

Thursday, January 25, 2007

Dear Faculty, Staff and Students,

As you may know, all of us will be required to change our Windows logon password in the next week or two. Faculty and staff will be forced to change it next Monday, January 29 and students must change their passwords on Monday, February 5. Jannette Corpus, the Information Security Officer, has sent out a series of messages to this effect and many of you have shared your concerns with us regarding this new policy. I'd like to address some of the questions that you personally may have regarding why it is necessary.

Q: Why do we need a new password policy?

A: We realize that this will be an inconvenience for everyone. However, there are a host of reasons why we must implement the new password policy.

If someone discovers your password through electronic means, guesses it or learns it by watching over your shoulder as you type it, they automatically gain access to a number of systems on CMA's network. These include PeopleSoft, Self Service and WebCT. In the near future, the Web server will be included in this list.

Social security numbers and other personal information for students, faculty and staff are contained in the PeopleSoft database (even though the SSN is not used as an identifier). Then, too, massive amounts of information can be copied very quickly or programs that log keystrokes can be installed using removable media such as USB flash drives by using your Windows credentials to log onto your computer. If confidential information is compromised, it may be very costly to the Academy and its reputation. None of us want the bad publicity and damaged trust that results from a security breach.

Both federal and state laws mandate ethical responsibility for personal and confidential data that we maintain for our students, faculty and staff. Strong passwords which are changed frequently are one aspect of protecting our data.

In addition to federal and state laws, the CSU system mandates a password policy and holds us accountable by performing security audits. The first question auditors ask is whether Cal Maritime has implemented a password policy.

Q: I don't have access to any sensitive, personal information. Why do I need to change my password?

A: Even if you don't have access to sensitive data, your computer or logon credentials can be used to launch an attack against one or more critical systems on the

Academy's network. The software to accomplish this is freely available on the Internet. These cracking programs encrypt lists of words from dictionaries and other sources and compare the encrypted results against the encrypted password(s) on the computer that is being attacked. When an encrypted word or phrase matches the encrypted password on the machine under attack, the perpetrator is able to determine the password.

If you feel for any reason that your password has been compromised (discovered by someone else), you should immediately change your password. Never share it with anyone—including IT staff members.

Q: Okay, but why do we have to change it every three months?

A: Time can be used against us or it can be our best ally. Any password is discoverable given enough time and computing resources. The more frequently passwords are changed (and the more complex the password), the less likely it is that the perpetrator will discover it.

Keyboard logging programs, when installed on a computer, can capture sensitive information. They run silently in the background and capture everything typed on the keyboard. Sensitive information, including passwords, can then be garnered and discretely forwarded to the perpetrator. The more frequently passwords are changed the less likely the perpetrator will be able to use the password to gain access.

Three months is an industry standard and has been widely adopted by universities around the world.

Q: How can I remember my passwords if I keep changing them?

A: Most of us are required to remember a variety of passwords to gain access to online shopping sites, electronic banking, personal and university-owned computers, web publishing, etc. It is important, however, that passwords not be written down (at least in a decipherable manner). Jannette has forwarded some email messages containing ideas on how to remember them. In addition, Information Technology's Help Desk has published brief articles which provide useful tips regarding how to remember passwords. The website at <http://www.csum.edu/IT/tipoftheweek.asp>. Also, please feel free to discuss ideas with any of the IT staff.

Q: Do I need to change my password for PeopleSoft and WebCT?

A: No. When you change your password, you will not be required to change it for PeopleSoft and WebCT. When you log into PeopleSoft or WebCT, it will authenticate using your new password.

Q: Can I change my password when I access my email from off campus?

A: We plan to enable this feature in the near future. If you are off campus when the password policy is implemented, you should continue to use your old password to access email until you come to campus, logon and are forced to change your password.

Q: What are the procedures to change my password?

A: On Monday, January 29 (for faculty and staff) or Monday, February 5 (for students), the system will prompt you to change your password as soon as you logon. The message box will state that “Your password has expired and must be changed.” Click OK. Then another box will appear that will ask you to enter your “old password” (the one you just used to logon), your “new password” and “confirm new password.” If your new password matches your confirmed new password and it meets the criteria for a strong password, you will see a message indicating that your new password has been changed.

Each of us can contribute to helping safeguard our institution’s confidential information. Like a chain, we are only as strong as the weakest link. Please do your part in this battle by using a strong password, keep them confidential and change them often! If you have any questions, please do not hesitate to contact either Jannette Corpus (jcorpus@csu.edu, x1725) or me.

Thanks!

Stephen L. Frazier

Chief Information Officer
California Maritime Academy
200 Maritime Academy Drive
Vallejo, CA 94590-8181
Voice: 707-654-1084
Fax: 707-654-1042

<http://www.csum.edu/>