

2-step Verification for Google Apps

Overview: This document is intended to walk you through the necessary steps to configure 2-step verification for your Union College Google Apps account, which includes Gmail, Google Drive, and other Google Apps for Education services. Two-step verification provides an additional layer of security to help prevent unauthorized access to your account.

IMPORTANT: Users who do not own cellphones or do not regularly carry one with you, please **DO NOT** enable 2-step verification at this time. ITS will provide further information for this situation in the near future.

Note: Voice and data charges from your cellular service provider may apply when 2-step verification is enabled. Please review your plan documentation and check with your service provider for further details.

Helpdesk contact information

Email: helpdesk@union.edu

Voice: 518-388-6400 or x6400

Let's get started!

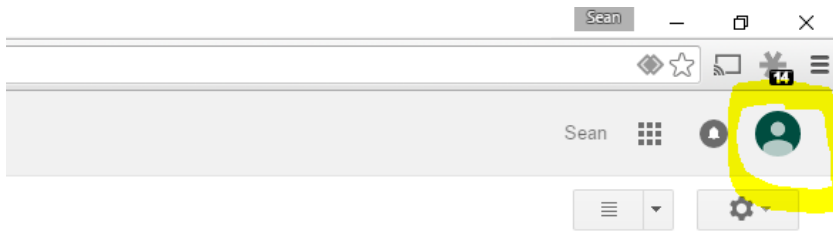
1. Sign into your Union College Google account with your Union credentials here: <https://accounts.google.com>

Note: You must be using a web browser to complete this process. If you are already logged into Union College mail in a web browser, please start at Step 2.

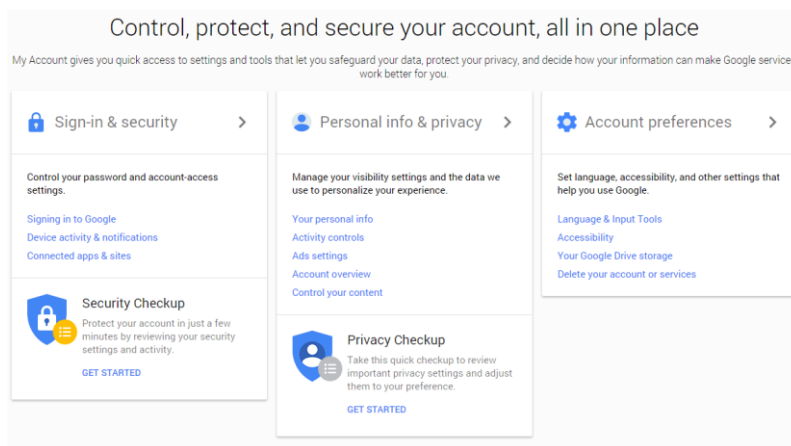
You may be prompted to add a recovery phone number if you have not set one up already for your Union College Google Apps for Education account. Please add your primary cell phone number using the guided prompts that Google provides.

2. If you are already logged into Union College mail in a web browser, please click your account icon in the top right hand corner of your email (highlighted in the circle pictured on the right).

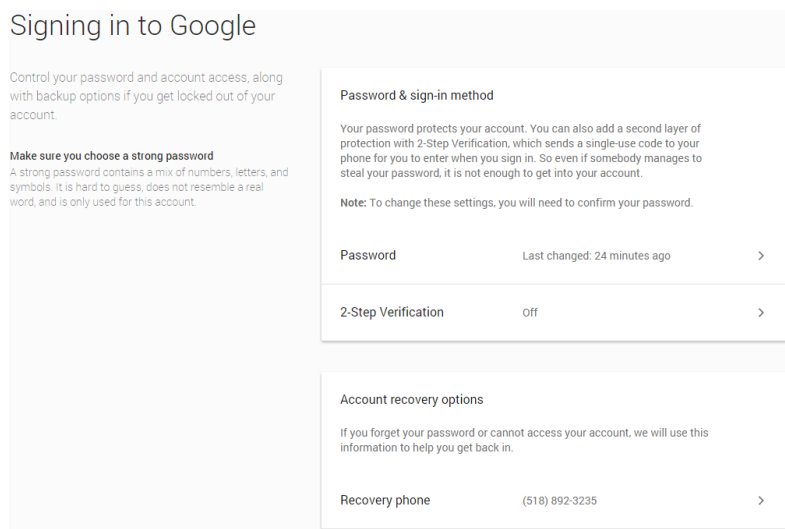
On the menu that appears, click the blue **My Account** button and proceed to step 3.



3. You should now see the page pictured to the right. Click **Signing in to Google** under the **Sign-in & Security** sub-section.



4. You will now see the page pictured to the right. Please click **2-step Verification**.



5. Review the information provided in the 2-step verification overview and then click **Start setup**.

Signing in with 2-step verification



Signing in will be different

You'll need verification codes: After entering your password, you'll enter a code that you'll get via text, voice call, or our mobile app.



Keep it simple

Once per computer, or every time: During sign in, you can tell us not to ask for a code again on that *particular* computer.



Help keep others out

You'll still be covered: We'll ask for codes when you (or anyone else) tries to sign in to your account from *other* computers.

2-step verification

Keep the bad guys out of your account by using both your password *and* your phone.

[Start setup »](#)

[Learn more](#)

6. You may be prompted for your password to confirm secure access.

If there is no prompt, please continue at step 7.

Please re-enter your password

First Middle Lastname
lastnam@union.edu

Password

Sign in

[Need help?](#)

[Sign in with a different account](#)

7. Enter your primary cell phone number and choose method of receiving codes (text message recommended). Then click **Send code**.

Set up your phone



Which phone should we send codes to?

Google will send a numeric code to your phone whenever you sign in from an untrusted computer or device.

Phone number ex: (201) 555-5555

- Google will only use this number for account security.
- Message and data rates may apply.

How should we send you codes?

- Text message (SMS)
- Voice Call

[« Back](#)

[Send code](#)


8. Look for a six-digit code to be sent to your cell phone.

There are occasionally delays in receiving text messages of at most a couple of minutes.

Verify your phone

1 — 2 — 3 — 4

We sent a text message to (518) 555-1212 with a code



Enter verification code

Verification codes are 6 digits long.

« Back Verify [Didn't get the code?](#)

9. You will be asked if you want to **Trust this computer**. This means you will not be prompted for a code for signing into any Google Apps for Education service for 30 days by the trusted computer.

You will still be prompted for codes to log into your account on any untrusted device.

Click **Next**.

CAUTION: Do not check the box to Trust this computer on any public or shared access computer or device!

Trust this computer?

1 — 2 — 3 — 4

Trusted computers only ask for verification codes once every 30 days.

If you lose your phone, you might be able to access your account from a trusted computer without needing a code. We recommend that you make this a trusted computer only if you trust the people who have access to it.

Trust this computer
You can always change which computers you trust in your Google Account settings.

« Back Next »

10. Click **Confirm** to save the 2-step verification settings that you have just configured.

Confirm

1 — 2 — 3 — 4

Turn on 2-step verification

You'll only be asked for a code whenever you sign in using your account every 30 days, on each trusted computer or device.

If you lose your phone, you can always change it in account settings.

The Google Apps SLA (Service Level Agreement) does not apply to any services that are used in connection with 2-step verification, if the verification process relies on third-party voice or data providers to deliver the verification code. Details of the agreement are available [here](#).

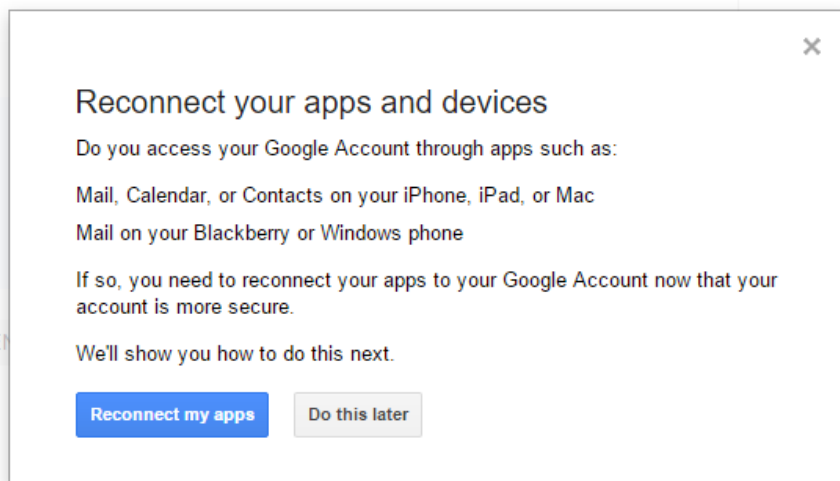
« Back Confirm

11. You may receive a prompt to **Reconnect your apps and devices.**

Click the button to **Do this later.**

Then click the **OK** button to confirm this choice.

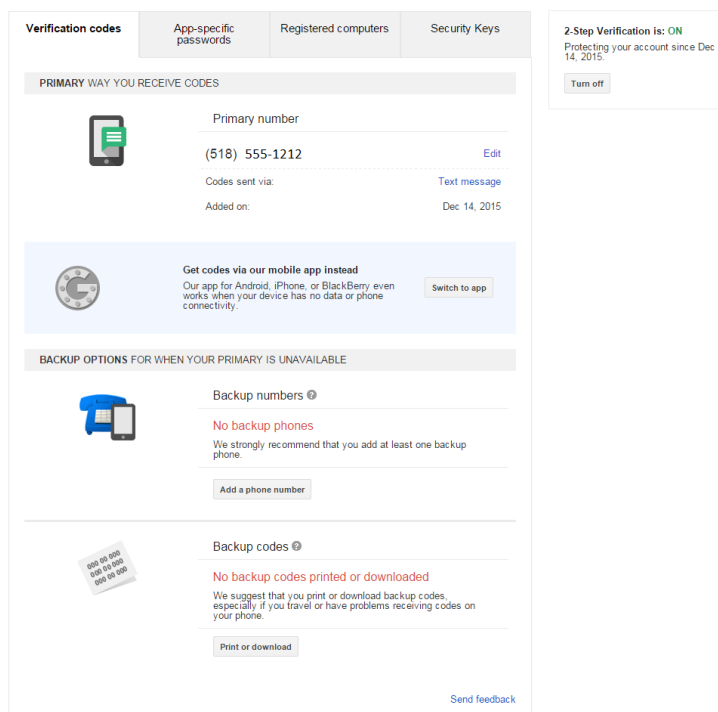
Note: Step 16 will provide further information with regard to reconnecting your apps.



12. You are now enrolled in 2-step verification and will be redirected to the 2-step verification configuration page.

You should take this opportunity to set up **BACKUP OPTIONS** to access your Google Apps for Education account in the event your cell phone is lost, stolen, or otherwise inaccessible.

2-Step Verification



13. Worried about not receiving codes? At the same settings page in step 15 you also have the opportunity to use an app on your phone to produce codes called Google Authenticator.

Instructions for setting this up can be found here:

<https://support.google.com/accounts/answer/1066447>

Install Google Authenticator

If you set up 2-Step Verification using SMS text message or Voice call and also want to be able to generate codes using the Android, iPhone, or a BlackBerry, you can use the Google Authenticator app to receive codes even if you don't have an Internet connection or mobile service.

To set this up, first you need to complete [SMS/Voice setup](#). Then, follow the directions for your type of device explained below.

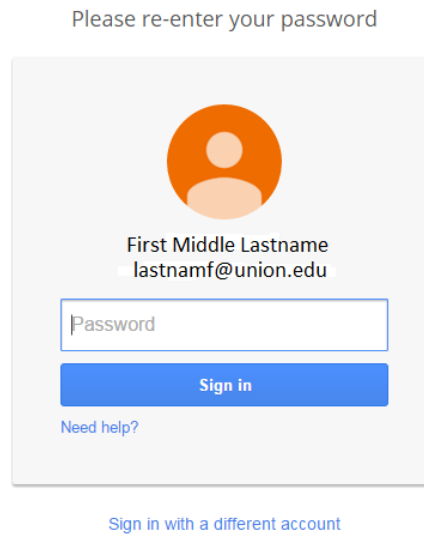
[Android devices](#)

[iPhone, iPod Touch, or iPad](#)

[BlackBerry devices](#)

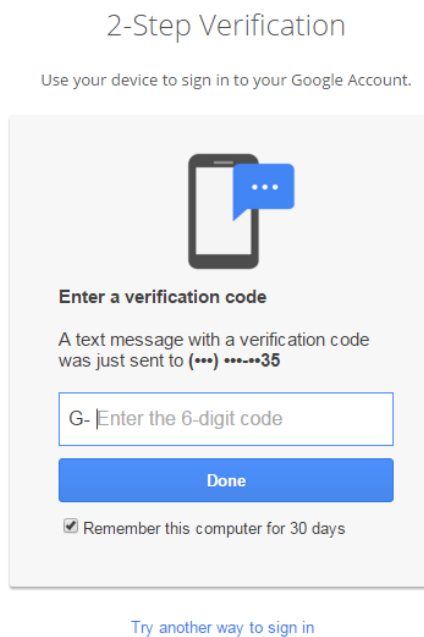
14. To begin using 2-step verification, sign out of your account, and then sign back in.

You will encounter your typical username and password prompt.



15. If you have not set the device you are logging in on as a trusted device, you will see prompt for a code, which you should look for on your cell phone.

Remember, if this is a public or shared device, you should uncheck the **Remember this computer for 30 days** checkbox to protect your account.



16. In some cases, you may be using applications that don't support the texted codes. They will need specific application codes configured.

If you are having trouble logging into this type of application on your computer, your tablet, or your phone, more information can be found here:

<https://support.google.com/accounts/answer/185833>

Sign in using App Passwords

An App password is a 16-digit passcode that gives an app or device permission to access your Google Account. If you use [2-Step-Verification](#) and are seeing a "password incorrect" error when trying to access your Google Account, an App password may solve the problem. Most of the time, you'll only have to enter an App password once per app or device, so don't worry about memorizing it.

Note: If you have iOS 8.3 on your iPhone or OSX 10.10.3 on your Mac, you will no longer have to use App passwords to use 2-Step Verification.

[Why you may need an App password](#) ▼

[How to generate an App password](#) ▼

[Forgot your App password](#) ▼

17. When you log in, you may be prompted again to set up backup methods to get codes.

CAUTION: This is optional, but please remember, if you do not have a valid code, you will not get into your account.

What if you lost your phone?

When you don't have access to (518) 555-1212, you'll need another way to get your code for 2-Step Verification. [?](#)


Add a backup phone number, so you don't get locked out of your account. [Learn more](#)



Provide a backup phone number

We'll only use this number for account security purposes.

Primary phone number: (518) 555-1212

Backup phone number:  (201) 555-5555

Receive codes via: Text message (SMS) Voice call

[Save number](#)

[Remind me later](#)