Public

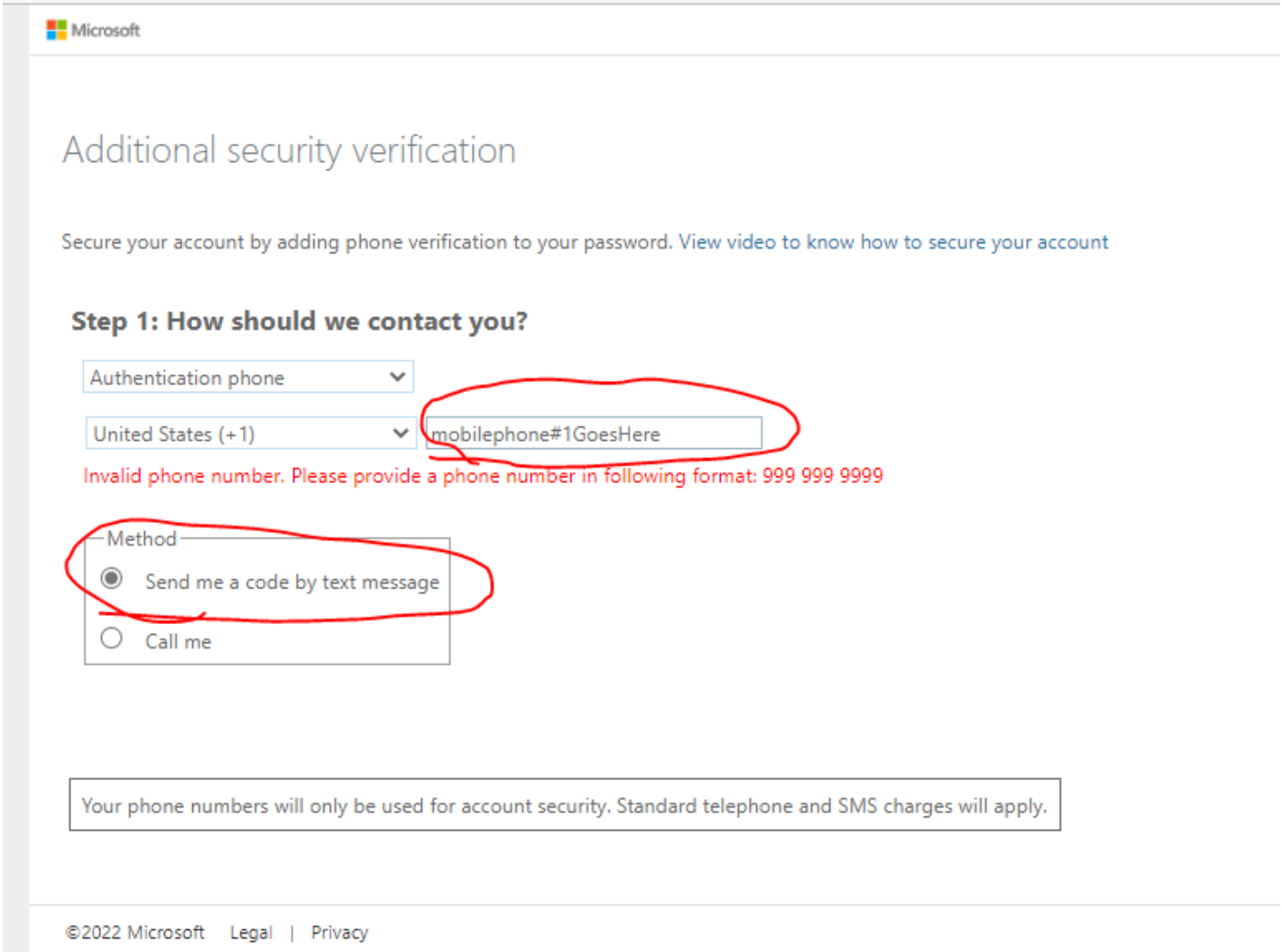
- Office 365 MFA User Setup
- Response to Compromised or Breach Email (in progress)
- Bulk Contact migration on iPhones

Office 365 MFA User Setup

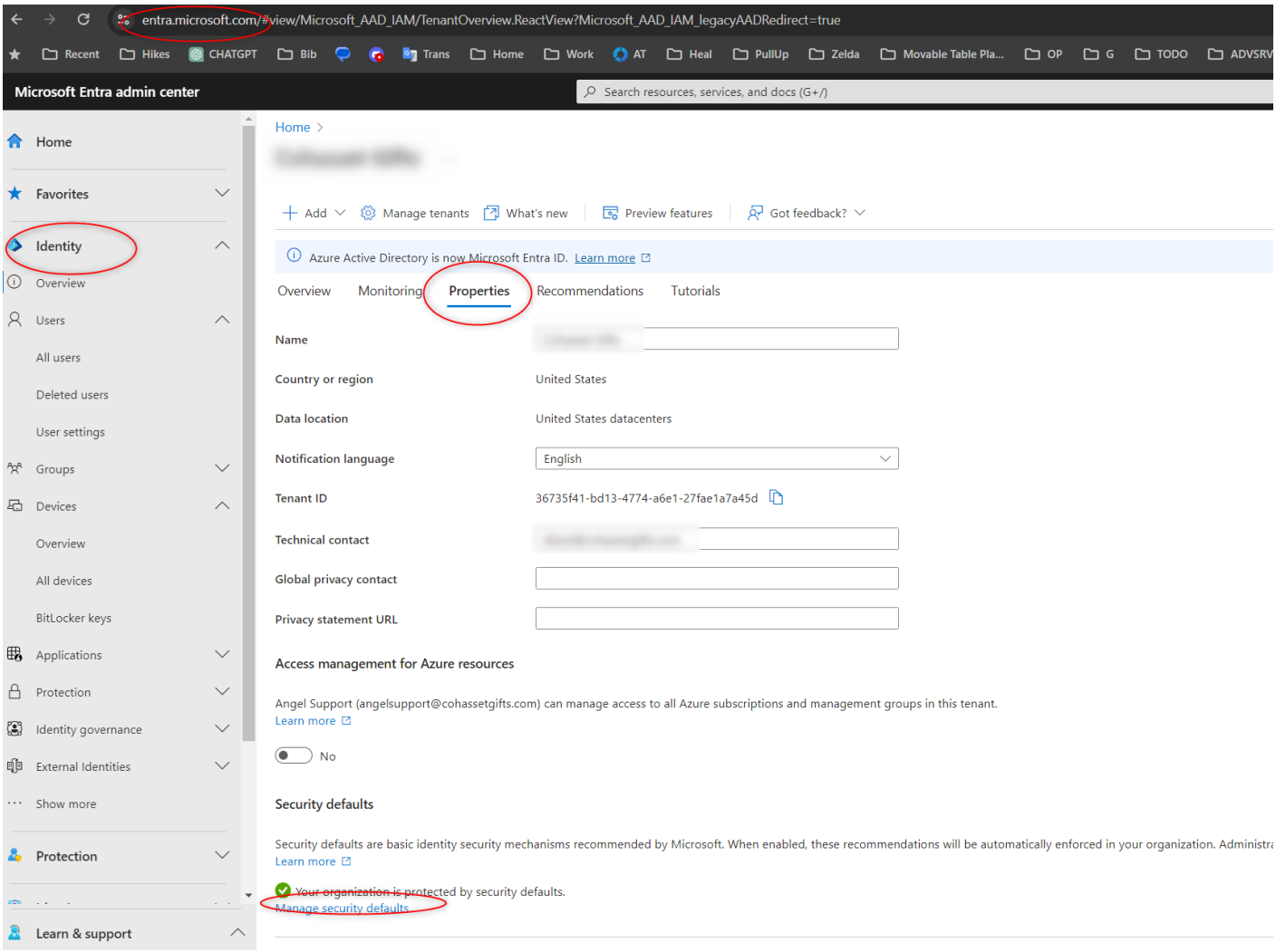
Summary: This article provides url for 2Factor,2FA,MFA,Microsoft,O365,Email,Prompt

https://aka.ms/mfasetup
Click Above
Sign in to your account
If multiple users use the email provided add more then one multiple factor authentication method
IE. Cell Phone for User1
Office Phone for User2
MultiFactor Authentication App like Authy, Microsoft Authenticator or other

> Note: If using Authy or something besides Microsoft you have to click "Use Verification Code" then select the link Configure app without notifications



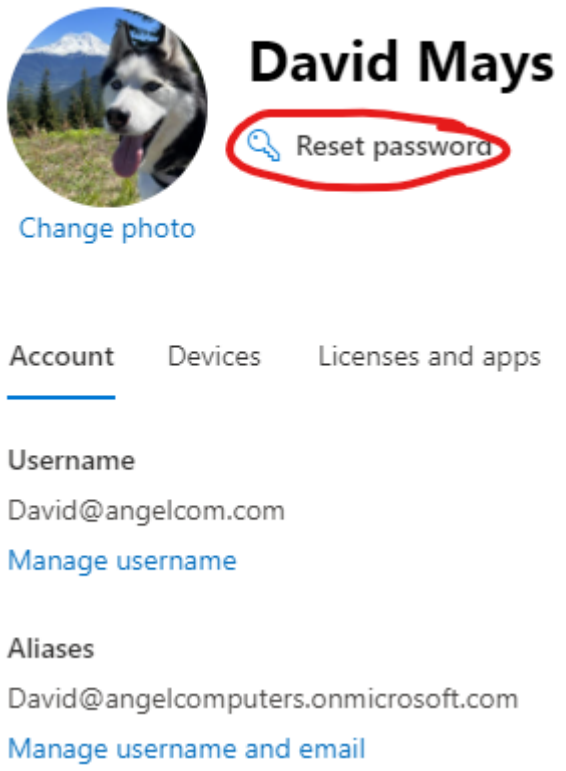
Turn on for everyone


entra.microsoft.com/#view/Microsoft_AAD_IAM/TenantOverview.ReactView?Microsoft_AAD_IAM_legacyAADRedirect=true
Recent
Hikes
CHATGPT
Bib
Trans
Home
Work
AT
Heal
PullUp
Zelda
Movable Table Pla...
OP
G
TODO
ADVSRV
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Home
Favorites
Identity
Overview
Users
All users
Deleted users
User settings
Groups
Devices
Overview
All devices
BitLocker keys
Applications
Protection
Identity governance
External Identities
Show more
Protection
Learn & support
Home
Add
Manage tenants
What's new
Preview features
Got feedback?
Azure Active Directory is now Microsoft Entra ID. Learn more
Overview
Monitoring
Properties
Recommendations
Tutorials
Name
Country or region
United States
Data location
United States datacenters
Notification language
English
Tenant ID
36735f41-bd13-4774-a6e1-27fae1a7a45d
Technical contact
Global privacy contact
Privacy statement URL
Access management for Azure resources
Angel Support (angelsupport@cohassetgifts.com) can manage access to all Azure subscriptions and management groups in this tenant.
Learn more
No
Security defaults
Security defaults are basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will be automatically enforced in your organization. Administra
Learn more
Your organization is protected by security defaults.
Manage security defaults

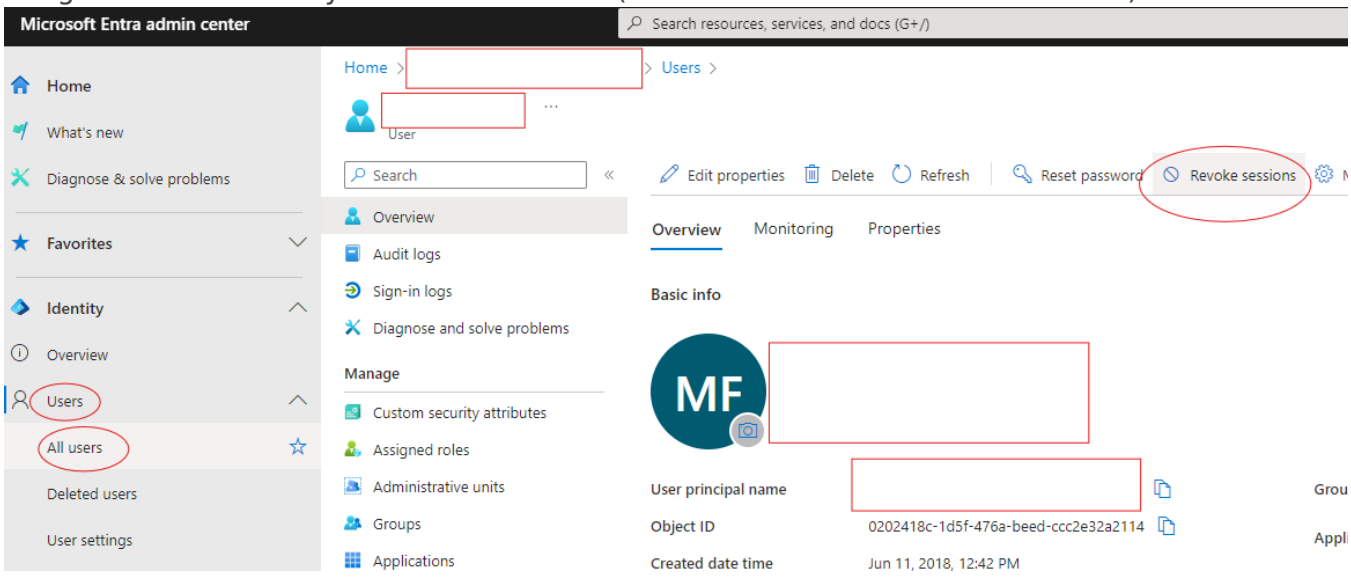
Response to Compromised or Breach Email (in progress)

If a user has their email and/or password compromised, please follow the instructions below as quickly as possible to secure the account.

1. Reset User Password in the Office 365 admin page, Admin Portal Users>Active Users

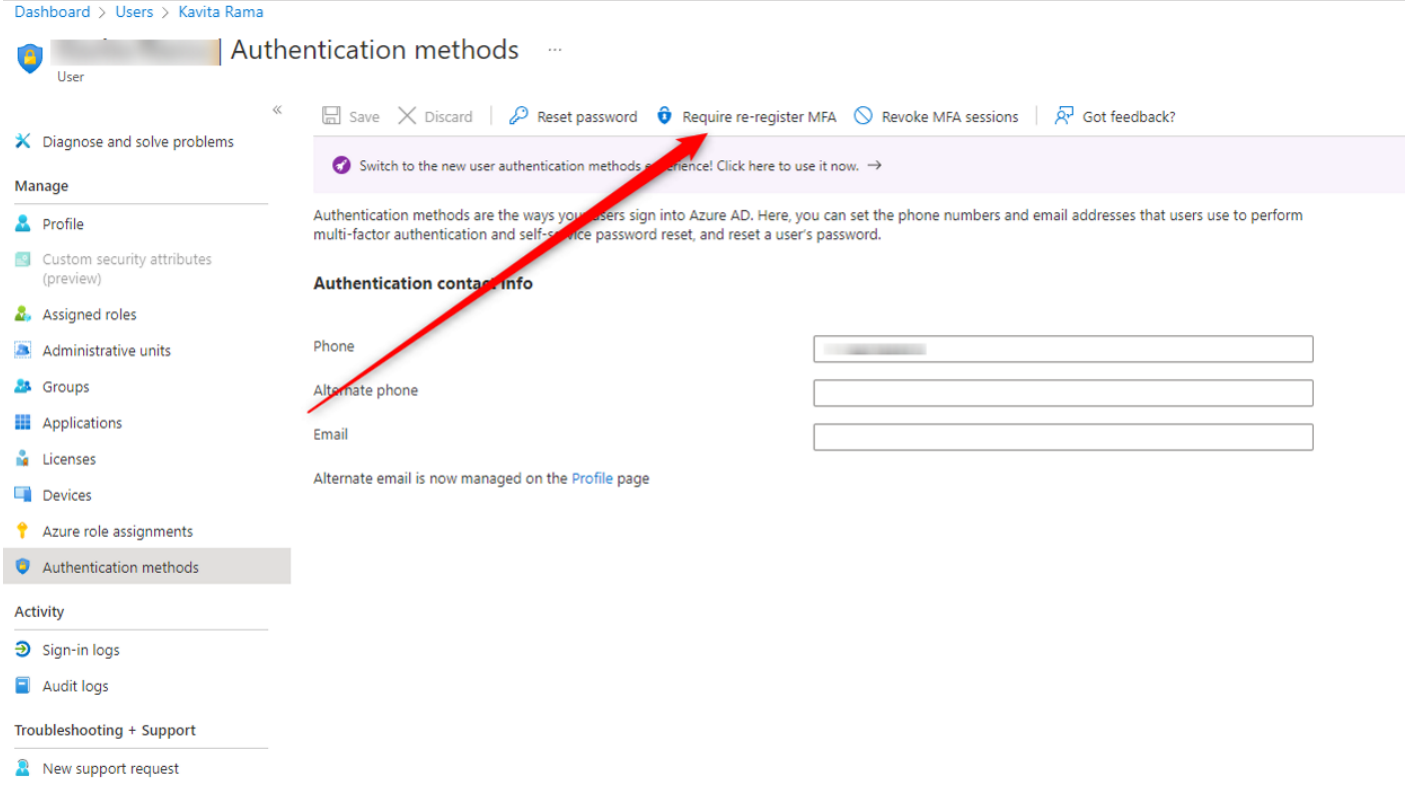


2. Sign user out of every Office 365 session (Now done from Entra Admin Center)

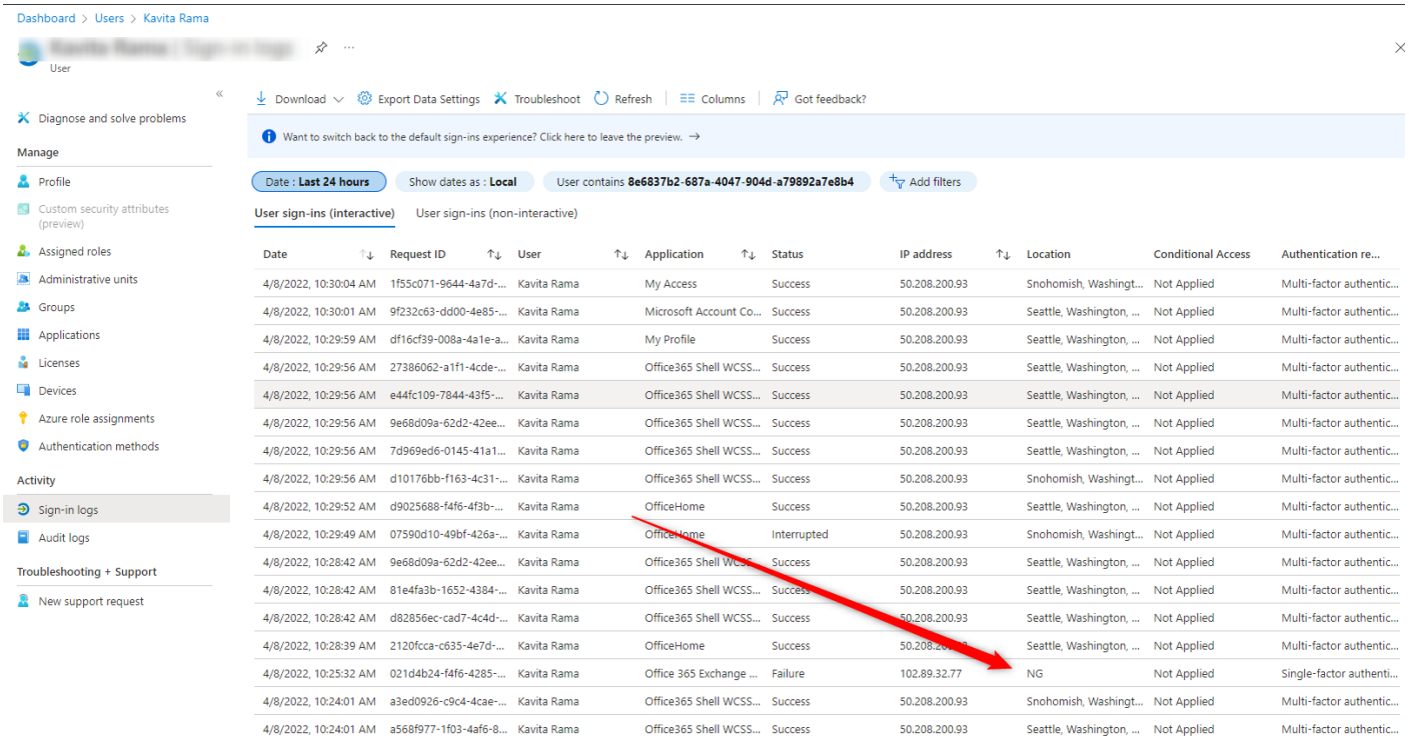


3. Setup MFA
4. Reset MFA if it was already setup (Do this through Endpoint Manager)

If endpoint manager is not available through 365 admin, going incognito and signing into entra.microsoft.com will bring you to the area below as well



5. Look at sign in logs and take note of irrugular locations. Export data and format into a neat excel workbook and name it "Summary of Breach for [user's name]". We want to make this a report that the user's manager can document since banks (or some vendors) will require some of this info and action plans from our clients to restore access.



6. Look in Outlook OWA (or access individual mailbox through exchange admin center) for any odd rules redirecting emails or deleting emails.
7. In Exchange Admin Center, pull a message trace for any email sent by that user for a timeframe that covers the whole breach. Export those results into a second page in the excel workbook that you started and format it with relevant columns and make it easy for the user to read.
8. Look for any Registered devices in Azure that aren't good devices
9. If user is a Global Admin go to next section
10. Send an email to the relevant manager of that user with the user CC'd with a small summary of what kind of compromise it was (session highjack/user provided access, or something else?) and attach the summary workbook. That will give them the info of when the bad guy got access and what emails they were able to send and to whom. I am attaching an example email to this documentation with sensitive data removed but will show what the client should see.

11. If you're fully satisfied that the account is secured again, remove the user from "Restricted Entities" if they're still there: https://security.microsoft.com/restrictedusers

---

Was the User a Global Admin?

1. Verify if the user needs to be a Global Admin
2. Remove all unnecessary Global Admins
3. Look for any outbound connectors in Exchange that don't belong
4. Look for any rules in Exchange that don't belong
5. Verify all users have MFA enabled

> There is also this company that specializes in digital investigations and stuff, called Asceris. I am putting their name down here as a potential partner in the future

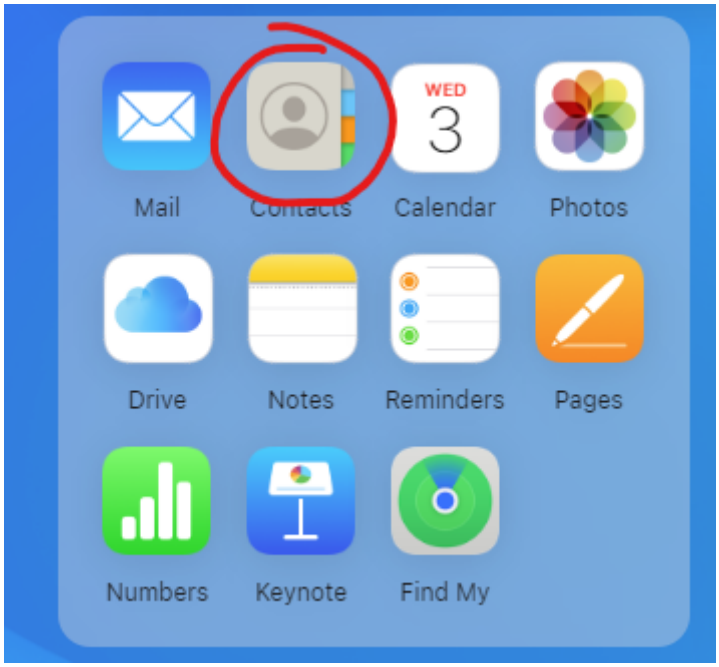
https://www.asceris.com/bec if clients ever need a investigation specialist type service that is more indepth than our own stuff (I don't even know if they're more in-depth yet)

Bulk Contact migration on iPhones

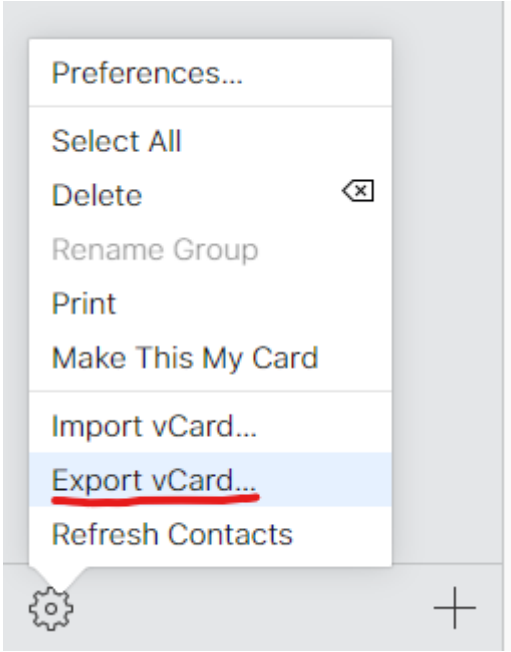
Problem:

Apple iPhone's do not have a built in bulk contact export function programmed into them. Rather they expect that you can share 1 contact at a time, or that you would log into another iPhone with your iCloud account if you needed all of your contacts. However, there is a way to get a single vCard file that contains any or all of your contacts. Please follow the instructions below for this process. As always, please reach out if further assistance is needed, thank you!

Resolution:

1. Ensure that your current (old) iphone has its contacts synced to your iCloud account
   You can check this by going to Settings > click on your name at the top > iCloud > Show All and then make sure "Contacts" is switched on
2. Go to https://icloud.com and login to your iCloud account
3. Click on the "Contacts" icon towards the bottom of the page
   

4. Select all of the contacts that you would like to move over to the new phone. You can do this by holding "Ctrl" and selecting multiple contacts, or by holding Shift and selecting the last contact to highligh ALL contacts.
5. On the bottom left of the screen, click on the gear icon and then select "Export vCard..."



6. The file that downloads can then be emailed to the new phone (or anyone else) and opened. At that point, the iPhone will ask if you'd like to import all of the contacts in the file.

This will allow you to move any number of contacts from one iPhone to another without a shared iCloud account. Have a wonderful day!