Two-Step: Best Practices & FAQ (Students)

Last Modified on 04/19/2021 3:00 pm EDT

Two-Step Verification can be a complex service to setup 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

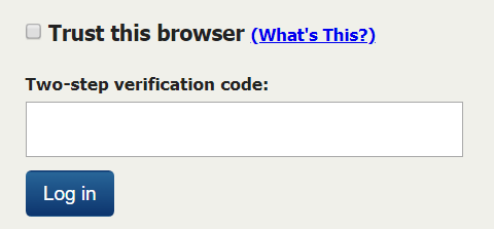
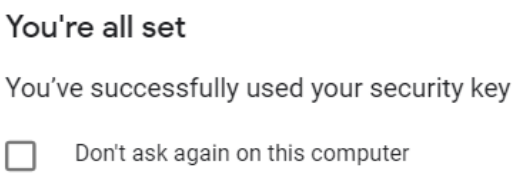
Access requirements: Active PennKey & Google@Wharton accounts

Which app should I use?

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

Trusting Browsers

"Trusting" or "saving" a browser means that the next time you login, you won't be prompted for a two-step code. **Only check this option on personal devices that you use frequently.**

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

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.

- **Backup Codes** (Google@Wharton; PennKey):
  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

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 bad for two reasons: **1)** you are required to have good cellular reception to receive the code, and **2)** codes sent via SMS can be compromised by man-in-the-middle attacks. Push notifications don't require you to be connected to the internet or to mobile data, this means you can always get a code when you need one!

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! For your Google@Wharton account, Google has support for security keys like the YubiKey -- you can find out more on Yubico's documentation. For Pennkey, ISC recommends that you use a SafeID keychain fob purchased from Computer Connection -- you can find out more at ISC's Two-Step FAQ article.

Questions?

Contact: Wharton Computing Student Support

Email: support@wharton.upenn.edu