



Your PC with a new  
memory upgrade!



DealsOnTheWeb Daily Deal: [Nextar P3 Portable GPS Navigation System with MP3 Player](#): \$114.99 Delivered – \$25 Drop

## TMO Reports - Mac Vs. Windows On Campus: Does Platform Matter In Virus Assaults?

by [Robyn Weisman](#), 2:15 PM EDT, September 30th, 2003

The onslaught of Internet-borne viruses and worms could not have come at a worse time for college and university campuses. The latest SoBig worm, the "SoBig.F" began its attacks in late August, around the time most colleges and universities have begun their freshmen orientation programs and campus-wide registration process.

The travails of these schools, most of which run on Windows, have been well-publicized. Returning students have come equipped with infected laptops that have clogged campus [mail servers](#) with thousands of SoBig.F-generated spam. Understaffed IT departments have resorted to charging students fines for hooking infected PCs onto networks and charging additional fees to have these PCs cleaned and patched. Networks themselves have been forced to shut down in order to contain the havoc generated from seemingly innocuous e-mails apparently sent by friends promising a new "wicked screensaver" or a clip from "That Movie."

About the only ones happy about the development are the Internet security software vendors who stand to make a mint cleaning, patching, protecting, and terrifying beleaguered IT people, who only get noticed when things are screwed up.

### Everyone pays

Craig Schmugar, virus research engineer with McAfee's Anti-Virus Emergency Response Team (AVERT), told The Mac Observer that in some respects, college campuses are somewhat similar to corporate environments with their varying mix of platforms, both on the client and server side. But unlike corporations, college campuses generally have less coverage on the support side.

Moreover, trying to track down infected computers takes more time because students regularly plug into so many different networks on campus, Schmugar said. A student may plug his or her computer into a classroom network, but by the time the infected PC is discovered, that student has gone and is now logging on to his or her dorm network. This moving target aspect makes for a greater loss in productivity than at a typical corporation.

Schmugar did note that college campuses tend to have more Mac users than the average enterprise, and, as a result, there is a larger population of systems that do not need to be checked for infection. However, even Mac users on campuses still suffer the campus-wide impact of congestion caused by spam generated from SoBig and others.

Said Schmugar: "If it takes down the network, it's going to affect you no matter what platform you use."

### What Else Is New?

But not all colleges and universities are struggling with these cyber catastrophes. When asked by The Mac Observer whether his school had been impacted by the summer's latest worms, Dominic Muruako, director of IT at Stillman College, said that the effects were minimal.

Why? Because Stillman College is one of the few institutes in the country that, with the exception of a few legacy servers, is an all-Mac school.

The University of Nebraska (UNL) apparently is slogging through the virus morass. Recently, The Mac Observer received from a source who wished to remain anonymous a copy of a note UNL sent to students with the subject line: "Another new computer virus--all UNL at risk". The e-mail's tone is alarmist from the get-go:

Is your computer completely protected yet? (Don't assume it is protected like the 45 Residence Hall students whose ports were de-activated just today!) -- UNLESS YOU HAVE SET YOUR ANTI-VIRUS SOFTWARE TO AUTOMATICALLY UPDATE DAILY, YOU ARE VULNERABLE..

According to the e-mail, Kent Hendrickson, associate vice chancellor in the information services department at University of Nebraska, approved the message, which warns students that, "if you fail to protect your computer and it affects the network, your computer port will be de-activated -- [and] you will be required to purchase a [US]\$50 certification package from ResNet and have your machine certified before your port will be reactivated."

In a terse e-mail interview, Mr. Hendrickson told The Mac Observer that the recent worms have caused downtime hours on its networks and that, at one point, the entire student body was kept off the network for 24 hours.

Hendrickson also said that "many" man-hours were needed to get the university's system up and running again and that spam generated from these e-mail worms slowed down the university's network, though he declined to specify the number of the man-hours needed or to what degree the resultant spam assault clogged the campus network.

### Mixed Environments

Dan Updegrave, vice president for information technology at the University of Texas in Austin, told The Mac Observer that of the 40,000 university-owned systems, approximately 60 to 70 percent are Windows, while 20 to 30 percent are Mac. He estimated that over 85 percent of the students own Windows-based PCs, with 10 percent owning Macs.

Because UT is such a large campus, multiple systems exist to handle online traffic. According to Updegrave, UT uses a wide range of [operating systems](#) for its many servers, including MVS, Sun Solaris, Windows, Linux, AIX, HP-UX, and Mac OS X Server.

While UT has not experienced any general network outages, Updegrave said some [servers](#) and client machines were either disabled or restricted from network access because of vulnerabilities to Blaster and related worms. In addition, students who did not properly patch their PCs had their network access curtailed, although he said the university does not as yet have good data on the number or duration of student machine restrictions.

"No doubt thousands of person-hours were required to install and test all the patches, install and update anti-virus software and firewalls, scan and block vulnerable systems, et al.," Updegrave said. "This is counting time spent by professional network, systems, and security

administrators as well as time spent by individual users on their UT and/or personally-owned systems."

Updegrave also said that UT experienced backlogs on e-mail servers caused by the vast number of inbound messages containing or generated by SoBig.F.

"Spam did not clog up networks, per se, but did result in delays in e-mail delivery until we installed filters," Updegrave said. "In a 13-day period, we filtered over 4.6 million rogue messages."

### Stillman Moves to Mac

Stillman College, a small liberal arts college based in Tuscaloosa, Alabama, is for all intents and purposes an all-Mac school. Although some of its e-mail and administrative services servers do not run the Mac platform, the college is progressively introducing Mac servers, IT director Muruako told The Mac Observer.

Back in 2001, Stillman College president Dr. Ernest McNealey, himself a Mac user, helmed an initiative to bring students greater access to technology at a reasonable cost. Bucking conventional wisdom, he believed that Macs were in fact more cost-efficient than PCs.

The school started the 2001-2002 school year with 200 Mac laptops and 1,400 Toshiba laptops, and "over that year we discovered a high rate of maintenance on the PC side as compared to the Mac side."

By the next year, the college, impressed with the Mac's security and reliability junked PCs entirely. Now all students carry iBooks, while professors carry PowerBooks.

The Blaster and SoBig.F attacks happened in tandem with Stillman's registration process, but students were not affected.

Said Muruako: "Compare that with 1,400 Toshibas deploying [during that time]. It could have been overwhelming for a campus of our size."

### Observer Comments

Show: [Subjects Only](#) | [Full Comments](#)

[Comment on this Article](#)

Show:   comments per page.

[Save Settings](#)

Guest Posts Hidden. [View Them.](#)

[Back to top](#) Page 1 of 1

[Log in](#) | [Register](#) | [Having Problems? Reset TMO Cookies & Try Again](#)

Username:  Password:  Log me on automatically each visit

You are not logged in, and this post will appear as "Guest." Log in with your username and password from the TMO forums. If you do not have a username, you can [register here](#). Please note that guests are limited to including a maximum of two URLs per post.

### Post A Comment

Subject

### Your Comments