**Announcement of upcoming Campus Phishing Exercise**

We are about to begin an on-going program of ethical phishing that will help all end users learn about the dangers of phishing attacks. Phishing is the phrase used to describe fake and often malicious emails used to place unwanted software on home computers and business computer networks allowing criminals and corporate data thieves to steal personal and corporate information. Emails are the easiest technique used to hack an employee’s computer, because if an employee clicks on a link, or opens an attachment, malicious code can attempt to be downloaded onto the computer without the employee realizing what has happened.

Ethical phishing is the practice of using hacker’s email techniques to educate rather than to infect an employee computer with malware or malicious software. The best way to educate employees in how to recognize and avoid fraudulent and malicious emails is to send employees similar looking emails to those used by hackers, but which explain how the end user could recognize the email as fraudulent should the end user click on a link or open an attachment or enter data as a result of receiving the email. It uses the same technique as hackers, but with instructional intent instead of malicious intent.

Ethical phishing education is not punitive, and individual results will not be shared. Think of it as a challenge, not a test. During the program, you may receive one or more simulated phishing emails per quarter that mimic the phishing emails that target our organization. The purpose of these emails is to give you hands-on experience with phishing emails and to allow you to improve your skills in spotting and avoiding these scams.

The phishing emails will be easy at first, and become harder and harder to detect over time. Everyone will fail to recognize one as a simulated malicious attack at one point or another – so relax, **and take the time to read the educational materials that appear if you get fooled**.

REMEMBER:

* If an email is not work related or seems suspicious, DELETE IT.
* If an email contains links which you do not regularly receive or use, DON’T CLICK.
* If you are unsure about an email, do not send it to others. Move it to your SPAM FOLDER and notify abuse@csusb.edu.
* If you have any questions or comments about this program, please contact: security-training@dsusb.edu or visit: <http://iso.csusb.edu/awareness>.