbi.gov\)](http://ifccfbi.gov)
[FBI Field Office contact information \(fbi.gov\)](http://fbi.gov)
[U.S. National Central Bureau of Interpol \(usdoj.gov\)](http://usdoj.gov)