Demsetz, Laura

From: Raznick, Eric
Sent: Tuesday, January 17, 2012 11:17 AM
To: All District Employees
Subject: SMCCD Network Update

You may have read about the recent data breach at City College of San Francisco and may have been wondering about the security of data at San Mateo. This message will give you a brief overview of our current network environment and how we are addressing network security.

The District maintains a high performance data network that connects the workstations and devices of the three college campuses and the District Office. The District Office works with companies such as AT&T and CENIC to provide fast, redundant, and reliable connectivity for each of the college campuses and to the Internet. Firewall appliances from Cisco are used to protect the District's network from unwanted traffic from outside networks. All buildings on campus have access to wireless networks for both public use and secure access to administrative services. Exinda appliances are in place between the College networks and the Internet to help prevent the illegal sharing of copyrighted material and to prevent the misuse of our network.

Securing College data is a high priority and a number of hardware and software tools are in place to protect the network and to detect and block unauthorized access. Here is a brief list of some of the tools that ITS uses to protect the network and our data:

- *Sophos Anti-Virus and Microsoft Forefront:* antivirus and malware detection and removal tools to protect all desktops and servers
- *Sophos Puremessage:* to detect and quarantine spam email messages
- *Snort:* to detect and control unauthorized network intrusion
- *Cisco Netflow*: to monitor and report on network connections
- *Exinda*: a packet-shaping appliance that blocks peer-to-peer services, like BitTorrent, and other services that can introduce malware and viruses
- *Microsoft Group Policies*: applied to District owned and managed PCs to protect them from malware, plug-ins that are malicious, file attacks, and to prevent students from installing software on PCs in the instructional computer labs
- *Public Wireless Network:* open to use by students and allows access to internet services; access to the public wireless network is automatically shut down from 11:00pm to 6:00am daily
- *Private Wireless Network:* a secure wireless network that requires authentication and provides access to services like Banner
- *OpenDNS:* to prevent faculty, staff and students who use our network from being redirected to known malicious web sites
- *WebSMART Passwords*: a modification was made to WebSMART to make passwords more secure by allowing passwords that can be up to 12 alphanumeric (*numbers and letters*) characters in length

As always, it takes all of us working together to keep our network secure. Continue to use good judgment when logging into websites and never share your passwords. If you receive an email that seems questionable you can always ask the ITS Helpdesk for assistance.

No network that allows access by the public can ever be 100% secure, but the District has taken many steps to make our network and private data as secure as possible.

--
Eric Raznick
Director, Information Technology Services
San Mateo Community College District
raznick@smccd.edu / 650.358.6703