



# Computer Viruses

ResNet - Northern Arizona University

## Introduction

Getting a computer virus can be an unnerving situation. On ResNet, the most popular operating systems are Windows and Macintosh. There are many known viruses for both operating systems. Northern Arizona University is committed to providing a safe and reliable network for students, faculty, and staff. This document will provide you with the knowledge to begin to protect your computer and prevent you from infecting other users.

## What is a Computer Virus?

The most simplistic description of a computer virus is: a computer virus is to a computer as a human virus is to a person. It makes you sick in varying degrees depending on the strength of the virus and your ability to withstand it. Technically, a computer virus is a self-replicating program, written intentionally to modify,

disrupt, or damage files and programs, and to spread throughout the system without your knowledge or permission. Computer viruses are designed to attach themselves to other program files and become activated when those programs are run. While active, a virus replicates by copying itself to other programs on any available

disk. Computer viruses are easily spread from system to system, and since many ResNet users will be sharing information with other users, it is very likely that many systems will become infected at some point in time. Computer viruses have been infecting computers for over 30 years.

## How Do You Get a Computer Virus?

Our experience is that many people are unaware that their computers have been infected by a computer virus and attribute their problems to another reason. While computer viruses may not be the leading cause of loss of data and other computer related problems, viruses probably cause more damage than most people realize. Computer viruses move

from computer to computer when people share executable (.exe) programs and bootable disks either by disk swapping or over computer networks.

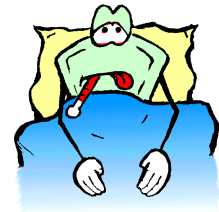
Viruses can be transmitted by:

- Starting a PC from an infected floppy disk, zip disk or CD
- Executing an infected program

- Opening an infected file

Common routes for virus infiltration include:

- Floppy disks or other media that users can exchange
- Email attachments
- Pirated software
- Shareware



How your computer feels after getting a virus

### *In This Issue:*

- [What is a Computer Virus?](#)
- [How Do You Get a Computer Virus](#)
- [Types of Computer Viruses](#)
- [Protecting Your Computer](#)
- [NAU and Viruses](#)
- [What Should I Do if I Suspect a Virus?](#)
- [Virus Resources](#)

*“An executable file is one that ends in .exe, .bat or .cmd”*

# Types of Computer Viruses



Don't let a computer virus do this to your PC!

*“Computer virus: a computer program that attaches itself to another program in computer memory or on a disk, and spreads from one program to another. Viruses are often malicious and may; damage data, cause the computer to crash, display messages, and delete files.”*

## Boot Sector Viruses

A boot sector virus places its starting code in the boot sector. When the computer tries to read and execute the program in the boot sector, the virus goes into memory where it can gain control over basic computer operations. From memory, a boot sector virus can spread to other drives (floppy, network, etc.) on the system. Once the virus is running, it usually executes the normal boot program, which it stores elsewhere on the disk.

## Macro Viruses

Unlike previous viruses, macro viruses do not infect programs; they infect documents and templates. Opening a document or template that contains a macro virus will infect your system and the virus will spread to other documents and templates you may have on your system. Many applications, such as Microsoft Word and Excel, support powerful macro languages. Once a macro virus gets onto your machine, it can embed itself in all future documents you create with the application.

## Program Viruses

Program viruses are the most common and they come in the forms of files that end in **.exe**, **.bat** or **.com**. They infect your system when the program is executed. The infection can spread to other programs and usually grows in size, often unnoticed by the computer user. Program viruses can travel on media like a CD or across the Internet by email

attachment. They hide in an apparently useful program and then run when the program is opened. Program viruses may be deliberately hidden in a program by the developer, or attached after the fact at some point along its travels from computer to computer.

## Hoaxes

The first thing you should notice about the message is a request to "send this to everyone you know" or some variant of that statement. This should raise a red flag that the warning is probably a hoax. No real warning message from a credible source will tell you to send this to everyone you know. Next, look at what makes a successful hoax: technical sounding language, credibility by association.

If the warning uses the proper technical jargon, most individuals tend to believe the warning is real. For example, the Good Times hoax says that "...if the program is not stopped, the computer's processor will be placed in an *nth-complexity infinite binary loop which can severely damage the processor...*". The first time you read this, it sounds like it might be something real. With a little research, you find that there is no such thing as an *nth-complexity infinite binary loop* and that processors are designed to run loops for weeks at a time without damage. When we say *credibility by association* we are referring to who sent the warning.

## Worms

Worms are parasitic computer programs that replicate, but unlike viruses, do not infect other computer program files. Worms can create copies on the same computer, or can send the copies to other computers via a network. Worms often spread via email in the form of a joke program or software of some sort. It may do damage and compromise the security of the computer.

## Trojans

A Trojan horse (a.k.a Trojan) is a program that appears to do something amusing or useful (screen saver or game) and actually does something else. It may destroy data or compromise your system's security. However, a Trojan horse does not replicate itself or transmit itself to other computers. The most (in)famous Trojan horse was the so-called "Love Bug" in May 2000. If this apparent love letter was opened, it would unleash a slew of problems, such as sending itself to everybody on your email address book or IRC channel, erasing or modifying your files, and downloading another Trojan horse program designed to steal your passwords. Many Trojan horses also allow crackers (aka "hackers") to take over your computer and "remote control" it, such as to take over your IRC channels, use your computer to serve off illegal material, or attack other users on the campus network and across the Internet.

## Protecting Your Computer

To protect your computer, take a proactive approach! It is much easier to prevent contracting a computer virus than it is to remove it.

Here are our suggested guidelines:

- Use a good commercial antivirus product like McAfee VirusScan or Norton Antivirus. (NAU has a McAfee license that covers students. See “NAU and Viruses”)
  - Update your virus definitions files frequently. For example, setup your software to check for updates weekly.
  - Never double-click (or launch) any file, especially an email attachment, regardless of who the file is from, until you first scan that file with your anti-virus software.
  - Turn on macro virus protection in MS Word and beware of all word macros, especially if you don't know what they
- If someone unexpectedly sends you an executable file - in other words, a file that ends in .EXE, .CMD, .BAT - delete it.
  - If you use Windows 2000/XP, use a strong password (has numbers, and punctuation)
  - If you share files, password them and only allow READ access.
  - For Windows computers run Microsoft Windows Update weekly to patch vulnerabilities. <http://www.windowsupdate.com>
  - For Macintosh computers run Software update <http://www.apple.com/swupdates/>

## NAU and Viruses

Northern Arizona University is committed to providing a safe and reliable network for students, faculty and staff. As part of this commitment, NAU runs virus detection software on the central Email server. This service scans all Email for known viruses prior to their delivery. If a virus is found, it is held on the mail server and then notifies the user by Email of the problem. This service has proven itself to be most valuable for NAU as a first stage preventative measure against viruses reaching computers on the NAU network. NAU gathers statistical information on the number of emails processed and viruses trapped each day. To view the statistics :

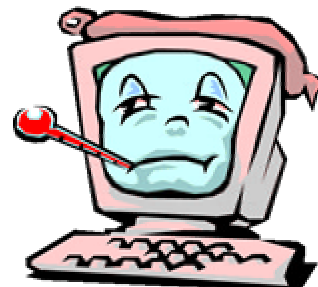
[http://mailgate1.nau.edu/virus\\_count/email\\_out.html](http://mailgate1.nau.edu/virus_count/email_out.html)

are. For more information, check out [Macro Viruses . http://www.nau.edu/resnet/support/documentation](http://www.nau.edu/resnet/support/documentation)

*“Our experience is that many people are unaware that their computers have been infected by a computer virus and attribute their problems to another cause.”*

As part of this commitment, NAU has purchased a campus wide license that provides McAfee Antivirus software to students, faculty and staff.

You can download McAfee from the ITS Software Downloads page at [http://www4.nau.edu/its/swat/Software/SW\\_Search.asp](http://www4.nau.edu/its/swat/Software/SW_Search.asp) . If you need help installing or configuring McAfee, please contact the Academic Computing Help Desk at 523-9294 to setup an appointment with a Student Computing Assistant.



## What Should I Do if I Suspect a Virus?

If your computer becomes infected with a virus, don't panic! Please contact the Academic Computing Help Desk immediately (523-9294), and setup an appointment with a Student Computing Assistant. Do not use the infected computer, and unplug your network cable from the jack or DSL modem. If your antivirus software says it has cleaned the virus, please call for an appointment anyway. Some viruses take a special application to fully remove it. In the case of rather nasty viruses, you may have some damaged files that cannot be fixed. If you backup your computer, you may be able to restore the damaged files (*after scanning them first*). Call the Academic Computing Help Desk at 523-9294 if you need any assistance.

*“There are thousands of viruses that are detected and removed each month by NAU Email servers.”*

## Computer Virus Resources

There are a variety of online newsletters and web pages which provide up to date information about viruses. Here are some examples:

- ◆ Virus Hoaxes
  - [Sophos Antivirus Hoax Information](http://www.sophos.com/virusinfo/hoaxes/) (http://www.sophos.com/virusinfo/hoaxes/)
  - [HoaxBusters Virus Hoax Information](http://hoaxbusters.ciac.org/) (http://hoaxbusters.ciac.org/)
  
- ◆ Virus Information, Hoaxes and Alerts
  - [McAfee Antivirus site](http://www.mcafee.com/anti-virus/default.asp) (http://www.mcafee.com/anti-virus/default.asp)
  - [Norton Antivirus site](http://www.symantec.com/avcenter/index.html) (http://www.symantec.com/avcenter/index.html)
  - [F-Secure Antivirus site](http://www.f-secure.com/virus-info/) (http://www.f-secure.com/virus-info/)
  
- ◆ McAfee Antivirus software for students
  - [NAU's Virus Resource Center](http://www4.nau.edu/its/swat/Software/virus.asp) (http://www4.nau.edu/its/swat/Software/virus.asp)

**ResNet**  
**Northern Arizona University**

*We're on the Web!*  
[www.nau.edu/resnet](http://www.nau.edu/resnet)

**Phone: 928-523-9294**  
**Email: [ResNet.Support@nau.edu](mailto:ResNet.Support@nau.edu)**

*ResNet provides high speed internet connections and networking support for the on-campus students of Northern Arizona University. The ResNet staff works closely with the Academic Computing Help Desk to provide support to NAU students living in the on-campus residence halls including installing network cards and other connection related issues. If network or virus issues are unable to be resolved over the phone, Student Computing Assistants are available by appointment to come to a student's campus residence and resolve the problem there. You can schedule an appointment by calling the Academic Computing Help Desk at 523-9294.*