



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

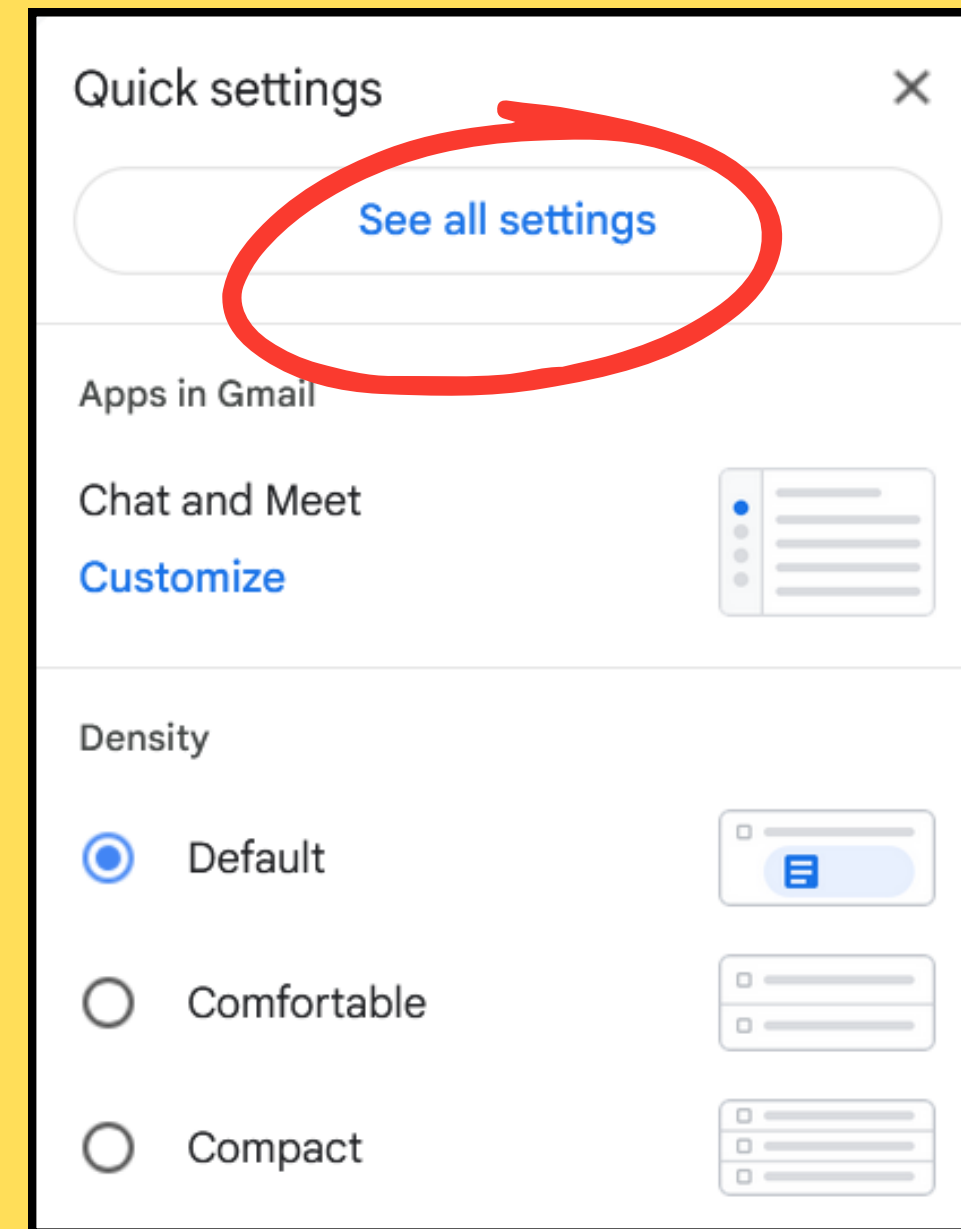


ALL OF THESE STEPS NEED TO BE FOLLOWED

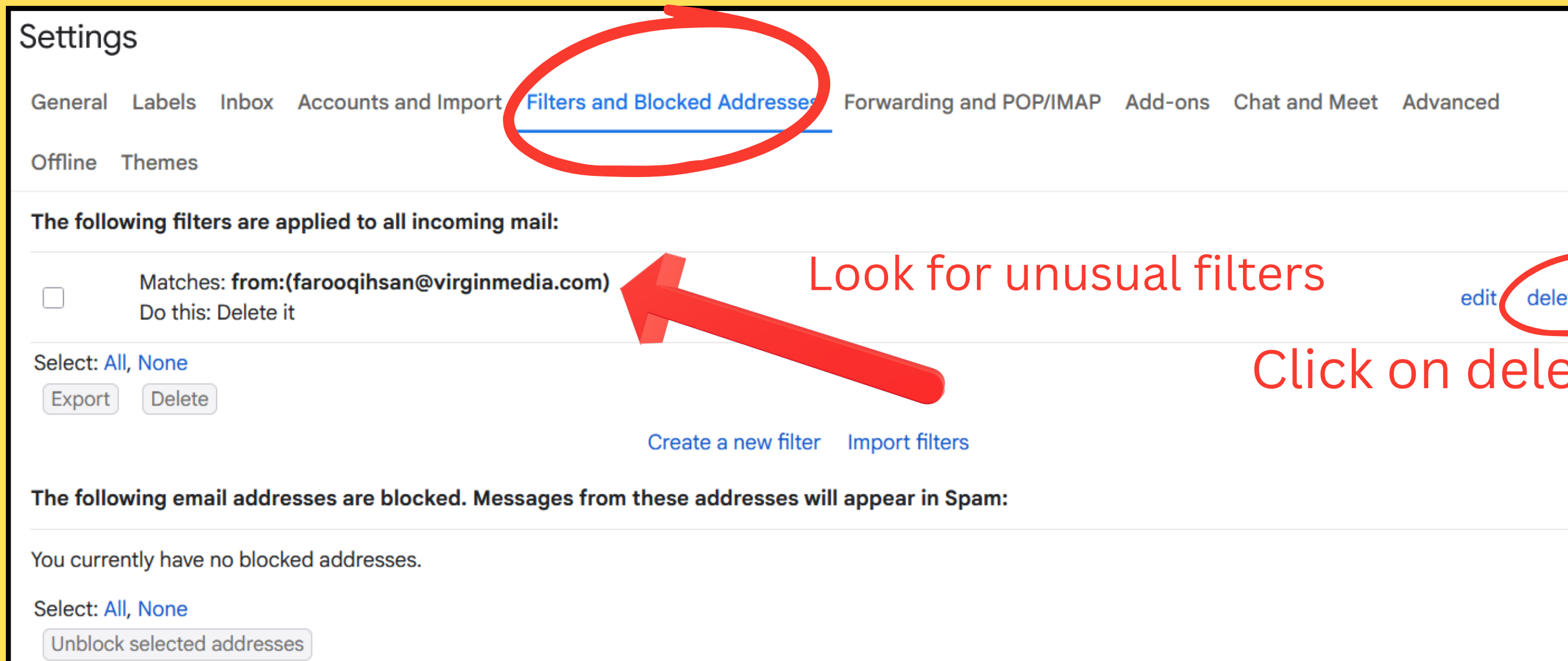
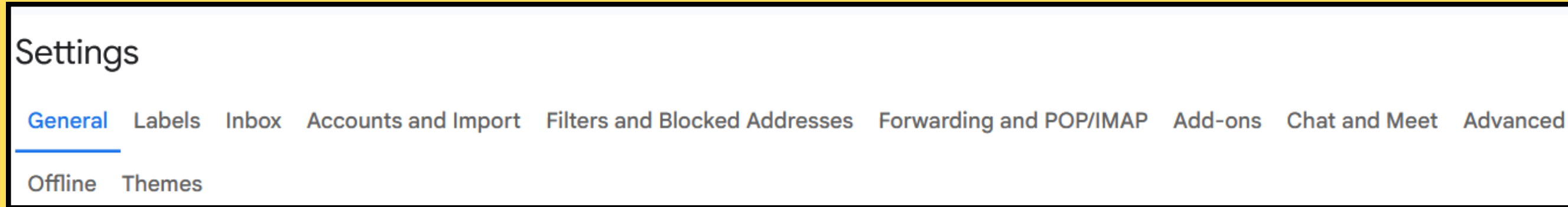
In your Gmail click on the gear icon for Settings



Click on “See all settings”



1. CHECK FILTERS



2. CHECK FORWARDING

Settings

[General](#) [Labels](#) [Inbox](#) [Accounts and Import](#) [Filters and Blocked Addresses](#) [Forwarding and POP/IMAP](#) [Add-ons](#) [Chat and Meet](#) [Advanced](#)

[Offline](#) [Themes](#)

Forwarding:
[Learn more](#)

☐ Disable forwarding

☒ Forward a copy of incoming mail to

gingert@san.rr.com (in use) ▾

 and

keep Gmail's copy in the Inbox ▾

Add a forwarding address

Tip: You can also forward only some of your mail by [creating a filter!](#)

POP download:
[Learn more](#)

1. Status: **POP is enabled** for all mail that has arrived since 11/5/24

☐ Enable POP for **all mail** (even mail that's already been downloaded)

☐ Enable POP for **mail that arrives from now on**

☐ **Disable POP**

2. When messages are accessed with POP

keep Gmail's copy in the Inbox ▾

3. **Configure your email client** (e.g. Outlook, Eudora, Netscape Mail)
[Configuration instructions](#)

IMAP access:
(access Gmail from other clients using IMAP)
[Learn more](#)

When I mark a message in IMAP as deleted:

☐ Auto-Expunge on - Immediately update the server. (default)

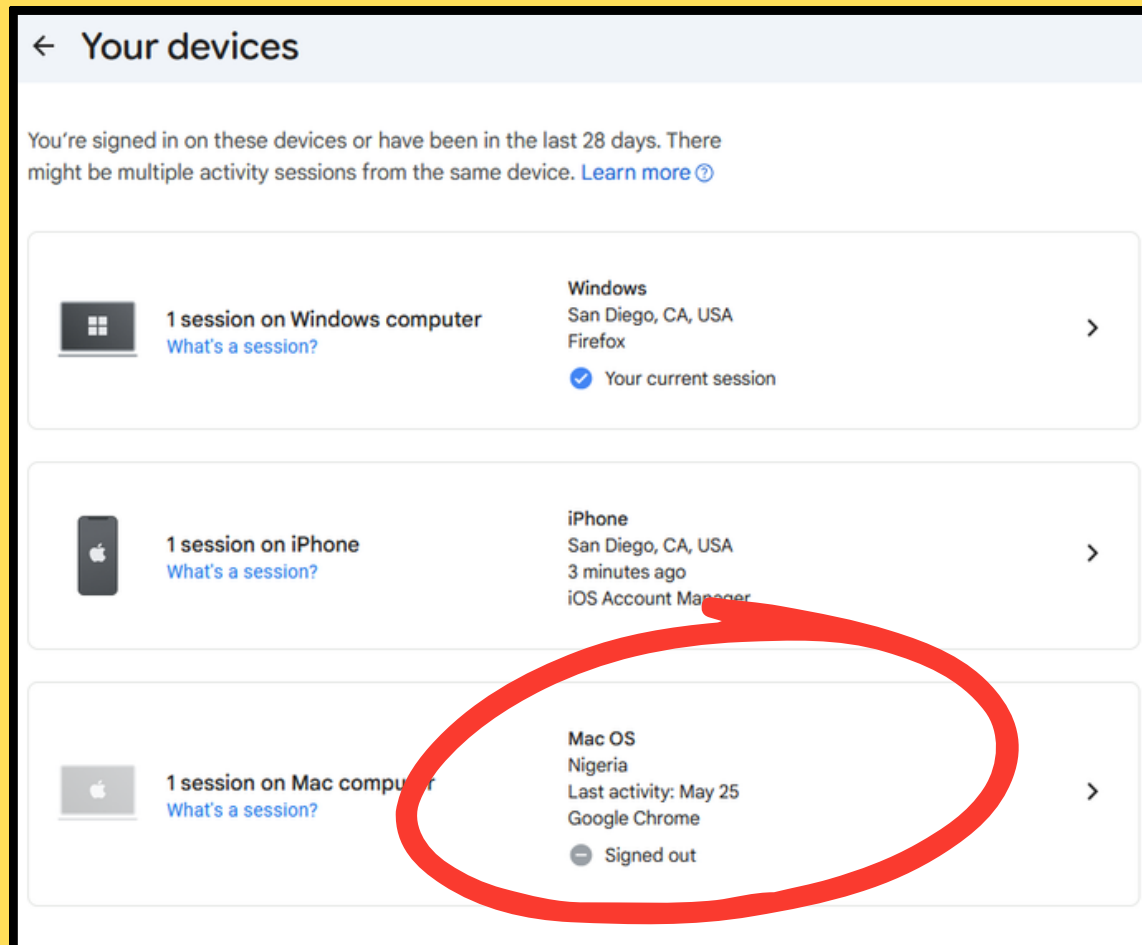
☒ Auto-Expunge off - Wait for the client to update the server.

When a message is marked as deleted and expunged from the last visible IMAP folder:

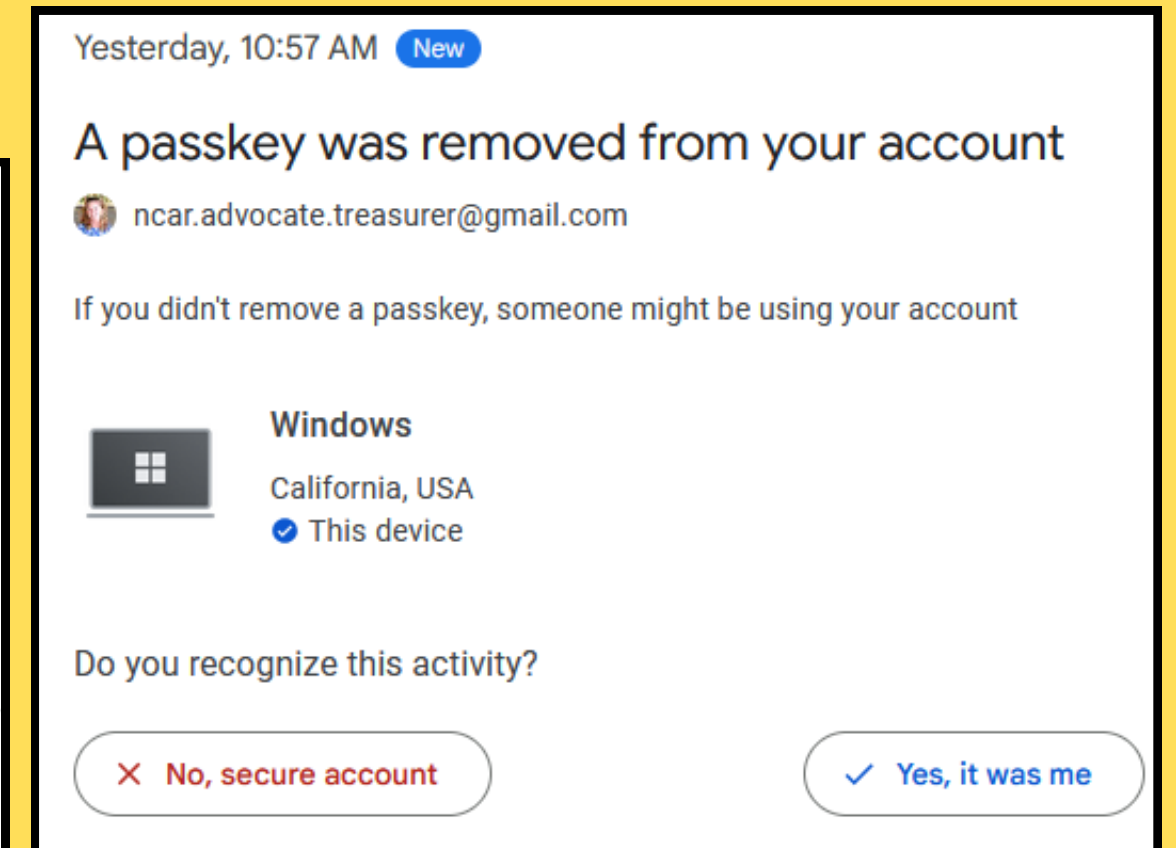
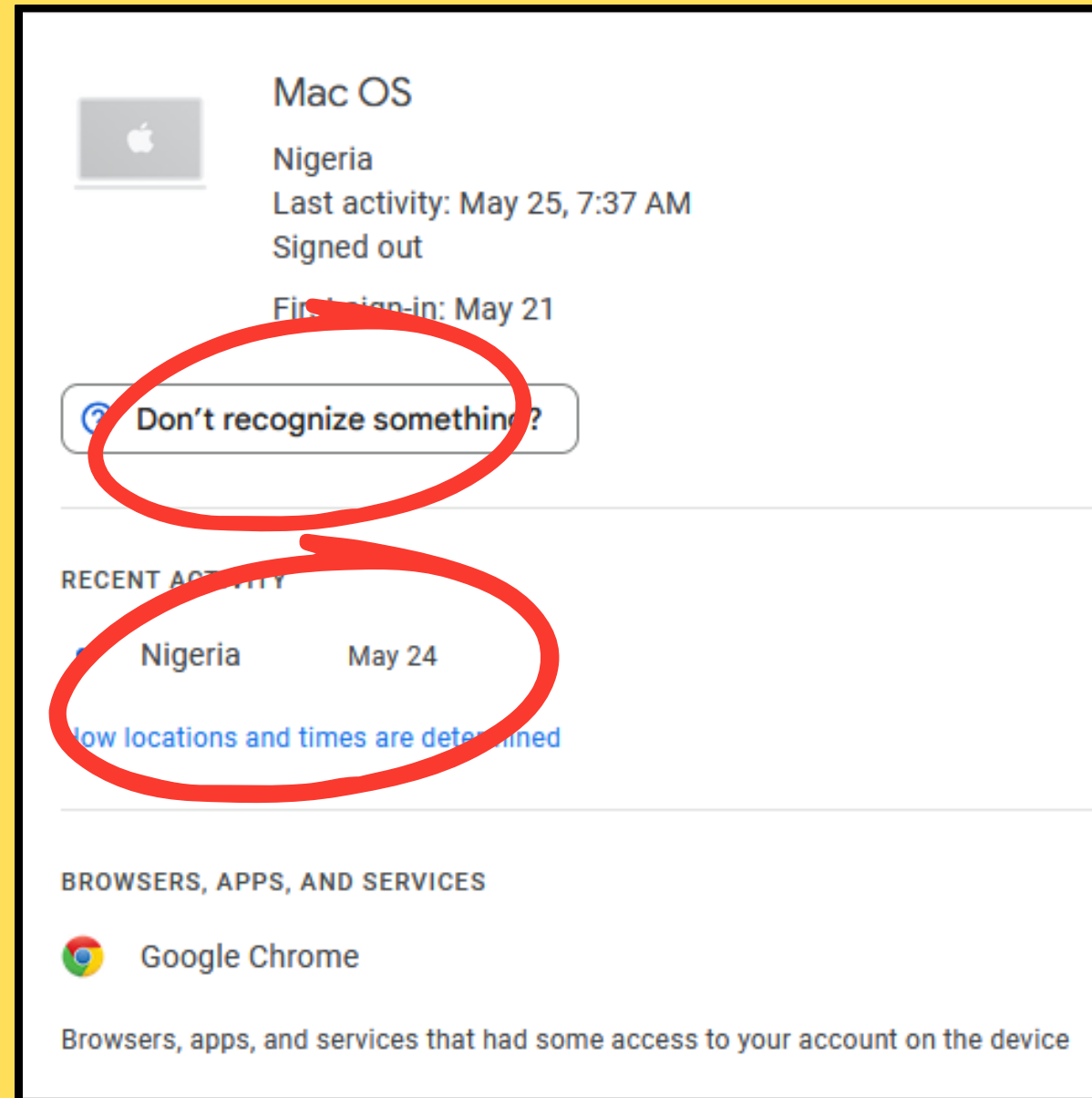
Look for unusual forwarding address and delete it

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.