CyberSecurity News *"Top Ten"*

2012/2013 Volume 1, Issue 1

From the Office of Information Security

October is "National CyberSecurity Awareness Month." This year's theme is, "Our Shared Responsibility", which aims to expand on the importance for ***ALL*** Internet users to do their part in making the Internet safer. The following is a list of "top ten" items to help secure your information.

1. **CSUB Passwords:** Must not contain the user's account name or parts of the name that exceed two consecutive characters. Must be at least eight characters in length. Changed at least once per year and contain characters from three of the following four categories:
   A. Uppercase characters (A through Z)
   B. Lowercase characters (a through z)
   C. Numbers (0 through 9)
   D. Non-alphanumeric characters (for example: !, $, #, %)

   Systems incapable of enforcing compliant passwords shall have user enforced compliant passwords. If compliant passwords are not permitted then other mitigating controls, determined on a case by case basis, shall be user enforced; e.g. shorter password lifetimes, longer passwords, or inactivity screen locks. http://www.csub.edu/infosecurity/password.shtml

2. **CSUB External Devices:** Electronic media such as CD's, DVD's, Flash Drives, etc. shall not be used for the storage or transport of Level 1* confidential data, unless the data is encrypted or biometric security is employed at the device level. http://www.calstate.edu/icsuam/sections/8000/8065_FINAL_DRAFT_Data_Classification_CW_V4.pdf

3. **CSUB Portable devices** such as laptops, PDA's, cell phones, etc. shall not be used for the storage or transport of Level 1* data unless the data is encrypted.

4. **Phishing and Social Engineering:** Phishing is a tactic to obtain your personal information, such as credit card numbers, bank account numbers, social security numbers or other information. The tactic is to entice email recipients into clicking on a link or opening up an attachment, which is infected with malware. "Mouse over" the link to show the actual address in the status bar. Be cautious about all communications you receive, including those pretending to be from "trusted" sites.

5. **Online transactions:** *ONLY* shop at sites that you are familiar with and trust. Look for the "lock" symbol or "*HTTPS*" in the website address. *DO NOT* use a public computer or public WiFi for transactions.

6. **Updating your systems and software:** It is extremely important to keep your systems and software up-to-date. Restart your computer regularly or shut down your computer when not in use for an extended time. Set your application programs to "auto-update" to avoid missing critical updates. This includes the operating system, office programs, media players, Adobe programs, Browsers, Apps and any other programs.

7. **Protecting and securing your mobile devices:** With mobile technology and apps changing rapidly, it's *important* to secure and protect both the device and the information contained on the device. Use a strong sign-on password and limit your screen lock to a maximum length you can allow. Leave your Bluetooth *OFF* when it is not needed. Encrypt your information and device as well as any transmission when possible.

8. **Use anti-virus and anti-spyware programs:** Anti-virus programs stop your devices from performing slowly. Anti-virus and anti-spyware programs help to stop viruses, worms, and other malware. Avoid such things as popups, collecting personal information or changing the configurations of your device. Keep these programs to the most recent version and receive regular updates.

9. **Securing your home wireless networks:** Wireless networks are not as secure as the traditional "wired" networks. Minimize the risk by enabling WPA2 encryption and changing its' default passphrase, change the default administrator password, change the "SSID" and turn of its ability to broadcast, and enable "*HTTPS*" while performing initial administrative tasks.

10. **Personal information:** Make every effort to protect information that is confidential and personal. Individuals who access, store or transport protected information must use due diligence to prevent unauthorized access and disclosure of such information. Protect your information from theft, unauthorized use, and from others in listening distance.

For assistance, please call the Helpdesk at 654-2307.

Important links:

Confidential data classification:
http://www.calstate.edu/icsuam/sections/8000/8065_FINAL_DRAFT_Data_Classification_CW_V4.pdf

CSU Information Security Policies:
http://www.calstate.edu/icsuam/sections/8000/

CSUB Information Security:
http://www.csub.edu/infosecurity/