

2-Step Verification helps protect your account from unauthorized access. Even if your password is cracked, guessed, or otherwise stolen, an attacker can't sign in without a verification code.

Initially, verification codes are set up to be delivered to your mobile device via text message (SMS) or phone call, but there are other options available.

Important Note: Codes can only be used once and they do expire after a certain period of time.

Option # 1 SMS or Voice Call

- This choice is the best one for those who have a mobile device with a data plan.
- You can decide whether to have the code sent to your device via text message or a phone call.
- Phone call option does not work well with VideoPhones or Google Voice.

Option # 2 Google Authenticator App

- This choice is the best one for those who have a mobile device without a data plan.
- This choice is also good for those who prefer not to receive text messages or voice calls.
- Requires you to download and install an app on your mobile device.
- Works with Apple, Android and Blackberry devices.

Option # 3 Security Key

- This choice is best for those who do not own a mobile device.
- Instead of using verification codes, you insert your Security Key into your computer's USB port.
- Requires you to use a FIDO U2F Security Key.
- Requires you to log into your account on a computer that has an available USB port.
- Requires you to log into your account using only the Google Chrome web browser. (version 40 and up).

Option # 4 Backup Codes

- This choice is good for those who do not own a mobile device and access their account on just one computer.
- This choice is used as a backup option when your primary delivery method can't be used.