Tech Talks: 2-Factor Authentication (Apple/Android)

Explore your options for extra account security

2-Factor (Multi-Factor Authentication) - Security measure requiring a combination of two or more different forms of identifying evidence. Ideally, this means one thing you **know** and one thing you **have** (e.g. username/password and security key). 2-Factor is typically optional and enabled from your account settings. 2-Factor authentication options include:

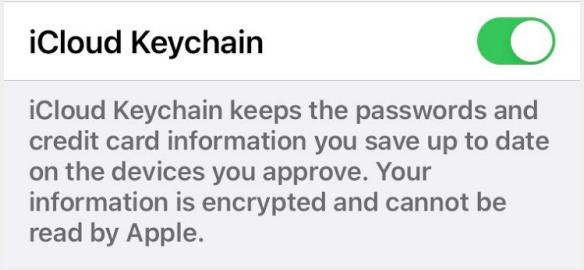
- **SMS** (Short Messaging Service) - Standard protocol for sharing alphabetic and numeric messages across different platforms and devices.
- **Push Notification** - Automated message sent from an application service that is delivered even when the user is not actively using the application
- **Security Key** (e.g. Thetis) - Small physical device that looks like a USB thumb drive and works in addition to your password on sites that support it.
- **Authenticator App** (e.g. Authy) - Free app that links to your account and generates temporary codes that are required for logging into that linked account.
- **Biometrics** (e.g. face scan) - Body measurements and calculations related to human characteristics that are used as a form of identification and access control.

Password Management

Apple

iCloud Keychain

Settings > Apple ID > iCloud > Keychain > On/Off



Settings > Passwords

Android

Google Password Manager

Google App > Manage your Google Account > Security > Signing in to other sites > Password Manager > Gear Icon > Offer to save passwords (Turn on) > Auto Sign-in (Turn on)

Settings > Privacy > Autofill service from Google > Use Autofill with Google (turn on)

SANTA CRUZ PUBLIC LIBRARIES

updated 02/25/2021