

Two-Factor Authentication Devices

Many accounts require a second factor (2FA) beyond the password — usually a code from a phone app or a physical key. Here's how to handle that.

Authenticator App

App Used	<i>[e.g., Google Authenticator, Authy, Microsoft Authenticator]</i>
On Which Device	<i>[e.g., Steve's iPhone, also on iPad]</i>
Backup Method	<i>[Does the app sync to cloud? Is there a backup device?]</i>

Physical Security Keys

Key Type	Location	Accounts It's Used For
<i>[e.g., YubiKey]</i>	<i>[e.g., On keychain, in safe]</i>	<i>[e.g., Google, GitHub, Bitwarden]</i>

<i>[Backup key]</i>	<i>[Location]</i>	<i>[Same accounts]</i>
---------------------	-------------------	------------------------

SMS / Phone-Based 2FA

[Which accounts use text message codes? These will go to Steve's phone — you'll need access to that phone number. See "Phone & Cell Plan" for how to transfer or access the number.]

How to Access Steve's Phone

Phone Model	<i>[Model]</i>
PIN / Passcode	<i>[Where to find it — e.g., password manager, written in safe]</i>
Biometric	<i>[Face ID / fingerprint — won't work for others, use PIN]</i>

If You Can't Get 2FA Codes

Most services have a recovery process. Look for "Recovery Codes" on the next page, or contact the service's support with a death certificate — most major services (Google, Apple, Microsoft, etc.) have a deceased user process.

