The SirCam worm has been spreading around the world in the last month and is one of the most widely prevalent worms today. This worm sends its code to everyone listed in the e-mail address book of infected systems by attaching itself to randomly selected documents. For full information see (among many other places) <http://www.trusecure.com/html/tspub/hypeorhot/rxalerts/hohsircam_cid118.shtml >.

I had an interesting experience recently when an infected computer began sending out files every twenty minutes. I received half a dozen files in a row from the same user. Some were MS-Excel spreadsheets, others were MS-Word documents. These files seemed to be confidential; they included lists of members for a professional association, some budget figures, and other information that the author surely did not want spread throughout the Internet.

I did not know the originator of these messages, but the return address seemed valid, so I sent an e-mail after seeing the first file warning her of the infection. When I continued to receive files over the next couple of hours, I did a WHOIS on the sender’s domain and located a telephone number for a technical contact. The receptionist transferred me to the victim, who explained that she was aware of the infection and working with technical support to update her antivirus software and remove the worm.

I asked, “Have you unplugged your system from your Internet connection?”

She had not.

I (quite emphatically) instructed her to pull the network connection at once and put it back in only when disinfection was complete. She did so, and I received no further infected confidential files from her computer.

The lesson here is that it’s very nice to update your antivirus and disinfect your machine, but if you are the victim of an e-mail enabled worm, for goodness’ sake unplug your computer at once from your network connection to prevent further activity by the worm.

In summary, technical support staff should instruct their users to

(a) report all suspected malicious-software infections at once;
(b) never criticize a user for a false positive (thinking there’s a virus when there’s not);
(c) tell users to disconnect their possibly-systems from access to all networks immediately;
(d) resolve the problem using updated antivirus software and appropriate disinfection techniques; and
(e) only then reconnect the system to the Internet.

In addition, I urge everyone not to ignore infected computers. It may not be practical for everyone to respond to each infected message sent by a worm (and if everyone responds to every infected message the bandwidth consumption will be enormous), but if you receive several infected files from the same computer over an hour or so, it’s only courteous to let the originator know that they have a problem. After all, someone has to be the bearer of the bad news.