Two-Step: Best Practices & FAQ (Students)

Last Modified on 01/16/2024 10:45 am EST

Two-Step Verification can be a complex service to set up and manage, especially as you begin to enable it for your various accounts. Below are listed some best practices as well as some frequently asked questions regarding the service.

Enroll in Two-Step

Access requirements: Active PennKey & Google@Wharton accounts

Table of Contents

Choosing Your App(s)

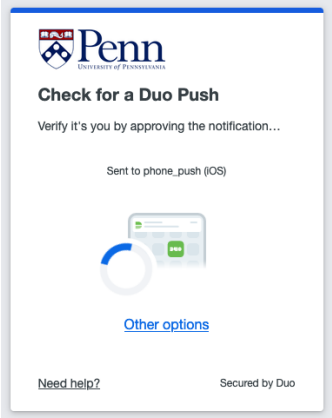
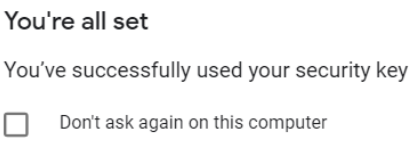
See our Two-Step: Methods of Verification article to determine which Two-Step method/app is best for you!

^Top

Trusting Browsers

Trusting or **saving** a browser means that the next time you log in, you won't be prompted for a two-step code.

Only trust a browser on personal devices that you use frequently. Trusting a browser on a public machine leaves you open to identity theft and hacking. **This includes the option "Don't ask again on this computer."**

PennKey	Google@Wharton
 Duration: 30 days Revocable via Two-Step Management	 Duration: Does not expire Recoverable via Account Management

^Top

Backup Options

You should always have a second or third way to authenticate with Two-Step, in the case that your primary device is unavailable. This ensures that you'll never be locked out of your account. By default, *Text or Voice Message* is configured during initial Two-Step setup.

> See our Two-Step: Account Recovery article for more information on supplementary ways to authenticate.

- **Backup Codes:**
  Backup codes are useful for when you don't have access to your primary Two-Step device. Having access to these codes will ensure that you always have access to your account.
  - *Pros*:
    - Always available
    - Can be stored in a personal account
    - No need for help from an Admin
  - *Cons*:
    - Limited-use
    - Must be stored in a secure & accessible location

- **Text or Voice Message:**
  - *Pros*:
    - Easy to setup

        - Can enter alternate phone numbers (i.e. family, friends, spouse, etc.)
    - *Cons*:
        - Must have cellular reception
        - Must be requested

^Top

Frequently Asked Questions

What are the different methods of verification that I can use?

Check out our Two-Step: Methods of Verification article!

What should I do if I don't get a push notification from DUO?

Open the app, tap on your account, and use the code provided.

Why is using push notifications better than receiving codes via SMS?

Receiving Two-Step codes via SMS is problemeatic for two reasons:

- you are required to have good cellular reception to receive the code. Push notifications don't require you to be connected to mobile data, you only need internet. This means that anywhere there's wifi, you can always get a code when you need one!
- codes sent via SMS can be compromised by man-in-the-middle attacks.

Can I use Two-Step without a network or mobile data connection?

Yes you can! Code generator apps, push notifications, and security keys all work without requiring a connection to the internet.

Can I use Two-Step without my phone?

Yes you can! You can use a Security Key, or a Hardware token, depending on which account you are logging into

Option	Description	Works With...
Security Key	• Purchase your own security key (e.g., YubiKey at Amazon, Yubico website) • Plugs into USB port on your device; click a button to authenticate. • Good backup option when traveling	• Google@Wharton [1] • PennKey • PennO365 • Others
Hardware Token	• Duo fob • SafeID fob (only previously registered) • Penn provides (Tech Center in Library)	• PennKey

[1] Google accounts created before December 2023

Questions?

Contact: Wharton Computing Student Support