



ITS Virus and Malware Quick Help Guide

Washburn University's Information Technology Services must deal with computer viruses and malware on a daily basis. ITS repairs and maintains several hundred computer systems that are Washburn owned and operated. Because of this demand and other duties ITS is unable and unprepared to handle students, faculty, and staff personal computers. This document gives information about what users can do to find if a computer is infected and whether to seek further professional assistance with removing a virus infection.

Legal Notice:

Washburn University is not liable for any modifications of hardware or software or removal of data from your computer. This document is presented as is with no guarantee. It is for informational purposes only. The reader of this document assumes all risk and financial liability from following these instructions.

Instructions for Windows XP

Q1: Help! I think I have a virus.

A1: There are three ways to determine if a computer has a virus or malware.

1. An antivirus software or malware detection program gives a warning that it has found an offending file or program.
2. The computer shuts down or programs do not work correctly. Internet windows may pop up at random times. A slow network connection may be noticed.
3. A program or file is in the wrong location or has been inexplicably modified. This method is more common with people who have extensive computer experience.

If a virus is suspected, the user should run antivirus scan software (see Q4 with some recommended vendors). If antivirus software does not work or will not open, see below.

Q2: I have tried to run my antivirus software, but it will not open.

A2: If the antivirus software is not working, a virus may have disabled or corrupted it. Contact the antivirus vendor for information on how to fix it. Otherwise, contact a professional to restore functionality on the computer.

Q3: I cannot get to my antivirus vendor's Web site. Instead I get taken to another site.

A3: There are two possibilities. Either the host file has been rewritten or there is a proxy server running and rerouting the network connection. Proxy servers are more common with malware, while viruses are more likely to rewrite the host file.

To see if the host file has changed:

1. Click **Start** then select **Run**.

2. In the Run window type in **explorer**.
3. Click the **OK** button.
4. Navigate to **C:\WINDOWS\SYSTEM32\DRIVERS\ETC** *Note: if a warning appears that system files are hidden, click the link to "Show the contents of this folder."*
5. The ETC directory should include a file called **"HOSTS"**.
6. Double-click the file to open it. If the system asks for a program to open the file, select **Notepad**.

Some companies have a custom IP address set. Otherwise, the **HOSTS** file should appear as:

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
# 102.54.94.97 rhino.acme.com # source server
# 38.25.63.10 x.acme.com # x client host
127.0.0.1 localhost
```

If the **HOSTS** file differs from the default (above), a virus has changed the file. Users can correct the file by removing the contents of the file and replacing it with the default information.

To determine if a proxy is set up:

1. Click **Start**. Select **Control Panel**.
2. Click the category Network and Internet Connections. (If the Control Panel is set for "Classic View," skip this step and proceed to step 4.)
3. Click **Internet Options**.
4. In the Internet Options window select the **Connections** Tab.
5. Click the **LAN Settings** button.
6. If there is a checkmark in the box beside "Use a proxy server for your LAN..." remove the checkmark unless you know you should be using that proxy server.

After making the changes, close Internet Explorer and restart it. If Internet Explorer still has a problem, check the proxy settings and the HOSTS file again. If the changes to the proxy settings and HOSTS file are reset, the virus problem may be advanced and will require more troubleshooting. Please consult an antivirus vendor or PC technician.

Q4: I do not have any antivirus software. Where can I get this software?

Antivirus software can be purchased from most retail electronics or computer stores. The two most common brands are Norton Antivirus and McAfee. Below you will find some online resources for antivirus software.

- Norton Antivirus: **www.symantec.com** (fee based)
- McAfee: **www.mcafee.com** (fee based)
- Antivir: **www.freeav.com** (free for private and individual use)
- Grisoft: **free.grisoft.com** (free for private and individual use)
- Trend Micro: **www.trendmicro.com** (free online scan)