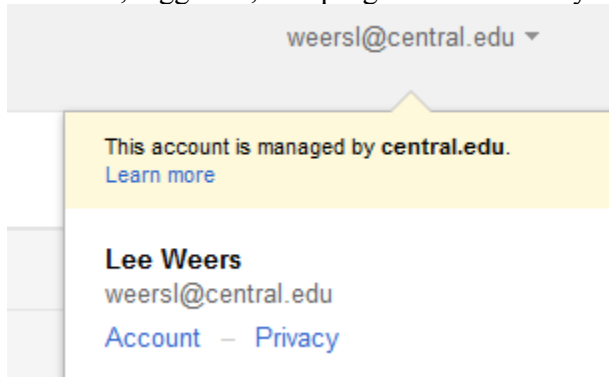


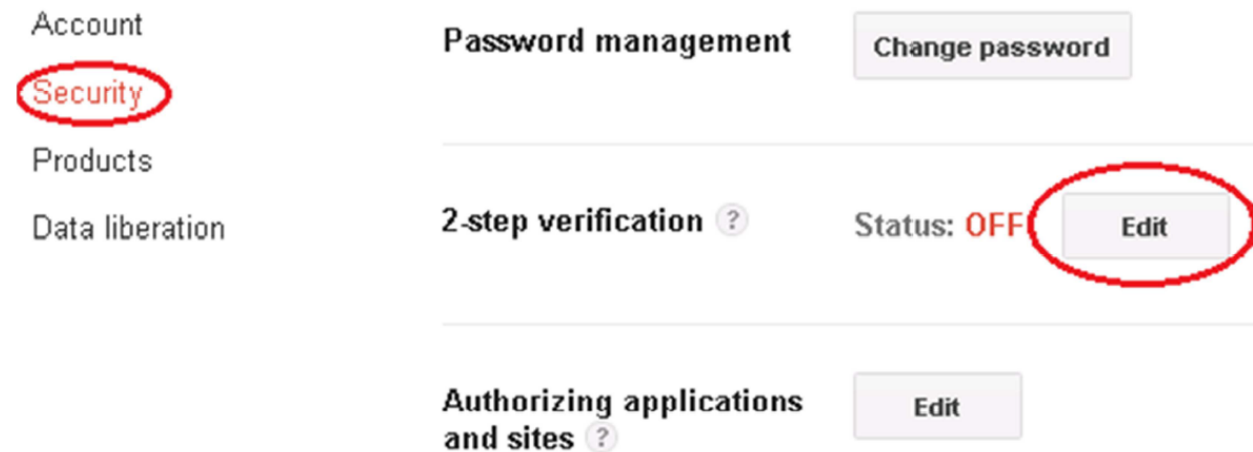
Google Mail & Your Phone

For Android Phones

1. On your computer, using any browser, log into the portal at: <https://my.central.edu>
2. Verify that the **Student Home** tab is selected
3. Login to your **Email** account found under **Cloud Services**
4. Once, logged in, in top right corner select your email address name and click on **Account**.



5. Select the **Security** Category. You are going to click on the **Edit** button to turn on 2-step verification. (middle row)



6. Click **Start setup**

How sign-in works with 2-step verification



Enter your password

Whenever you sign into Google you'll enter your username and password as usual.

Enter code from phone*

Next, you'll be asked for a code that will be sent to you via text, voice call, or our mobile app.

That's it, you're signed in!

Now your account has additional protection against hijackers.

**You can choose when we ask for a code, either every time you sign in or only when you sign in from a new device.*

7. Enter your **Phone number**. Please make sure to enter your mobile phone number that you intend to setup your Google mail.
8. Select the preference as to how Google can send your verification code.
Text Message or Voice Call.
9. Click **Send code**.

Set up your phone

1

2

3

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) 234-5678

• Google will only use this number for account security.

How should we send you codes?

- Text message (SMS)
- Voice Call

« Back

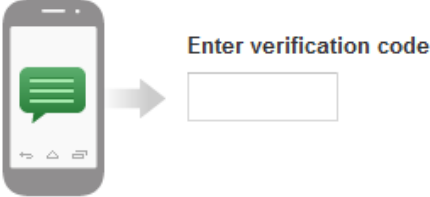
Send code

10. Enter the verification code from the text message or call from your phone
11. Click **Verify**

Verify your phone

1 — 2 — 3 — 4

We sent a text message to (641) 780-8560 with a code



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

12. Read the message regarding trusting your computer, and answer appropriately, do not answer yes if you are on a lab computer or a public computer.
13. Click **Next**

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.

14. Click **Confirm** to turn on the 2-step verification



Turn on 2-step verification

You'll only be asked for a code whenever you sign in using your **student@central.edu** 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](#).



15. Verification appears that 2-step verification is turned on

16. In the section, *Application-specific passwords*, click on **Manage application-specific passwords**.

Application-specific passwords

Some applications that access Google Accounts from a phone, desktop, or other devices (like mobile Gmail, desktop Picasa, or AdWords Editor) cannot ask for verification codes.

[Manage application-specific passwords](#)

To use these applications, you'll need to enter an application-specific password in the password field instead of your account password. [Learn more](#)

17. Enter an identifying word such as *Central Email* and click **Generate password**

Application-specific passwords

Some applications that work outside a browser aren't yet compatible with 2-step verification and cannot ask for verification codes:

- Apps on smartphones such as Android, BlackBerry or iPhone
- Mail clients such as Microsoft Outlook
- Chat clients such as Google Talk or AIM

To use these applications, you first need to **generate** an **application-specific password**. Next, **enter** that in the password field for each application that needs one. [Learn more](#)

[Watch the video on application-specific passwords](#)

Step 1 of 2: Generate new application-specific password

Enter a name to help you remember what application this is for:

Name:

ex: "Bob's Android", "Gmail on my iPhone", "GoogleTalk", "Outlook - home computer", "Thunderbird"

18. A one-time password appears. KEEP THIS SCREEN until complete

Application-specific passwords

Step 2 of 2: Enter the generated application-specific password
You may now enter your new application-specific password into your application.

Note that this password grants complete access to your Google Account. For security reasons, it will not be displayed again:

cozp luck zext qhvs

No need to memorize this password.
You should need to enter it only once. Spaces don't matter.

Done

19. This is the end of the computer portion of the setup process

On your Android phone

1. Go to **Settings – Accounts – Add Account – Select Google.**
2. Click **Next** button.
3. Where it says, “**Already have a Google Account?**”
4. Click **Sign in** button.
5. Enter your email address for your **username**: (i.e. username@central.edu)
6. Enter the one-time **password** that was provided to you from Google’s step 2 of application specific passwords.
7. Click **Sign in** and select types of features you would like to synchronize your mobile phone with
8. Google Apps and you are done.