May 8, 1997

Practicing safe computing

Macro viruses are everywhere so smart users need to take precautions / **Simson L. Garfinkel**

COMPUTER VIRUSES are the scourge of the on-line world. Because the Internet has made it easier for people to communicate with one another, it has also made it dramatically easier for computer viruses to spread.

A few years ago, when viruses like Brain and Friday the 13th made front-page news, there were two simple rules that computer users could follow to protect themselves from these electronic vermin: Don't share programs, and don't leave floppy disks in your computer's drive when you reboot the system. This protected users against viruses that could hide in application programs as well as those dreaded "boot-sector" viruses, which hid on the first track of a DOS floppy disk.

Then Microsoft Corp. released Word 6. Soon millions of PCs and Macs around the world had become breeding grounds for a new kind of virus. Word 6, as well as Word '95 and Word '97, all have the ability to let you hide computer programs inside of word processor documents.

Called macros, businesses use them to create forms such as expense or travel reports as well as to automate common tasks. Virus writers seized upon the Word macro language to create a new generation of viruses.

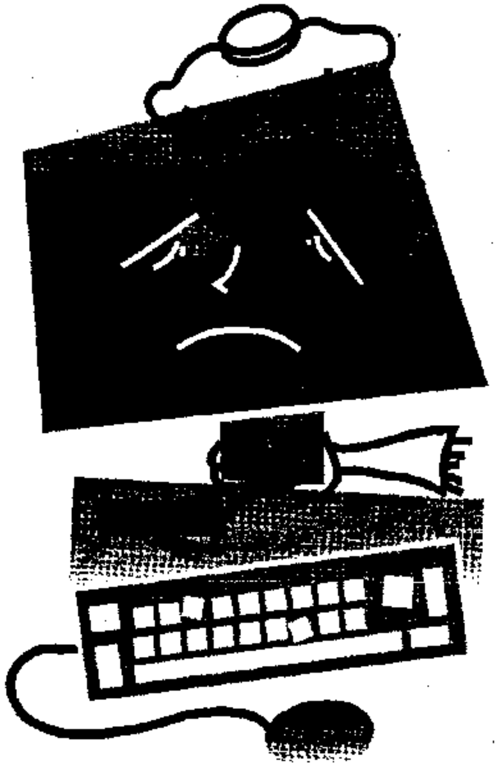
Word macro viruses automatically run when you open an infected file. A typical virus will infect your computer's Microsoft Word templates. Then, every time you open another word processor file, it gets infected too. Some viruses do little more than spread themselves around your hard drive in this manner. Others randomly insert or delete words in your documents, and some can even run other programs on your computer, snoop around your company's network, and send electronic mail.

Because most Word macro viruses do not actually shut down your computer and keep it from rebooting, few companies have regarded these beasties as anything other than annoyances. Many office workers continue to work with infected computers and some companies, including Microsoft, even distribute CD-ROMs containing infected Word documents.

To prevent infection, I adopted a "no Microsoft Word attachments" policy and asked people sending me e-mail to resend the files as plain text if they wanted me to read it.

Another way to deal with attachments is to open them with a word processor other than Microsoft Word. However, many other programs cannot fully interpret Word files because Microsoft has been unwilling to share the Word file format with competitors. An option for Windows 95 users is to open the file with WordViewer. This program will let you see what's in the potentially hostile file and copy the text (but not the macros) into another document.

Another way to avoid Word macro viruses is *not* to use Microsoft Word, but that's not practical. Word is a vastly superior word processor.



So, you need good antivirus software to be secure. The antivirus field is viciously competitive, with many companies making claims about their own and other products that are difficult for the average computer user to verify.

After speaking with a few experts, and trying several programs, I settled on VIREX, by Datawatch Inc., to protect my Macintosh computer, and Dr. *Solomon's Anti-Virus Toolkit to* protect by Windows 95 machine. Both automatically check each Microsoft Word attachment as it is downloaded for macros viruses. They can also scan your computer every day for unexpected infections, do quick scans when you boot your system, and make it relatively easy to download updates – essentially lists of new viruses that have been discovered.

Although some computer users actually blame Microsoft for creating the virus problems that now plague them, the company seems to be taking the viral threat seriously. Word '97 will include some antivirus features, automatically scanning for common viruses and warning users if they are about to open a file containing macros – although the program can't tell the difference between a harmless toolbar and a vicious virus.

But Microsoft hasn't given users a way of disabling the built-in basic interpreter, says Wolfgang Stiller, president of Stiller Research, a maker of antiviral software. This means that your computer can still get infected with a word macro virus – for example, if somebody else using your computer opens a virus-infected file – and then it will pass the infection along. "I have spoken to a number of users that don't really understand what Microsoft did in Word '97 and think they no longer need to worry about Word macro viruses," says Stiller.

Microsoft has begun a new project to work closer with the antivirus community. But while the company recently issued a joint press release with the National Computer Security Association saying it would "help antivirus vendors give customers better tools against macro viruses," there is a lot of bad blood that the company must overcome.

"The truth is that they have not solved the problem at all, they are *creating* the problem . . . by not telling us what the bloody file formats are," says Vesselin Bontchev, an antivirus researcher in Iceland. "In short, they are idiots."

In short, from now on, I'm using my antivirus software religiously.

Technology writer Simson L. Garfinkel can be reached at plugged-in@simson.net