-->

Two-Step: Methods of Verification

Last Modified on 05/14/2026 4:32 pm EDT

There are many different ways to verify your identity using two-step verification - choose the one that's right for you! Your options may vary from service to service.

Faculty, Staff, and PhD Students

Contact your IT Support Representative for the best option to use with two-step verification.

Two-Step Methods: Key

Push Notifications - The best balance between security & convenience, just approve the push notification to sign-in!

Authenticator App - Use virtually any app available – this method generates a code every 30 seconds that you'll need to manually enter.

Physical Security Key - No need for a phone, just keep the FOB on your keychain for easy two-step verification on the go!

Voice or Text Message - The least secure form of two-step verification, receive a code via text or voice message. Make sure you have cell reception!

Two-Step Methods: Comparison

	Push Notifications (**Recommended**)	Authenticator App PennKey, Google[2]	Physical Security Key: PennKey	Physical Security Key: Google[2]	Voice or Text Message
Security Ranking (*e.g. #1 - most secure*)	#2	#2	#1	#1	#3
Usable w/o network?	✗	✓	✓	✓	✓
Usable w/o cellular?	✓	✓	✓	✓	✗
Usable w/o a phone?	✗	✗	✓	✓	✗

How to use	Approve a notification	1) Open an app 2) Copy & paste a code	Type in a 6-digit code	1) Plug-in via USB 2) Tap the key	1) Receive a text 2) Type in a code
Requirements	Duo Mobile Google Prompt[1, 2]	Authenticator app (*i.e. Duo Mobile*)	N/A	$40 purchase	N/A

[1] See the *Before You Start* section about push notifications in our Two-Step Verification (Google Accounts) article.
[2] If your Google account was created after December 2023, this option does not apply to you.

Questions?

For questions, please contact Wharton Computing Client Support Services