National Cyber Security Awareness Month: "Protect Your Information and Fight-back"
By Sue Rivera

It's becoming routine to use your device or phone to tweet about your day, use Wi-Fi in most public places, or bank online. You may use your phone to pay for lunch. While it's nice to have device and phone convenience, navigating through settings for privacy protections can be challenging. It's important to know how to protect your information and fighting back when information is lost or stolen.

Facebook for example; have you ever posted too much information about yourself or tell everyone where you were going for the weekend only to be a victim of theft or stalking? Did the FB group you join oust your secret, all because the group owner chose "Open" or "Closed" instead of "Secret"?

* Reread the message before you post.
* Manage the account privacy settings. Remember, your friends can share your information or tag you in a photo they posted. You can remove the tag or ask your friend to delete the photo.
* Check out your account privacy settings for timeline and tagging. Read what you are sharing and select how you want to share that information.
* Look at the info accessible under account privacy settings for Apps and Websites. You can control the categories of information that people can bring with them.
* Leave the group http://www.facebook.com/help/174988392554409/#!/help/412300192139228/
*Stop. Think. Connect.

Have you ever received an email that begins with Dear Customer, your account has exceeded the storage limitation and you must click on the link immediately in order to keep your account active, or the email expressed that your helpdesk needs to change your password and to click on the link now to make the changes. These are common **scams** to get you to click on the link and then hackers try to use your information to steal your identity or your money. DON'T click the link. Delete the email.

Do you get on the Internet through public Wi-Fi or perform transactions through web addresses starting with ***http***? DO NOT perform transactions or provide confidential information while on these type of connections or websites.

*Use ***https*** which allows for a secured connection.
*Turn on your firewall and check your browser settings.
*Consider using a private virtual network.

As Facebook reaches 1 billion active users, your information is expanding world-wide almost immediately and the information may be located in other countries. If your personal information is stolen, or you are a victim of identity theft or fraud, try some suggestions below.

*Report it to your local law enforcement or University Police.
*Call a credit bureau: TransUnion, Experian or Equifax.
*Report it to the U.S. Department of Justice http://www.justice.gov/actioncenter/crime.html.
*Review ID Theft, Fraud, and Victim of Cybercrime: http://www.staysafeonline.org/stay-safe-online/protect-your-personal-information/id-theft-and-fraud.
*Talk to someone you trust.