No. 17, January 1995

VIRUSES REVISITED

This issue in the series was supposed to be about RAM, but I thought it best to postpone that subject based on a recent experience. Remember back to #13 in the series on VIRUSES AND HOW TO FIGHT THEM? Remember that I talked about the VSAFE program that comes with versions of DOS from 5 up? Remember how I told you that it was a TSR (Terminate and Stay Resident) program that would watch for a virus attack ... and prevent it? Did you take my advice? Well, I did, and yesterday, it saved my tail! Here is some background.

My students at both the Medical College of Wisconsin and the University of Wisconsin - Milwaukee use several educational software packages - Computer Assisted Instruction (CAI) modules - authored by me. They use them to learn about medical genetics, and about the cells and tissues of several organ systems in the human body. These CAI packages work well for the students. They can use them to learn at any hour of the day or night, at home or wherever they can get to a computer - even an old XT will work fine. A CAI package on one subject consists of several lessons, each followed by a test. When the student takes a test, the results are written directly to their unique student file on the floppy that contains the lessons. When finished with the entire package, a student returns the disk, I extract the grade from their disk (no, they can't fiddle with the grade...it is in an encrypted file that even I cannot successfully alter), and I give them credit for the work. They like it, and I like it. It is not the only way to learn, but it is a pleasant diversion from the usual classroom or laboratory experience; almost all students enjoy some self-directed learning.

Now, here is what happened. Yesterday, I had over 20 CAI packages to grade, but no time to do it during the day. Furthermore, students who had returned disks were anxious to check out new ones they had not yet completed. Therefore, the solution was to copy the student files onto a single floppy to take home and grade, thereby releasing all the student floppies for checkout by the clamoring students. Simple enough. However, my computer at UWM only reads 5¼-inch floppies, and each student gets both a 5¼-inch and a 3½-inch program disk, so they can work with whatever is available to them. Therefore, I borrowed the use of a colleague's computer, in a laboratory next to my office. It has both size drives, and I successfully copied all the student files to a floppy that lives in my briefcase for transporting files to work or back.

After supper, I prepared to run the program that un-encrypts the student files and sends the grades to my printer. I put the disk in the drive, and gave the command DIR A: just to take stock of the student files there. The computer beeped loudly, and the following flashed on the screen:

```
VSafe Warning
Disk infected by the Michelangelo virus
Run MSAV to clean the virus
Press any key.
```

The message was white letters on a bright red background, except that the top line ("VSafe Warning") flashed on and off in a bright yellow hue. It got my attention!

Of course, the important thing here is that VSAFE was sitting in memory, watching all proceedings. When the DIR command was given, it butted in before DOS could do anything, looked at the disk, determined it was infected, and STOPPED EXECUTION OF THE DIR COMMAND, which would have transferred the virus infection to my hard drive. Yes, it saved my tail. It is much harder to get rid of a virus infection on a hard drive than on a floppy, and there is much more data at risk.

Without going into great detail, let me relate that I captured those student files, and the students got their grades. The source of the infection? It turned out to be a graduate student of my colleague, who often used floppies brought into the laboratory from outside. It was my colleague's computer, not my student's computers, that was the source of the virus. Computer security experts at UWM are now examining the disk.

You know the moral of this story. It is quite simple. Everyone is at risk for becoming infected. If you take no preventive measures, you are courting disaster. If you take preventive measures such as I did, you can PREVENT disaster. It is a lot less stressful and time consuming to prevent an infection, than to try to cure an infection after it happens. Get out your DOS manual...the name of the program is VSAFE. Safe computing!

PS: My colleague was told the virus damaged the old drive, and that it was beyond repair. He went out and bought a new one. Then he gave me the old one to see if anything could be done. After putting it in a home computer and booting from a floppy, it took about 10 minutes to determine that the virus had scrambled the Master Boot Record, a little one-sector program on every hard drive that allows it to boot. The command FDISK /MBR wrote a new Master Boot Record and fixed the problem, a 10 second job to type and execute. The drive is now perfect. The lesson to be learned: while a virus infection may indeed scramble your data, it causes no physical damage that cannot be undone. Take heart!