National Cyber Security Awareness Month: "Our Shared Responsibility"
Sue Rivera

STORY: You logged into Facebook. You notice posts that you didn't create and your game tokens, gifts and credits are gone. Are you a victim of a hacker or online crime? Be glad it wasn't your bank account.

STOP: Before using the Internet, understand the risks and learn how to spot potential problems. Be cautious of who you trust and what information you provide. ***Avoid*** such things as:

- posting too much personal information on social networks (Facebook, Twitter or others), which make it easy for a hacker or criminal to use for stealing your identity, accessing your information and committing other crimes such as stalking. ***Once posted, always posted.***
- allowing those "need to have" apps on Facebook, Twitter type sites or your mobile device that share *your personal information*. Before you click on yes to an app, READ what information you are about to share.
- downloading attachments or clicking on links in unexpected email. When in doubt, call the sender or delete it. Links in email, tweets, posts and online advertising are some ways for criminals to compromise your device and steal your identity.
- clicking on a link within an email that you didn't expect. DON'T click! The sender address of the email may be disguised to fool you. Do you know for sure who sent the email and why? Did the email use your name? Call the sender first or go directly to their website by typing their address in your browser. http://www.hoax-slayer.com/phisher-scams.html#phishing-characteristics
- using unsecured WiFi or web addresses starting with *http* to perform banking transactions. DON'T allow websites to retain your credit card or personal information. Protect your money!

THINK: Take a moment to be certain the path ahead is clear. Consider how your online actions could impact your safety, device or your bank account. Watch for *warning signs* such as

- an advertisement offering free gifts, continual pop-ups, receiving unwelcomed messages, bullying or threats, or you are asked by someone to meet at a specific place and you don't know them. The person may be overly nice trying to earn your trust.
- you started downloading music, software or movies using BitTorrent. What you don't realize is that criminals also include malware or viruses that can infect your device and steal your personal information. Have you tried an alternative: "Grooveshark", "Last.fm" or "YouTube"?

CONNECT: Enjoy the Internet with greater confidence, knowing you've taken the right steps to safeguard yourself, your money, your family and your devices.

- Surf safely by remembering: **Stop, Think. Connect.**
- Look for our next article, "Protect Your Information" and what you can do to fight back.

For more information or to view this article: http://www.csub.edu/InfoSecurity/Security_Awareness.shtml .

Other helpful links:
Campus Downloading: Do it legally http://www.campusdownloading.com/
For everyone http://onguardonline.gov/
Homeland Security http://www.dhs.gov/national-cyber-security-awareness-month
National Cyber Security Alliance www.StaySafeOnline.org/NCSAM