

November, 2002
Vol. 19, No.5

A Technology Newsletter for Extension Specialists

Extension Technology and Computer Services
22 Heinkel Building, Columbia, MO 65211

573-882-2096



**Computer House
Cleaning**
page 2

S is for Sharing
page 4

**Inventory Reports
Due**
page 4

Anti-Virus Corner
page 2



University of Missouri,
Lincoln University,
U.S. Department of Agriculture
& Local University Extension
Councils Cooperating

University Outreach and
Extension does not discriminate
on the basis of race, color,
national origin, sex, religion, age,
disability or status as a Vietnam-
era veteran in employment
or programs.

Useful Information

By John Myers

While helping some users this past month with problems on their computers, I realized that the users wanted to learn more about the terms we use to describe events that take place on their computer. After explaining these events, the users would say "I wish someone would write this down for reference." The following paragraphs will explain what viruses, worms, Trojan horses, and hoaxes are and what tools we have to understand and combat them.

There are many different definitions of a computer virus. Most definitions state a virus is a program that can infect other programs or files. Until the infected program or file is processed on the computer, it can't do harm or spread itself. It requires "a user" to get it started. There are many different types of viruses; boot sector viruses, macro viruses, file viruses, logic bombs, and time bombs to name a few. Not all viruses are harmful, some just display messages on the screen or play little tricks, but there are some viruses that will delete files or reformat your hard drive.

Since a virus requires a user to get it started, there is time to find and clean viruses. This is what antivirus software does. When properly configured, antivirus software will scan a program or file before it is loaded into the computer's memory. If the software finds a virus it will either remove the virus or put the infected file in quarantine so it can't be spread. Viruses' main method of spread is by email and file transfer. Our email system has antivirus software running and scans all email messages for known viruses and removes any found in email. This prevents it from actually reaching your inbox. We also have antivirus software on our computers, but sometimes it gets turned off and then it doesn't get turned back on. There are a couple of things you can do to help protect yourself including leaving Norton Anti-virus enabled on your machine. Turn off the "Preview Pane" option in Outlook. If you get an email from someone you don't know that looks suspicious, don't read it! Delete it. If you get a cd or floppy from someone or have put your floppy in someone else's computer, scan it with the antivirus software before using it in your computer.



A worm is a virus that doesn't wait for someone to spread it around; it uses networks and the Internet to propagate itself. In English, this means worms are a more dangerous type of virus. They don't require a user to start them and they look for ways to propagate themselves. Worms look for file shares. When you create a file share, the default security permissions are set to allow everyone to access the file share. To protect yourself, you should restrict access to your file shares. If

you are running a Windows 9x operating system you should assign a password to your share. If you are running a Windows NT operating system (Windows 2000 or Windows XP) you should remove the "everyone" permission and assign rights to particular users or groups.



A Trojan horse is a program that appears to do one thing, but is actually doing malicious activities in the background. Technically, Trojans are not viruses since they do not replicate themselves, but Trojan horse programs can be just as destructive. Trojan horses can

be used to reduce security on your computer to allow others to gain access.

Hoaxes are the best "virus" of all. Hoaxes are usually emails that turn YOU into the virus. The email scares you into thinking that you received a virus and instructs you to delete it. It will tell you what to search for and delete. The only problem is that the file it wants you to delete is not infected and is a vital operating system file. Depending on the file you delete, things can immediately start effecting the operation of your computer or wait and make it unbootable.

If you receive a message about a possible virus, first think before acting. Ask yourself, "Is this person an expert on computer viruses?" The answer is usually no. Find out about the virus yourself first and then act. For example, recently I have seen an old hoax about jdbgmgr.exe reappearing. I went to Norton's site (<http://www.norton.com/>) and clicked on the "Search Virus Encyclopedia". In the search box I typed jdbgmgr.exe and then clicked on the search button. I was returned four hits that told me about this hoax. There are other web sites like <http://www.mcafee.com/anti-virus> that you can visit to find out if a virus is a hoax. If it's not a hoax then the sites will display useful information on how to remove the infection.



Computer House Cleaning

by Joe Lear and Jill Dourty



Some problems with computers can be avoided by just doing a little cleanup and preventative maintenance. Performing the following jobs on a weekly basis will help you keep your computer operating at its best.

Deleting Temporary Files:

Temporary files are created by programs as you create and edit files and the operating system performs its function. These files do not always get removed and they can interfere with your computer's operation if they are not removed regularly.

To Remove Temporary files:

1. Close all programs such as Word, Outlook, Internet Explorer, and any other programs.
2. Click the Start button, and then click Run from the Start Menu.
3. Type in C:\WINDOWS\TEMP on Windows ME/98/95 machines and TEMP on Windows 2000 and XP machines.
4. The Temp Directory window should appear.
5. Click once in the open window to make sure it is selected. Press the CTRL+A keys to highlight all the files and folders in the directory.
6. Press and hold the SHIFT key while pressing the DELETE key.
7. Click YES to ALL when asked to delete read-only or files that end in *.exe.
8. When all the files are deleted close the Temp folder window.

Deleting Temporary Internet Files:

As you surf the web, Internet Explorer keeps a copy of the web pages to help speed up your surfing experience as you browse. These files can take up to 10% of your hard drive space and can possibly lead to problems returning to pages on your next visit. Also, some web pages place cookies on your computer to remember your preferences when you visit their site again. If these cookies become corrupt, it can prevent you from accessing that site. Internet Explorer also keeps a history of the sites you have

visited for several days. These take up space on the drive and can be deleted as well.

To delete Temporary Internet Files:

1. Start Internet Explorer.
2. Click Tools on the Menu Bar and Click Internet Options.
3. Click the Delete Files Button and Click OK on the Delete Files Dialog Box.
4. Click the Clear History Button and then Click Yes to Confirm the Deletion.
5. You can click the Delete Cookies Button, but it is not absolutely necessary unless you are having trouble accessing some sites. Click Ok to confirm that you want to delete your cookies.
6. Click the Ok Button to Return to Internet Explorer.
7. Close Internet Explorer.

You can also free up disk space by emptying the Recycle Bin. On the Desktop Right Click on the Recycle Bin and Choose Empty Recycle Bin. Click the Yes Button if you are asked to confirm.

Windows also keeps track of the documents and files most recently accessed and stores the list in the Documents section of the Start Menu. You can clear this list by Right Clicking on the Task Bar, which is the bar which contains the Start Button and the Clock, and then Selecting Properties. (On XP Machines, click the Start Menu Tab, and then click the Customize Button.) Next click the Clear Button. Click OK and OK to exit the taskbar properties.

For Windows 2000, ME, 98, and 95 machines, click the Advanced Tab after Clicking properties on the Task Bar and then click the Clear Button. Click OK to exit the taskbar properties.

Running Scandisk and Defrag:

Scandisk checks your files and hard drive for errors and corrects these errors to prevent possible file damages and to keep the computer operating at its best. Defrag reorganizes your files for faster access.

Running Scandisk for Windows 2000 and XP:

1. Double click My Computer. Next Right Click on your hard drive and choose Properties.
2. Click the Tools tab in the window that appears.
3. Click the Check Now Button in the Error Checking section.

4. Click the Start Button. Error Checking will begin.
5. If you receive a message stating that the error checking could not be completed, place a check mark in Automatically fix file system errors and Scan for and attempt recovery of bad sectors. Click the Start button. Click Yes to schedule the error checking to happen on the next time the system restarts and then restart the computer.

Running Scandisk for Windows Me, 98, and 95:

1. Follow Steps 1-4 as stated above.
2. When complete, Click OK on the Scandisk report that appears, then Click Close.

Running Defrag on Windows 2000 and XP:

1. Double Click My Computer. Next Right Click on your hard drive and choose Properties.
2. Click the Tools Tab in the window that appears.
3. Click the Defragment Now Button.
4. Click the Defragment Button in the Defragmenter Program.
5. Click Close to Exit the Defragmenter. Click Ok to Exit the Drive Properties Dialog Box.

Running Defrag on Windows ME, 98, and 95

1. Follow Steps 1-3 for Running Defrag on Windows 2000 and XP.
2. Click Yes When the Defragmenter has completed.
3. Click Ok to exit the drive properties dialog box

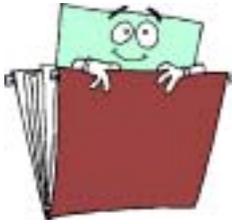
If you have trouble running Scandisk and Defrag on your Windows ME, 98, or 95 machines, try disabling the Antivirus software by right clicking on the Gold Shield next to the clock and clicking once on enable File System Real Time Protection. Then, try running scandisk and defrag again. Be sure to turn on the Antivirus software again when you are done. Without this program running, you aren't protected from viruses.

One of the most important things to keep your computer running smoothly is to install all the latest critical updates. For more information on critical updates see the July 2002 *Inner Circuits* article entitled Windows Updates by Charles Baerwald.



S is for Sharing

by Joe Lear



The S drive is a great place to share information with other faculty and staff across the state and judging by the amount of data on the S drive, there is a lot of sharing going on. We're happy to see everyone making full use of the service.

The best way to place files on the S drive is to save the file from the program to your local machine or, if you have a server, Q or R drive and then copy the file to the S drive.

Trying to save a file directly to the S drive can cause data corruption which will make your file unusable. If you save the file directly to the S drive, it will use all your system resources and that will prevent you from using your computer for other operations.

This goes for using a file from the S drive as well. Copy the file to your local machine or to your Q or R drive before trying to open the file. By opening or printing the file directly from the S drive you will tie up your computer making it impossible to do other jobs. You will also tie up the office internet connection making it impossible for others in the office to get their jobs done.

If you are collaborating on a document with others and sharing the file through the S drive, let the others

in your group know you are working on the file and copy it to your desktop. Make your additions and/or changes and then save the file to your local machine. When you are finished editing it, copy it back out to the S drive—again, do not try to save the file to the S drive!

When copying data to or from the S drive remember that in offices running on 56 Kb lines, it will take about 5 minutes to copy 1 megabyte of file size, so a 5 megabyte file would take 25-30 minutes to copy to or from the S drive. Even though the copy process may slow your computer while it's working you can still do other things on your computer, like read *Inner Circuits*!

Inventory Reports Past Due Date

by Jeanne Meyer

Inventory reports were mailed October 25 to all Extension offices. We requested that the reports be checked for accuracy and returned to me by November 15, 2002. At this time, we have received approximately 60 percent of the forms. Thanks to everyone who has returned them. If you haven't sent them, please do so at your earliest convenience. If you need another copy of your inventory reports, please contact me and I will send you another report.

Anti-Virus Corner

Current Norton Anti-Virus Versions



Program Versions:

Program: 8.00.9374
Scan Engine: 4.1.0.15

Virus Definition File:

Version: rev.4
Date: 11/13/2002



(Your versions should be at this level or greater.)

See <http://etcs.ext.missouri.edu/tips/default.htm> for instructions on updating your anti-virus.

Inner Circuits Mailing List Corrections/Additions

- Send an email message to ETCS or call 573-882-2096 to correct an address, add someone to or delete someone from the mailing list.