Resolving Compromised Gmail Accounts

NCAR Digital Presence Committee

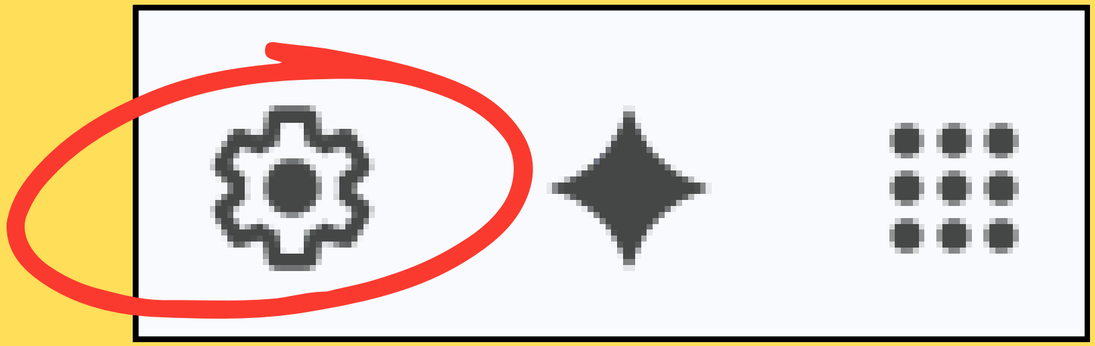
June 2026

If you received or know a chapter member who has received
or sent you an email with a suspicious invitation or subject matter,
it’s an indication that a Gmail account has been compromised.
Here are the steps to resolve it:

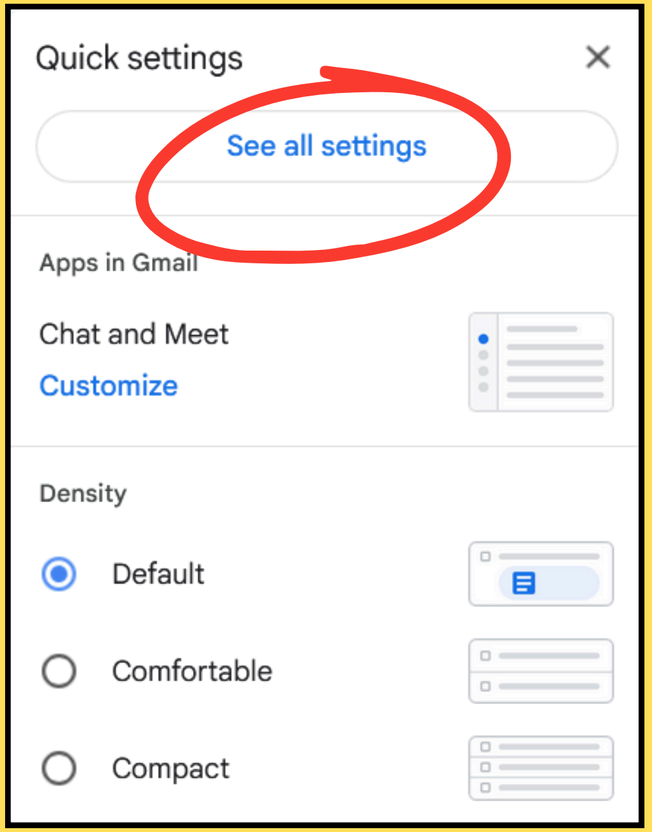
1. Filters
2. Forwards
3. Account Security/Devices
4. Check Drafts
5. Change Password
6. 2-Step Factor Authentication

ALL OF THESE STEPS NEED TO BE FOLLOWED

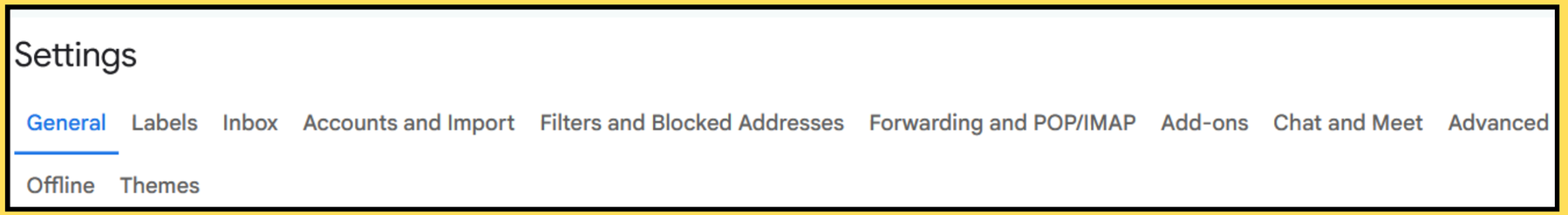
In your Gmail click on the gear icon for Settings

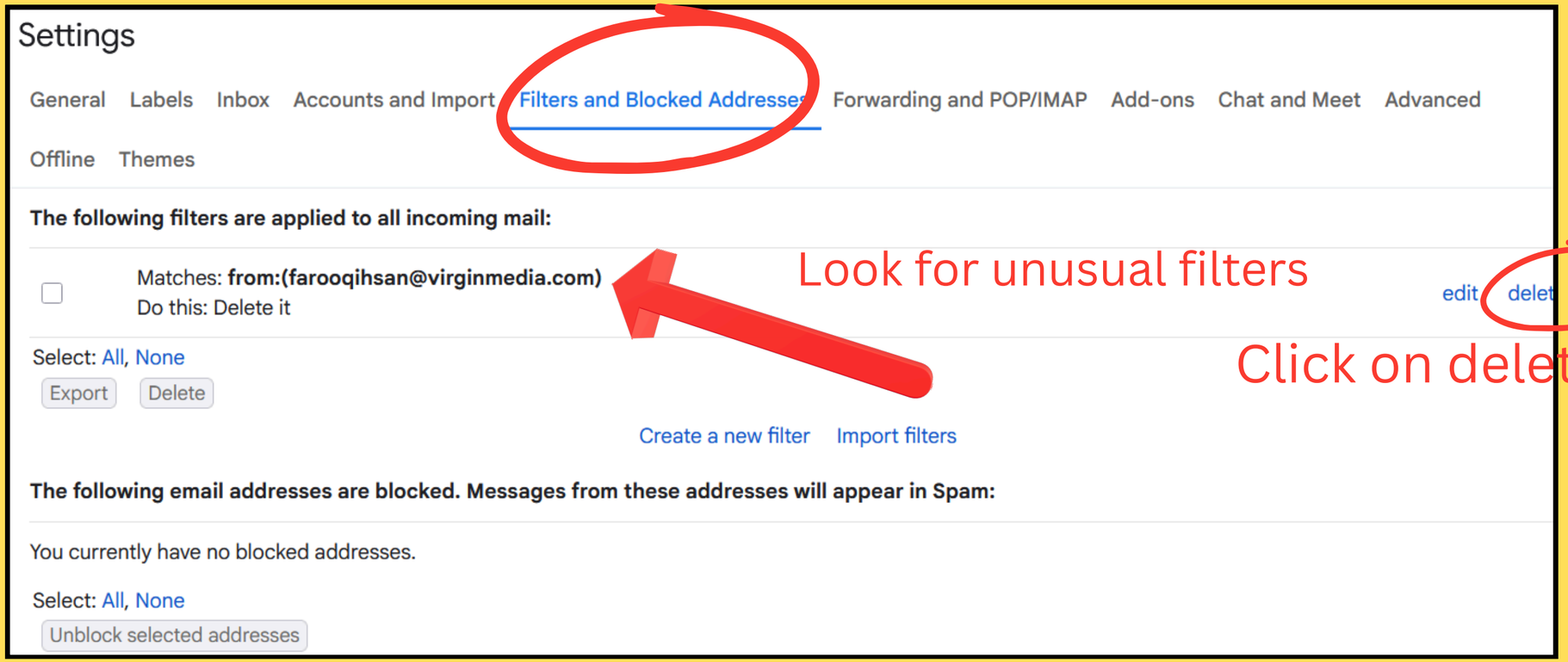


Click on “See all settings”

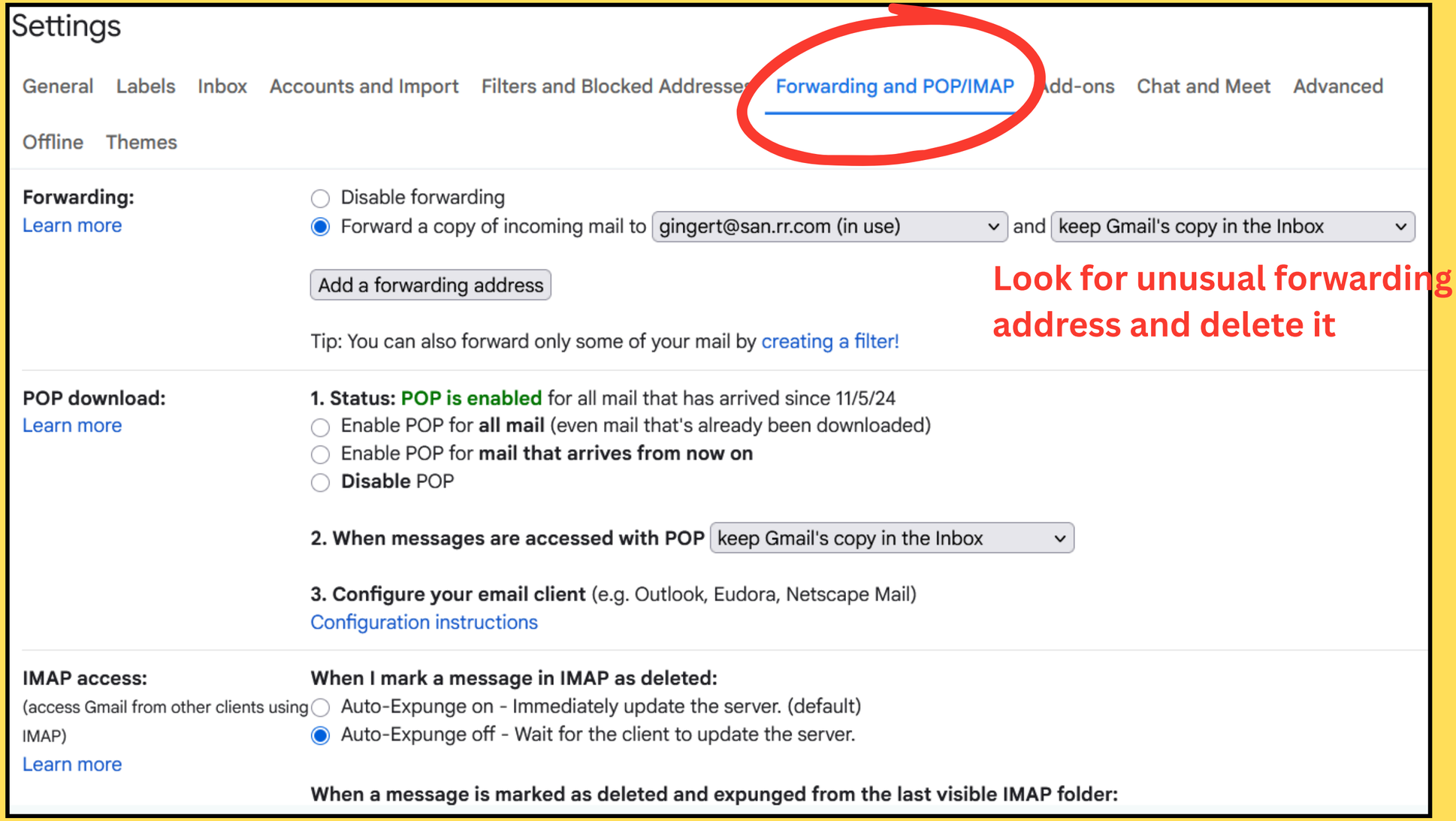


1. CHECK FILTERS



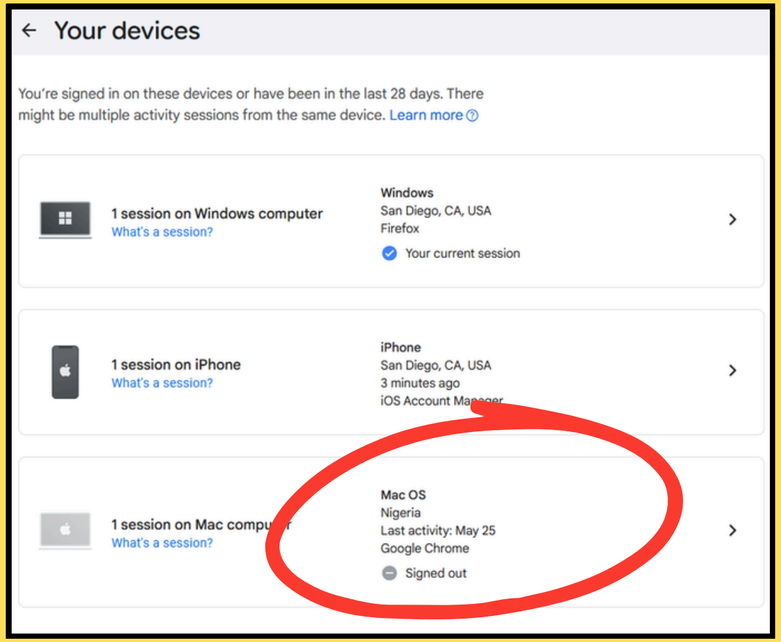


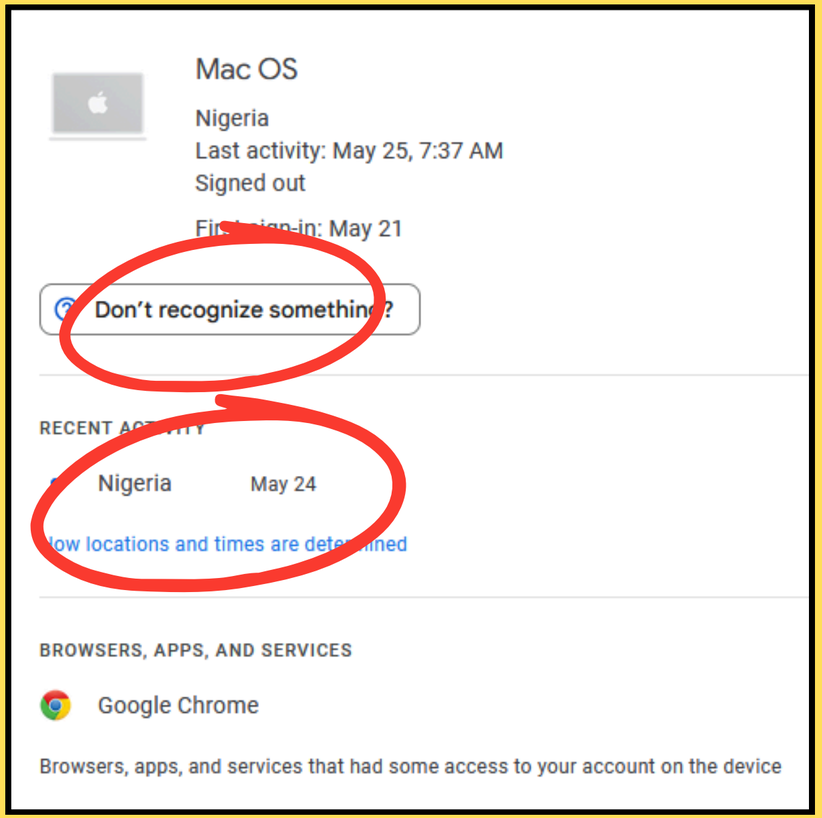
2. CHECK FORWARDING

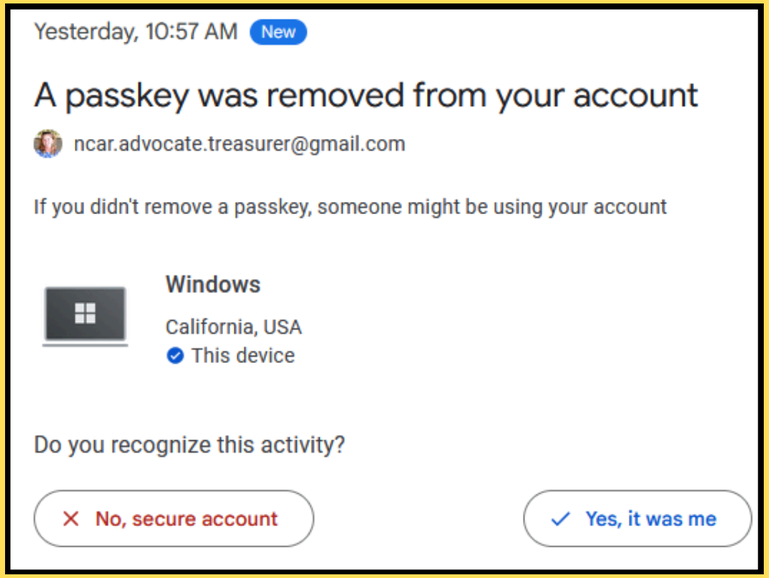


3. CHECK DEVICES

Go to your **Google Account Security Page**: myaccount.google.com/security.







Look for unusual activity

If you see *any* device or location you don't completely recognize (or an extra session of a browser you do use), click on it and select **Sign out**.

4. **Check your Drafts in your GMail for unusual activity**

5. & 6. CHANGE PASSWORD and USE 2-STEP VERIFICATION

Back on the main Security Page,
scroll to "How you sign-in to Google"
and change your **Password** to something entirely new and complex.

Make sure **2-Step Verification (2FA)** is turned on.
If it's already on, review your backup methods (like phone numbers or authenticator apps) to ensure the hacker didn't add their own phone number as a backup recovery option.