






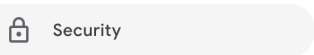

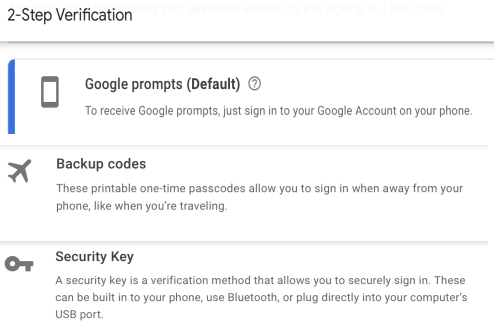
## Tech Talks: 2-Factor Authentication (Apple/Android)

*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. This means one thing you **know** and one thing you **have**.

<b>Text/Call</b> (e.g. 6-digit pin)	Many accounts require a registered phone number in order to complete the sign-in process by receiving a private pin code sent via SMS or read aloud through automated voice message.
<b>Push Notification</b> (e.g. Google Prompts)	Automated message sent to another already signed-in device that grants access to the new device.
<b>Authenticator App</b> (e.g. Google Authenticator)	Free app that links to your account and generates temporary codes that are required for logging into that linked account.
<b>Security Key</b> (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.
<b>Biometrics</b> (e.g. face scan)	Body measurements and calculations related to human characteristics that are used as a form of identification and access control.

### Setting up 2-Factor\* (Google Account Demo)

1		Download and Open a Google App (sign-in to Google account)
2		Tap circular profile icon (top right corner)
3		Tap "Manage your Google account"
4		Tap "Security" menu tab
5		Tap "2-Factor Verification" to turn ON
6		<p>Choose one (or more) options:</p> <ul style="list-style-type: none"><li>• Google prompts</li><li>• Backup codes</li><li>• Security key</li></ul> <p>* Please remember you are accepting responsibility for <b>having</b> your mobile device, backup codes or security key with you when access your account</p>