News reports in recent days have detailed the compromise of a reported 80 million social security records and other sensitive data from the health care insurance provider Anthem. In perspective, this means approximately 1 in 4 people in the U.S. are likely to be affected by this incident. It is likely that additional information and speculation as to the impact will be reported in the coming days and weeks. You may also receive direct information if you are or have been an Anthem customer. The Information Security Office (ISO) encourages everyone to continue with best practices in safeguarding your personal identity information and to consider whether additional steps are appropriate based on information you receive. Below you will find some information security practices that can help you reduce your personal risk.

We recognize that many staff members are or have been Anthem customers and may be at increased risk of phishing attacks. **Anthem has indicated that they will be contacting by USPS mail those who are impacted.** You may receive phishing email designed to appear to be from Anthem. This email is an attempt to lure you to an infected or fraudulent site masquerading as an Athem site or to install malware. Do not click on links in the email or provide your credit card and personal information to a website purporting to be from Anthem. Please forward any suspected phishing email sent to your Saclink account to the ISO abuse mailbox at abuse@csus.edu.

**Be wary of Phishing scams.**
Phishing is an ongoing problem and is not isolated to incidents like the Anthem breach. Therefore, the ISO team reminds you to stay vigilant.

**Continue to stay abreast of developments and reports so that you may assess your personal exposure, if any.** You can access up-to-date information on the Anthem breach by opening a browser and entering the URL: anthemfacts.com.

**Protect your web identity and online data.**
Change your password now and regularly at sites where you leave personal data, including banking institutions, Google, Yahoo, Facebook, Dropbox, Twitter, iCloud etc.

If you have further questions regarding the Anthem incident, please feel free to contact Information Security at iso@csus.edu.