May 2013

Use good password practices to protect your online identity!

As part of continuous efforts to increase SLU's information security posture, please be aware that it is everyone's responsibility to support the University's privacy and compliance efforts. Using good password practices is just one way we all must do our part. This means ensuring you change your SLU Net ID password every 180 days. (Notices for pending SLU Net ID password expirations are e-mailed at 21, 14, seven and one day(s) prior to the account being locked out.)

The explosion of passwords we need to remember on a daily basis has reached a point where it is difficult to remember any one of them, much less all of them. But it is important not to use your SLU password for any other accounts, such as your bank account, Facebook, or other personal e-mail account. If you use only one password for everything and it is compromised, it could take significant effort to clean up the problems caused by the criminals who stole your identity.

Good passwords are necessary to protect our accounts and to help us maintain our security and privacy. At SLU, passwords must follow these complexity rules:

- At least 8 characters long (The longer the better. We recommend using a sentence or phrase, complete with spaces. Example: The Quick Brown Fox jumped over 1 fence, TQBFjo1f.)
- At least 1 lowercase letter, 1 uppercase letter, and 1 number
- Cannot contain the following phrases: password, test, welcome, SLUNet ID, first name, last name
- Cannot contain the @ character
- Cannot contain single or double quote characters
- Cannot be a previously used password

If for some reason, you have not previously changed your password in the 180-day period, you are encouraged to go to password.slu.edu to update your password.

Here are a few tips for creating and using strong passwords:

- Use unique passwords for systems based on the type of service. For example, have a unique password for your online banking that is different than your SLU accounts.
- Use a strong password. Each website will have slightly different rules for creating a strong password and will likely differ from the SLU rules for creating passwords. Generally, longer passwords are stronger; these are also called passphrases.
- If you think your account or password has been compromised, you should change your password as soon as possible from a secure computer, or contact the website to notify it that your password has been compromised. For example, if you think your online banking password has been compromised, you may want to call or visit your bank and ask the banker to change your password right away. You should also ask if any suspicious transactions have occurred within your account.

None of these tips will help you remember passwords, but there is a service you may wish to consider:

- Use a securely configured password manager such as PasswordSafe on Windows or Keychain on Macs for managing your passwords. PasswordSafe and Keychain both allow users to set a master password and then securely store other passwords in the program on their computer. Users can enter any password and if they ever forget the password, they can check with PasswordSafe or Keychain to recover it. Built-in password managers within Web browsers should not be used because the security
of these tools generally is easily bypassed.

PasswordSafe can be downloaded free at: http://passwordsafe.sourceforge.net/index.shtml
Documentation on PasswordSafe may be found at: http://passwordsafe.sourceforge.net/index.shtml, Keychain is built into MacOS X and documentation may be found at: http://en.wikipedia.org/wiki/Keychain_(Mac_OS)
The use of such password retrieval tools is recommended for anyone who must use several passwords, and it will help assure accounts are not compromised.

For More Information:
http://www.consumer.ftc.gov/articles/0009-computer-security
http://www.onguardonline.gov/media/video-0081-computer-security