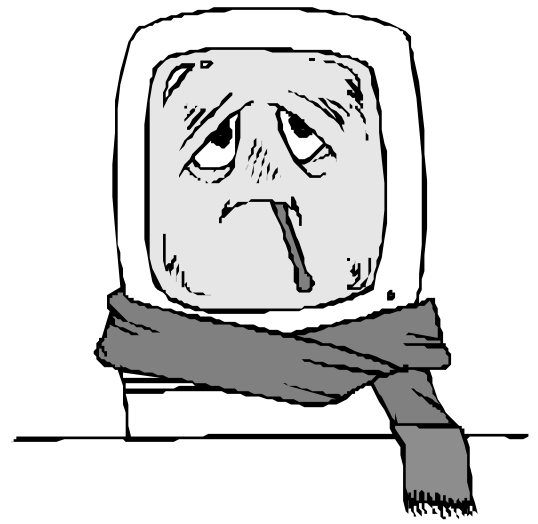


# Protecting Your Computer from Viruses



## WHAT IS A VIRUS?

A virus is simply a computer program that replicates itself. A virus does not necessarily have to be malicious. In fact, most viruses are not written to be destructive. The ability to make copies of itself and spread is the only real criterion for a virus. Viruses attach themselves to programs or files and spread through the sharing of infected software or disks.

Unfortunately, even so-called benign viruses can cause problems for users. Benign viruses (for example, viruses that cause your computer to beep or that display messages on the screen) can slow the performance of your machine as well as just be very annoying. Benign viruses can also have bugs in them making them incompatible with your system and causing crashes and freezes. Destructive viruses can cause a lot more damage, including overwriting or destroying files, reformatting the hard drive, and crashing your system.

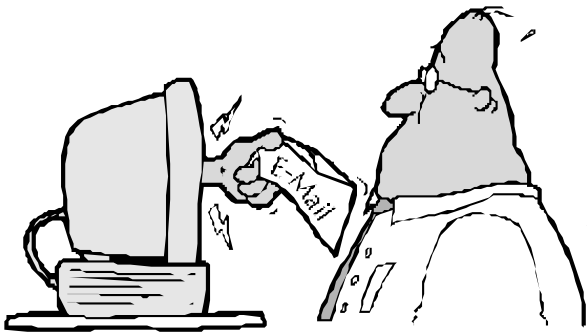
## HOW DO VIRUSES WORK?

In general, viruses are platform-specific. Macintosh viruses cannot infect PC's and vice-versa. For whatever reason, there are many more PC viruses than Macintosh viruses. Most Macintosh viruses are also not malicious. Macintosh viruses do exist, however, and as we mentioned before even benign viruses can cause problems and should be removed from your system as soon as you discover them.

The most common type of virus on the PC are so-called *boot sector viruses*. Boot sector viruses infect the boot sectors of floppy disks and the partition sector or DOS boot sector of hard drives. The virus infects the hard drive when you boot the computer from an infected floppy. The virus then becomes resident in memory and infects every disk you put in drive A. Stoned, Monkey, and Michelangelo are well-known examples of boot sector viruses.

Another type of virus is the file virus. File viruses attach themselves to files, usually executable files. When the infected file is run the virus is transferred to memory and then begins to infect other programs as they are run. Die Hard is an example of a PC file virus. A multi-partite virus is particularly nasty in that it combines the features of both boot sector and file viruses. It can infect both files and boot sectors/partition tables and spreads using both methods. Tequila and Junkie are examples of PC multi-partite viruses.

Macintosh viruses do not fall into such easily-defined categories, but most operate by infecting particular resources in the system file. One of the common Macintosh viruses is the MBDF virus, which is named after the type of resource that it uses to infect files. There are several other Macintosh viruses that use system resources to infect files, including the WDEF virus, the MDEF virus, and the CDEF virus. *(continued on page 4)*

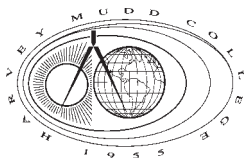


# Mailing Lists and E-Mail Aliases at HMC

## IN THIS ISSUE

Protecting Your Computer from Viruses -----	cover
Mailing Lists and E-mail Aliases -----	2
Editor's Notes -----	3
Tricks & Tips -----	7
Q&A -----	8

*Occasional Downtime* is composed on a Power Computing PowerBase™ 180 using Aldus PageMaker 6.0. The primary typefaces used are Times and Optima. We wish to thank Sally Rich Arroyo of the HMC Office of College Relations for all her help.



Recently a professor asked us to create a mailing list for him for his group of advisees. After some discussion we determined that it probably made more sense for him to create his own personal e-mail alias instead. Based on this experience we thought it would be useful to write an article about mailing lists and e-mail aliases, how they differ, and what each is especially good for.

## MAILING LISTS

Mailing lists are widely used at HMC. Every year Academic Computing creates a large number of mailing lists for use by faculty, staff and students. There are mailing lists for all of the courses taught at HMC, department majors, dorm residents, clinic groups, and department faculty, as well as for many of the committees and organizations on campus. In addition to these and other official mailing lists, there are also many "fun" lists for various clubs, hobbies, games, and sports.

HMC mailing lists are managed by an automated software package called Listkeeper. When you send a message to a mailing list Listkeeper takes care of resending your message to all of the people subscribed to the list. Listkeeper can also do a lot of other things for you. By sending e-mail directly to [listkeeper@hmc.edu](mailto:listkeeper@hmc.edu) you can find out all the lists at HMC, which lists you are subscribed to, or who is on a particular list. You also subscribe to and unsubscribe from a particular list by sending e-mail to Listkeeper.

Each list has an owner who manages the list. Most of the time the owner doesn't have to

do much; Listkeeper takes care of just about everything. In the case of a closed list, however, the owner has to approve subscriptions to the list. Lists can also be moderated. In that case, a moderator has to approve each message mailed to the list. The student mailing list, [students-1@hmc.edu](mailto:students-1@hmc.edu), is an example of a moderated list.

Mailing lists are most useful when you have a large group of people who may want to send e-mail to each other, especially when the group may change over time and you want people to be able to subscribe and unsubscribe themselves. The downside is that every mailing list created adds some burden to the listserver, even when the list is not actively used.

If you have a new mailing list you'd like to create you can send e-mail to [listmaster@hmc.edu](mailto:listmaster@hmc.edu). For more information about Listkeeper look at our documentation on the Web at <http://www.hmc.edu/comp/doc/listkeeper/>.

## E-MAIL ALIASES

System e-mail aliases are another tool we have at HMC. A system e-mail alias is an e-mail address which expands to one or more actual e-mail addresses. For example, the addresses [av-request@hmc.edu](mailto:av-request@hmc.edu) and [help-desk@hmc.edu](mailto:help-desk@hmc.edu) are system e-mail aliases.

System e-mail aliases are most useful when you want to create an easy to remember address that people can send e-mail to. It's also sometimes useful to hide the actual recipient of the e-mail, especially if that person might change later on. You can't subscribe to an e-mail alias;


adding or subtracting the people on an alias requires the manual intervention of a system administrator. To request a new e-mail alias you need to send e-mail to [postmaster@hmc.edu](mailto:postmaster@hmc.edu).

#### PERSONAL E-MAIL ALIASES

To create a new mailing list or system e-mail alias you need the intervention of a system administrator. There's another e-mail tool, however, that you have personal control over. In most e-mail programs it is possible to create personal e-mail aliases and distribution lists.

Depending on the program you use they are variously called Nicknames (Eudora), addresses and address lists (Pine), and aliases and distribution lists (PMDf Mail).

Personal e-mail aliases can be very useful and can save you a great deal of time. You can create aliases for people that you e-mail often so that you don't have to type out their entire e-mail address every time you send e-mail to them. You can also create an alias for a group of people that you send e-mail to often. Eudora and Pine don't really distinguish between creating aliases to single e-mail addresses and creating aliases to a list of addresses. You use the same method for creating both. Keep in mind that the aliases you create can only be used by you. Other people on campus or off-campus can't send mail to one of your aliases. So personal e-mail aliases are most useful when you're the only person who needs to send e-mail to all of the people in the alias. If the people on your alias need to send mail to each other then a mailing list is probably more appropriate. In the case of the professor who wanted a list for his advisees, since only he needed to send e-mail to the group we suggested that he use a personal e-mail alias. This reduced the burden on the listserver, as well as on AC staff.

Details on creating your own e-mail aliases and distribution lists can be found on our Web site at <http://www.hmc.edu/comp/doc/email/>. 

## Editor's Notes

This month's issue of *Occasional Downtime* focuses on two main topics: computer viruses and mailing lists and e-mail aliases at HMC. The article on viruses was prompted by an outbreak of the Good Times Virus hoax on campus early in the semester. It has turned out to be especially timely as one of the departments at HMC had an outbreak of the Microsoft Word Concept macro virus while I was writing the article. This gave me the opportunity for hands-on experience in removing the Concept virus for the article. All joking aside, computer viruses are a significant problem, especially in the PC world. So understanding how viruses spread, how to remove them, and how to protect yourself from them is an important part of working with computers.

Using e-mail effectively is also an important skill for all of our computer users. Mailing lists and e-mail aliases can make your work both more productive and easier. Understanding how Listkeeper works is particularly important. To that end, I've included the most frequently asked questions about mailings lists and Listkeeper in our Questions & Answers section this month.

—Elizabeth Hodas

---

*Occasional Downtime* is published bimonthly by the Academic Computing Department at Harvey Mudd College. It is also available in a variety of formats on the HMC Web Server. Comments and questions can be directed to [downtime@hmc.edu](mailto:downtime@hmc.edu).

Another common Macintosh virus is the Scores virus. You can read more about individual Macintosh viruses in the Disinfectant manual.

#### **MACRO VIRUSES**

A new type of virus, the macro virus, has become more prevalent recently and is developing into a serious problem for both Macintosh and PC users. Macro viruses are unusual in that they infect data files rather than executables. They are also not platform specific, meaning that the same virus can infect both Macintoshes and PCs. Macro viruses typically infect Microsoft Word and Excel documents, although they also can infect AmiPro documents. Macro viruses use the macro programming language of an application to infect documents and spread.

The Word Concept virus was the first macro virus and is still the most common. Opening a Microsoft Word document infected with the Concept virus installs the virus macros which then spread to other Word documents when they are opened. The virus does not cause any loss of data or damage, but it makes Word only let you save documents as templates, which is pretty annoying. (For more on the Concept virus, including detecting it and removing it, see this month's Tricks&Tips.) There are now many new macro viruses. Most are merely annoying, but destructive macro viruses are also starting to appear.

#### **WORMS, TROJAN HORSES, AND OTHER PROBLEMS**

Viruses are, of course, not the only destructive or annoying problem in the computer world. You may remember the famous incident of the Internet worm in the Fall of 1988. A worm is similar to a virus in that it is a computer program that replicates itself and spreads. It does not attach itself to other programs and is not spread by sharing software or disks, however. Worms usually spread through networks of

computers. The Internet worm infected and disabled several thousand government and university UNIX computers.

Another term you may come across is Trojan horse. A Trojan horse is a computer program that appears to be a useful program but which is actually destructive. Trojan horses do not generally replicate so they are not as much of a problem as viruses. Once it becomes known that a program is actually a Trojan horse it is easy to avoid.

One class of Trojan horses is joke programs. Joke programs are generally not destructive and do not replicate. They are a type of practical joke on the unsuspecting user and are usually easy to remove once you know what they are. There are quite a few Macintosh joke programs (for example there was one called DOS sHELL which replaced the "Welcome to Macintosh" startup with a DOS shell prompt).

#### **VIRUS HOAXES**

Virus hoaxes are another significant problem on the Internet. Hoaxes are reports of viruses that don't actually exist. One of the most famous virus hoaxes is the Good Times virus. This hoax started in November or December of 1994 and began as an e-mail message warning of another e-mail message with the subject "Good Times." The Good Times e-mail message was supposed to actually be a virus which when the unsuspecting user read it would destroy their hard drive. The warning e-mail message advised users to delete the Good Times e-mail message without reading it and to pass the warning on to all of their friends. The Good Times virus hoax has spread throughout the Internet and regularly crops up on newsgroups, bulletin boards and at companies and universities.

If they stopped to think about it most users would realize that it is impossible to be infected by a virus just by reading an e-mail message. A virus is a computer program that has to be executed in order to

spread. It would be possible to attach a file that was infected by a virus to an e-mail message, but the user would have to detach the file and execute it before being infected. (For example it would be possible to send a Word document infected by the Concept virus by e-mail to someone. However, the user would still have to detach the file and open it to be infected with the virus.) Simply reading an e-mail message cannot infect your machine with a virus. So the Good Times virus, and other supposed e-mail viruses, are, and always have been, hoaxes. If you're interested in finding out more about the Good Times virus you can read the Good Times Virus Hoax FAQ at <http://www.public.usit.net/lesjones/goodtimes.html>. The U.S. Department of Energy's CIAC (Computer Incident Advisory Capability) has a site on the Good Times virus and other Internet hoaxes which is also quite interesting at <http://ciac.llnl.gov/ciac/CIACHoaxes.html>.

#### **WHAT TO DO IF YOU THINK YOU HAVE A VIRUS**

First of all don't panic! Many of the symptoms of a virus infection are also consistent with a hardware or software problem on your machine. Symptoms include changes in the length of programs, changes in file dates or time stamps, slower program or system start-ups, reduced memory or disk space, unusual error messages or screen activity, and system crashes or freezes. If you are experiencing one or more of these symptoms you might have a virus or you might have another software or hardware problem. The easiest way to find out if you have a virus is to scan your hard drive with an anti-virus program. Academic Computing has several anti-virus programs available on Kato. For the Macintosh we have a freeware program called Disinfectant. For the PC we have a number of utilities, including F-Prot, a shareware program, and several utilities for identifying macro viruses.

#### **HOW DOES ANTI-VIRUS SOFTWARE WORK**

Most anti-virus programs are what are called scanners. The scanner program scans all of the files on the disk you specify looking for the presence of viruses. It will also scan for boot sector viruses. A scanner program can only detect viruses it already knows about so the program must be updated every time a new virus is discovered to be effective. Disinfectant and F-Prot are examples of scanner programs.

Scanner programs are extremely easy to use. You just launch the program and tell it to scan your hard drive or floppy for viruses. Some programs have separate scan and disinfectant modes; others will scan and disinfect at the same time. Most will also attempt to repair any damaged files, although this is not always possible.

Other anti-virus programs work continuously in the background. They scan every floppy as soon as it is accessed and scan every file when it is accessed. They may also monitor for suspicious system activities that may be indicative of the presence of a virus. Disinfectant includes a system extension for the Macintosh which constantly monitors for the presence of viruses. F-Prot also includes a background mode.

Viruses use various techniques to avoid detection. Polymorphic viruses mutate into different forms. This feature makes the virus harder to detect by anti-virus software. Both polymorphic boot sector viruses and polymorphic file viruses have been found. Stealth viruses use another technique to avoid detection. The stealth virus monitors your system's read/write calls so that when you open a file it first uninfected it. The file appears normal but when it is closed the virus then reinfects it. A stealth boot sector viruses uses a similar trick. It copies the legitimate boot sector to another part of the disk and displays it whenever the boot sector is examined so that it appears normal. Most good anti-virus programs have techniques for getting around these tricks, however.

## PROTECTING YOURSELF FROM VIRUSES

It's good to be concerned about protecting your computer from viruses, but there's no need to panic about it or take drastic measures. Some people believe that isolating their computer from the network will prevent it from being infected by viruses. In actuality, most viruses are spread from floppy disks, especially disks brought from home, not by downloading infected software from the Internet.

You can protect your computer from viruses by taking some pretty simple steps:

- ▼ Use an anti-virus program, preferably one that includes a background scanner. If you use a Macintosh, we recommend Disinfectant; it's freeware and includes both an on-demand scanner program and a system extension that works in the background. The most recent version of Disinfectant is version 3.7.1 and is available on Kato. The only disadvantage to Disinfectant is that it does not scan for macro viruses.

There are many commercial anti-virus programs to choose from for the PC. We use F-Prot in the PC labs; it's shareware and inexpensive and includes both an on-demand scanner program and a background mode. It has the advantage that it does scan for macro-viruses and also includes frequent updates for new PC viruses.

- ▼ Keep your anti-virus software up-to-date
- ▼ Scan your hard-drives with the on-demand version of your anti-virus software. You don't need to do this very often, but it's a good idea to do it on a regular basis, in particular before you perform a full backup to ensure that your backups are virus-free.
- ▼ Keep your original software on locked floppies. Make copies of the floppies and use those instead of the originals.

- ▼ Don't leave floppies in the floppy drive of your PC. Boot sector viruses infect your computer when the computer attempts to boot from the floppy drive. This most often happens when you insert a floppy into the floppy drive and forget to remove it when you turn off the computer. When you turn on the computer the next day it attempts to boot from the floppy drive. That's when the virus infects your system.

These simple steps should be enough to protect you from most viruses. Making backups has the added bonus of protecting you from other hardware and software disasters so they're a good idea in any case. 🐾

## SOURCES

CIAC Virus Database

<http://ciac.llnl.gov/ciac/CIACVirusDatabase.html>

CIAC Internet Hoaxes

<http://ciac.llnl.gov/ciac/CIACHoaxes.html>

Data Fellows Virus Information Centre

<http://www.datafellows.fi/vir-info/>

Disinfectant manual

Dr. Solomon's Virus Central

<http://www.drsolomon.com/vircen/>

Microsoft's Word for Windows Word Macro Virus page

<http://www.microsoft.com/MSWordSupport/Content/usage/MacroVirus/>

Symantec's Antivirus Research Center

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

Virus Bulletin Home Page

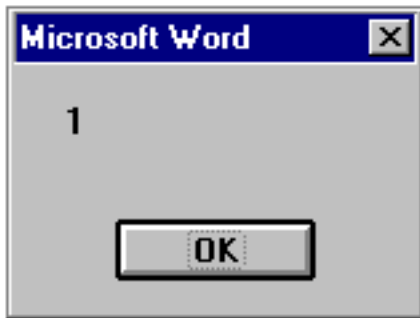
<http://www.virusbtn.com/>

# Tricks & Tips

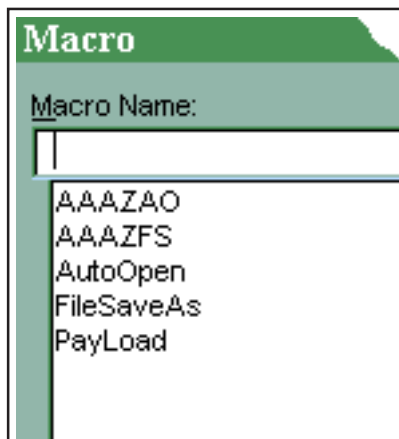
## & Tricks

### REMOVING THE CONCEPT MACRO VIRUS

The Concept macro virus is a virus that affects Microsoft Word 6.x or 7.x documents on both the Windows and Macintosh platforms. The virus does not cause any damage but it forces you to save all your documents as templates which is extremely annoying. Another symptom of the virus is that the first time you open a document infected with the virus you see a dialog box containing only the number "1" and an "OK" button.



To check if a Word document is infected by this virus open the document and select the Macros command from the Tools menu. If you see the macros AAAZAO and AAAZFS in the list of macros then the Concept virus has been installed.



To remove the Concept virus you have to delete the macros installed by the Concept virus. In the Macros dialog box select the macro AAAZAO and click the Delete button. Click Yes when you're asked if you want to delete the macro. Repeat these steps for the macros named AAAZFS,

AutoOpen, and FileSaveAs. There should be another macro called PayLoad that is also installed by the virus. Leave this macro alone; it does no harm, but its presence will prevent the virus from being reinstalled.

To convert a template back into a document, select all of the text in the document by choosing Select All from the Edit menu. Remove the document's final paragraph mark from the selection by pressing Shift + left arrow. Under the Edit menu select the Copy command. Under the File menu select New and then select the template you want to use. Click OK. Finally, under the Edit menu select Paste and then save the document.

Unfortunately, you have to remove the virus macros individually from every document infected by the Concept virus. If you have a large number of infected documents it's easier to use the Microsoft Macro Virus Protection Tool. The primary purpose of the tool is to alert you to Word documents which might be infected by macro viruses. You can also use the tool to scan your files for infected documents, however. It will remove the virus and convert the templates back into documents for you as well. The tool can be downloaded from Microsoft's Web site at <http://www.microsoft.com/MSWordSupport/Content/usage/MacroVirus/>. Be sure to read the documentation which comes with the tool before attempting to install and use it.

As always, feel free to call the Academic Computing Help Desk at extension 7-7777 if you have any questions about the Concept virus or any other virus. 🐾

*This Trick & Tip based on information obtained from Microsoft's Web site.*

# QUESTIONS *and* ANSWERS

---

**Q:** How do I subscribe to a mailing list?

**A:** Send e-mail to `listkeeper@hmc.edu` (or `listkeeper@claremont.edu` if it's a Claremont list). You don't need to specify a Subject line. In the body of the message put the line: `subscribe listname`. To unsubscribe from a list follow the same procedure except send the message: `unsubscribe listname`.

**Q:** How do I find out what lists I'm subscribed to?

**A:** Send e-mail to `listkeeper@hmc.edu`. In the body of the message just type the word: `which`. Listkeeper will send you back a list of all the mailing lists you're subscribed to.

**Q:** How do I find out what lists are available at HMC?

**A:** Listkeeper can send you a list of all of the mailing lists available at HMC. Send e-mail to `listkeeper@hmc.edu`. In the body of the message just type the word: `lists`. Listkeeper will send you back a list of all the mailing lists at HMC.

**Q:** How do I find out who is subscribed to a mailing list?

**A:** Send e-mail to `listkeeper@hmc.edu` (or `listkeeper@claremont.edu` if it's a Claremont list). In the body of the message just type the words: `who listname`. Listkeeper will send you back a list of all the people who are subscribed to the list.

**Q:** I'm the manager of a mailing list but I don't know what the password for the

list is. How do I find out what it is?

**A:** When a new mailing list is created an e-mail message is sent to the new list owner with the list password and other information. It's a good idea to save or print out the message for your future reference. If you can't remember the password and don't have the original e-mail message there's no way to retrieve the password. You can send e-mail to `listmaster@hmc.edu` to request that the password be reset, however.

**Q:** I'm the manager of a mailing list and I need to unsubscribe some students from the list because they have graduated. How do I do it?

**A:** You will need to know the mailing list password in order to unsubscribe people from a mailing list. Send e-mail to `listkeeper@hmc.edu` (or `listkeeper@claremont.edu` if it's a Claremont list). In the body of the message type the following line of text for each person you want to unsubscribe from the list: `approve password unsubscribe listname email_address`.

**Q:** Where can I find anti-virus software on Kato?

**A:** Disinfectant for the Macintosh is located on the volume Kato.Mac in the folder `Utilities:Free Anti-virus:Disinfectant 3.7.1`. Anti-virus software for the PC is located in the directory `G:\APPS\UTILS\DOS\ANTIVIR\`. 🐕