CCSF Network Security. Notes from the January Board of Trustees Meeting

During the Public Comment period at the beginning of the January 26, 2012 Board of Trustees meeting, four of our colleagues with expertise in technology and network security responded to newspaper accounts about a significant security breach at City College. Edited portions of their comments and notes are given below, with their permission.

Please note that it is always advisable to take precautions to protect sensitive data, your computer, and other devices from security threats. Learning that newspaper articles may be inaccurate should not lead to complacency about network security. Information Technology Services is taking steps to double-check all computers in offices and labs. Coming soon – updated instructions for downloading and using antivirus software on personal computers.

Craig Persiko. Chair of the Computer Science Department. Member of the Information and Technology Policy Committee. Chair of the Technology Plan Revision Workgroup focusing on the Technology Division.

I and many of my colleagues on the committees listed above are concerned that the allegations of this virus attack are overblown. All of us on these committees (and all of the Technology Division staff) learned of this virus infestation in the SF Chronicle. Rather than working with the excellent professional and academic resources available here at CCSF, the Chief Technology Officer has been working only with USDN, Inc., an outside contractor.

A concerned faculty member found that USDN, Inc. is a "SUSPENDED" corporation in the state of California, according to the California Secretary of State, for failure to pay taxes or file information (http://kepler.sos.ca.gov/cbs.aspx).

I do not believe this virus threat warrants any more money being spent on outside contractors. I ask that the Chief Technology Officer be directed to share all findings and suggested solutions with the Technology Division staff and with the shared governance committees that are charged with ensuring the network security of the college.

Carol Reitan. Foreign Languages Department and Education Technology Department. Chair of the Technology Advisory Group (TAG for short), convened by the Chancellor to advise Dr. Hotchkiss on communicating with the wider campus community.

I want to tell you how shocked I was when I saw the articles in the SF Chronicle about the computer security situation at City College. Why should CCSF employees first learn about a possible problem with network security in the newspaper? Even our colleagues who work in Information Technology learned of this first in the newspaper.

Some of our main networking people have no access to the specifics of what USDN is doing or what was found by security monitoring. There has been no information available to the campus community, including Information Technology staff. The vendor, USDN, (who stands to profit from the situation) is the one telling us that we have a problem that they just happen to know how to fix. As a public institution, the college needs to avoid the appearance of any possible conflict of interest or impropriety. We need to make sure that the college acts responsibly and initiates a technical review of any report produced by USDN. Multiple Information Technology staff and Computer Networking and Information Technology faculty with the appropriate expertise must be involved.
Sam Bowne. Instructor, Computer Networking and Information Technology.

I have taught at CCSF for more than ten years. My field is computer networking and my specialty is network security. I am well-known in the computer security field: I am a Certified Ethical Hacker and an Associate of (ISC)^2, and I have given talks at Defcon, Toorcon, and many other industry conferences.

It was interesting to me that articles came out in the Chronicle and the CCSF Guardsman showing that there was some huge network security problem at CCSF. As far as I can tell this is completely false.

Within college channels, I cannot obtain any information about the problem. In the newspaper, I read that there were viruses on some computers in a student lab. Our precautions are up to industry standards, but they are not infallible. There is nothing surprising or newsworthy about a few infected student machines at the college. The correct response is to clean the infected machines, improve antivirus measures if possible, and continue with business as usual. This is not news.

The reason to hire computer security professionals is to detect problems and fix them so that there won’t be newspaper articles and public humiliation. We don’t have a computer security problem, we have a public relations problem, and a major one.

Carmen Lamha. Chair of Computer Networking and Information Technology. Member of the Technology Advisory Group.

I am concerned of the lack of accuracy of what I am reading in the newspapers. I am concerned that the experts in our department are not called on for help. We offer network security courses. Our faculty are experts who travel around the nation to speak on this topic at conferences. We have tools, including a contract for free McAfee to the CCSF community. Yet, we have not even been given information. I was embarrassed that Microsoft has called me to offer help and I have been given no clue as to what is going on. Please use us. Let us help ourselves as we have helped other institutions around the country.

--------------------------------

You may watch the Board of Trustees meeting or any of its parts by going to: http://www.ccsf.edu/NEW/en/about-city-college/board-of-trustees/board-live.html and clicking on video for the January 26, 2012 meeting. The left margin will shows and index of the parts of the meeting, choose III. Public Comment 10 minutes for the full remarks that are excerpted above.