IT@UC
INFORMATION SECURITY

Personal Data Protection

Overview

Social media (Facebook, Twitter, LinkedIn, Pinterest, Google+, etc.) has become an integral part of our online lives. These sites are a great way to stay connected with others, but users should be wary about how much personal information they post. Hackers and malicious actors can use publicly available information obtained from social media platforms to create highly sophisticated attacks. Following these best practices will help limit exposure and increase the security of the user information.

Best Practices

- Use Strong passwords and change them regularly – Link
- Utilize two-factor authentication for online accounts whenever available – Link
- Activate all available privacy settings on social media sites – Link
- Refrain from posting information that identifies affiliations (law enforcement, military service, etc.), personal information, and carefully consider making comments on social media – Link
- Do not click on links in email or open attachments in unexpected messages, especially from unknown senders – Link
    - If you suspect any malicious activity or possible phishing attempts, please email abuse@uc.edu.
- Continuously monitor bank and credit activity for fraudulent activity - Link
- Request that real estate and property records be restricted from online searches - Link
- Perform annual online searches to identify what personal information is publically available - Link
- Review security settings on home computers and wireless networks - Link
- Password/PIN protect on all personal devices - Link
- Utilize encryption whenever available on devices such as phones, tablets, computers, etc. – Link
- Routinely update hardware and software applications, including antivirus, on devices - Link
- Create secure backups of all important files - Link
- Advise family and friends to utilize best practices