

## Creating Gmail Account

### Why Gmail?

1. It protects your personal email and phone number from spammers/hackers because you are not posting your information on the web (webpage, Facebook, newsletters)
2. It protects your members from spammers/hackers because you do NOT store their emails in the account. But members and other organizations can contact you.
3. You use it as a connection to other applications:
  - a. MailChimp: Email program, requires an email to set up
  - b. Shutterfly: Historian photo scrapbook, webpage, requires an email to set up
  - c. Google Docs/Forms: membership form, surveys, collaboration
  - d. WordPress: TRTA webpage requires Gmail to setup and update
4. All these accounts can be passed to the next officers, do not need to reinvent the wheel.

- 1) Go to Google.com. Click on Gmail. Click on 'use another account'. Click on 'Create account'.
- 2) Use your local units name as the persons name, i.e. first-Arlington, last-RSEA.
- 3) Use your locals name as username, ie. ARSEA or ArlingtonRSEA.
- 4) Use a generic password, i.e. Arsea17, again something which can be passed along and/or used by several people. (Must have upper and lowercase letters, numbers, and a symbol)
- 5) The person who is going to be the main Admin for the account needs to put your own cell number and personal email as a backup contact. The admin on the account will have to verify and accept other user devices in order for them to be able to use the account. (See verification directions)
- 6) Birthday should be your Local Units Charter date. (If you don't know it use 1-1-2000)
- 7) Gender select Rather not say.
- 8) Verify your phone number if you put one in. Skip or accept video calls and ads.
- 9) You must agree to Privacy and Terms.
- 10) Go through set up steps.

\*\*\* Make a note of the month and date you set up the Gmail account. You need to know this to retrieve your password if you forget it, or you will use the recovery email or phone number you set up.

## Verifying a Google Account-Adding users device

You will get a security alert email that looks like this.

New device signed in to  
Then will list the gmail address

Your Google Account was just signed in to from a new Mac device. You're getting this email to make sure it was you.

CHECK ACTIVITY

When you click on 'check activity' it will look like this

### New sign-in on Mac



 pjse1959@gmail.com

Your account is at risk if this wasn't you



Mac  
Safari (Browser)

 Just now

 Near Arlington, TX, USA  
2600:1700:ca80:eb0:801d:b823:e572:1  
23e (IP address) 

Do you recognize this activity?

NO, SECURE ACCOUNT

YES

Click on Yes if you know who this is, otherwise they will be blocked from logging in and using the account.

## Changing Admin on a Google Account

Log in to the Gmail account.

\*\*\* It gives you the date the account was created. You will need to know this to recover the password if you forget it, or you can use your recovery email or phone number. Write them on your login sheet.

Click on the colored circle with a letter in it in the upper right corner and click on Manage your Google Account.

Click on 'Security' on left.

What you are going to change under 'Ways we can verify it's you'.

1. Recovery Email- click on recovery email, you will need to enter the account password.

Click on the 'Add recovery Email' if there was not one or click on the pencil if there was one to add or change the recovery email to the new admins email. Click on Done.

The new admin will now get the emails to verify new devices.

(The admin and new user will need to coordinate when the new device is added so the admin is available to do the verification. (See verification directions))

The new recovery email will get an email letting them know they are a recovery email.

Click the left arrow at the top in front of Recovery email to get back to the security page.

2. Recovery Phone-click on recovery phone, enter the account password. Click on the 'Add recovery Phone' if there was not one or click on the pencil if there was one to add or change the recovery phone to the new admins email. Click on Done or Update.

The new recovery phone will get a text letting them know they are a recovery phone.

Click the left arrow on the blue bar to get back to the security page.

3. Under 'Signing in to Google'

Do NOT change the password if there is more than 1 user on the account.

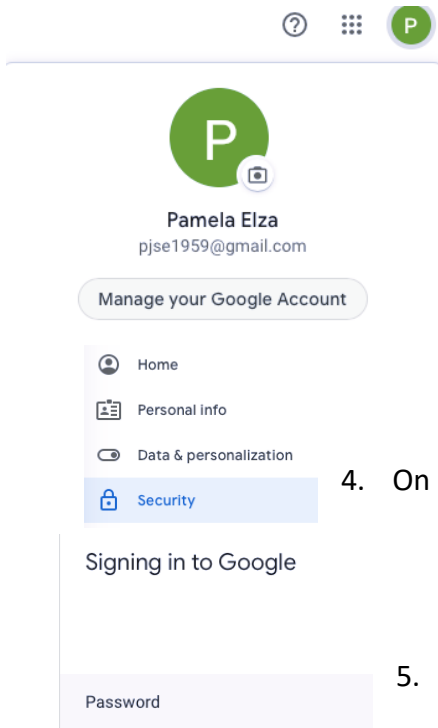
If you are passing the admin responsibilities on to a new admin and changed the password be sure to change the password to something generic so they can get started as the admin. 2-Step Verification is up to you.

4. Device activity & security events

You can review 'recent security events' and 'your devices' to see who has access to the account.

To remove a phone or tablet click on manage devices, then click on more details under the name of a device and click sign out.

## Resetting Gmail Password



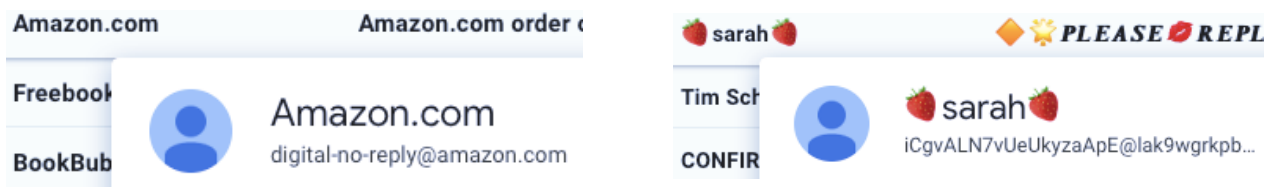
1. Open Gmail
2. In upper right corner click on the colored letter
3. Click on Manage your Google Account
4. On left side of window click on Security
5. In middle of window click on Password under Signing in to Google.
6. You will get a window asking you for your password again. Click on forgot password. It will ask for any past password. If you can't think of one or it doesn't work click on Try another way and follow any directions you are given.

You may be asked to go to a linked email or check your phone or answer a security question. If you can do whatever is asked successfully you will be allowed to reset your password.

Additional instructions here: <https://support.google.com/mail/answer/41078>

## Verifying for Spam In Gmail

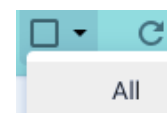
Hover your mouse over the sender name. The email address pops up. You can verify if it is legit.



Click in box in front of suspicious emails to get the check mark. Then you can click on the SPAM tool at top of emails.



In the spam folder again click in box at top left to get menu where you can click on ALL to put check mark in front of all emails.



Then click on **Delete forever** at top of emails.

Additional help: <https://www.mcafee.com/blogs/consumer/family-safety/7-ways-tell-fake/>