STAYING SAFE

HOW TO STAY SAFE IN A DIGITAL WORLD

WHAT IS A SCAM?

- A scam, or a confidence trick, is an attempt to defraud a person or group after first gaining their trust. Confidence tricks exploit victims using a combination of the victim's credulity (believing something to be true), naivety, compassion, vanity, confidence, irresponsibility, and greed.
- A scam can be executed through email, phone calls, text messages, social media, dating apps, software downloads, websites, and even in-person interactions.
- Examples include winning a prizes, charity, invoice fraud, phishing for personal data and investments with high returns/no risk.
- Let's go through some examples …

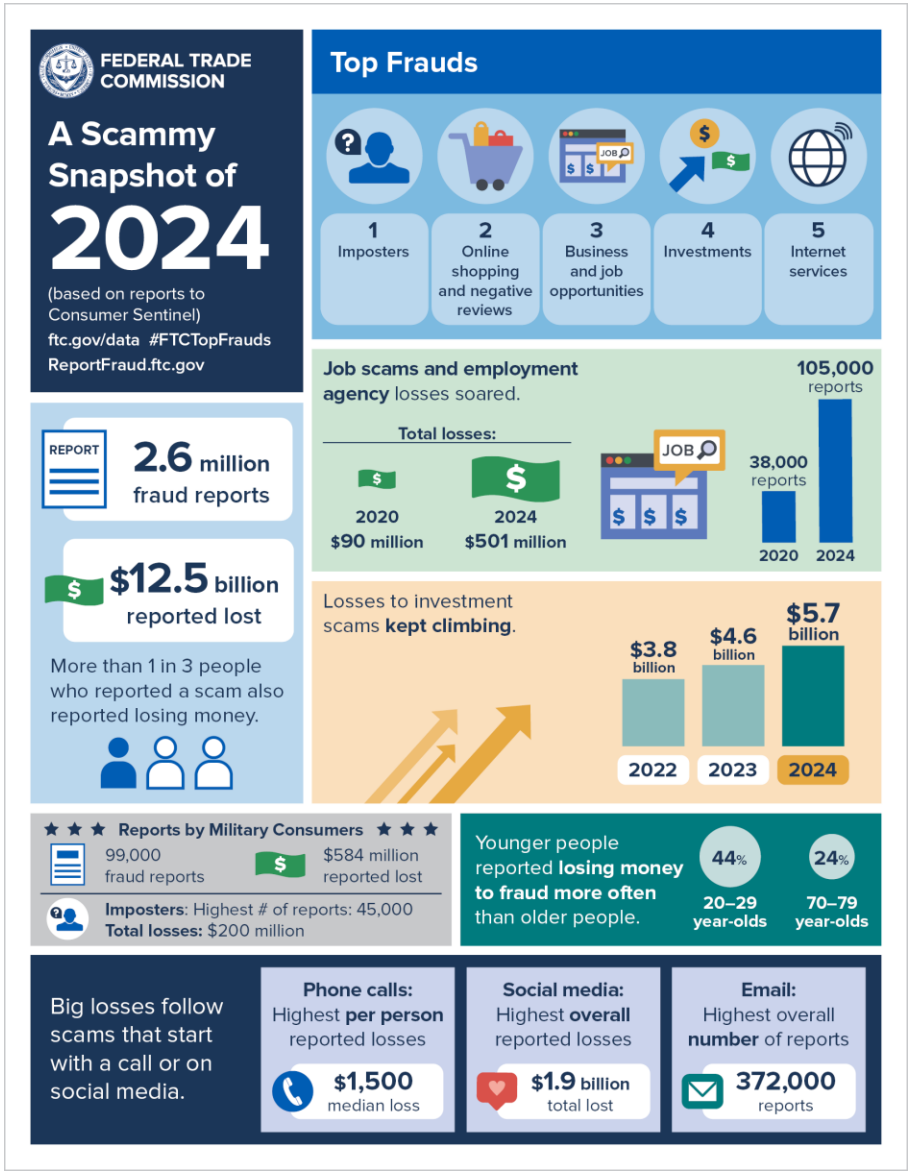
COMMON SCAMS TARGETING RETIREES

- A phone call asks for your Medicare number to verify information or offer a free service or device, warning that benefits might be lost if you don't comply.
- After the passing of a spouse, you get a phone call claiming the deceased owed a debt that must be paid immediately.
- You receive a letter or phone call claiming you've won a large sweepstakes prize. To claim the winnings, you must pay taxes or processing fees upfront, usually via wire transfer or prepaid cards.
- You see an ad online or receive an email offering prescription drugs at a very low price.
- A person knocks on your door saying that your roof is leaking and offers to a no down payment repair with a credit check asking for your DOB and SS#.

COMMON SCAMS TARGETING RETIREES

- You receive a call or email from someone claiming to be from the Social Security Administration, stating there's an issue with their account or benefits. The caller asks for personal information to verify you.
- You are approached by someone offering health insurance that covers everything at a very low cost.
- You are approached by someone offering a "can't miss" investment opportunity with promises of high returns and little risk.
- You receive a phone call from a supposed charity that plays on your emotions, asking for donations to help children, veterans, or disaster victims. The caller pressures you to donate immediately by credit card or bank transfer.
- A text message says that you have a romantic inquiry and provides a link to a web site that asks for some personal information to complete the connection.

SCAMS PLAY ON YOUR EMOTIONS AND FEARS


FEDERAL TRADE COMMISSION
A Scammy Snapshot of 2024
(based on reports to Consumer Sentinel)
ftc.gov/data #FTCTopFrauds
ReportFraud.ftc.gov
Top Frauds
1 Imposters
2 Online shopping and negative reviews
3 Business and job opportunities
4 Investments
5 Internet services
2.6 million fraud reports
$12.5 billion reported lost
More than 1 in 3 people who reported a scam also reported losing money.
Job scams and employment agency losses soared.
105,000 reports
Total losses:
2020 $90 million
2024 $501 million
38,000 reports
2020
2024
Losses to investment scams kept climbing.
$3.8 billion
$4.6 billion
$5.7 billion
2022
2023
2024
Reports by Military Consumers
99,000 fraud reports
$584 million reported lost
Imposters: Highest # of reports: 45,000
Total losses: $200 million
Younger people reported losing money to fraud more often than older people.
44% 20–29 year-olds
24% 70–79 year-olds
Big losses follow scams that start with a call or on social media.
Phone calls: Highest per person reported losses
$1,500 median loss
Social media: Highest overall reported losses
$1.9 billion total lost
Email: Highest overall number of reports
372,000 reports

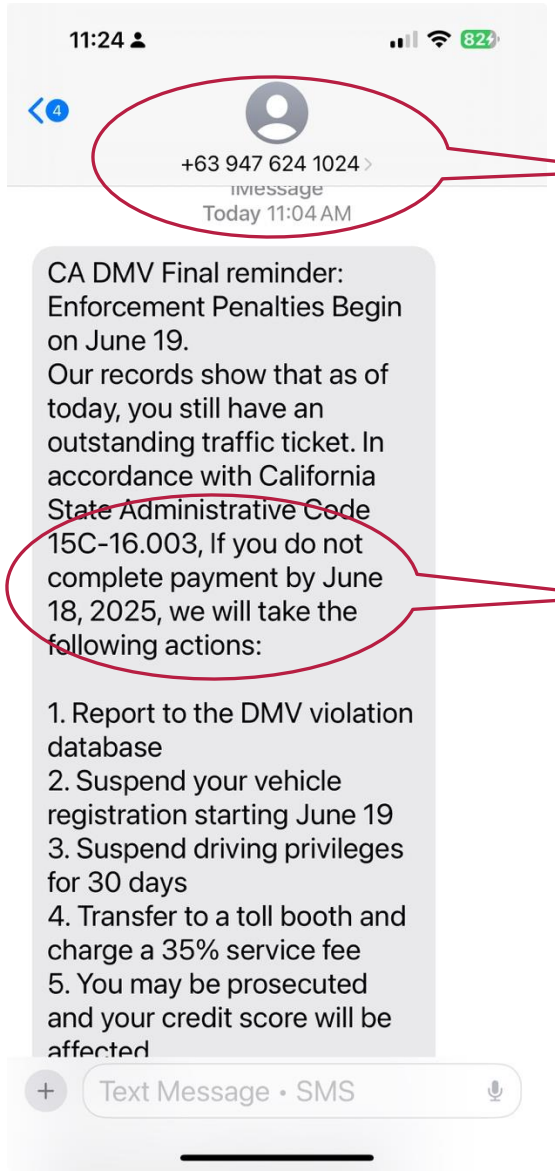
HOW TO STAY SAFE

- Phone calls that are unsolicited
  - Screen unknown calls using your answering service. Be wary of calls that "seem" legit as scammers can fake company identification.
  - If the message elicits a strong emotional response, ask a friend or relative for their opinion.
  - Don't provide sensitive information (DOB, credit card, Medicare number) over the phone.
  - Ask for the organization name and search for the "official" website and contact information
    - .gov for government agencies (slocounty.ca.gov)
    - .com for (bankofamerica.com)
  - Call the organization using the official contact information to confirm the inquiry
  - Let's run through an example that your bank called saying that your account has suspicious activity

IS THAT REALLY YOUR BANK CALLING?

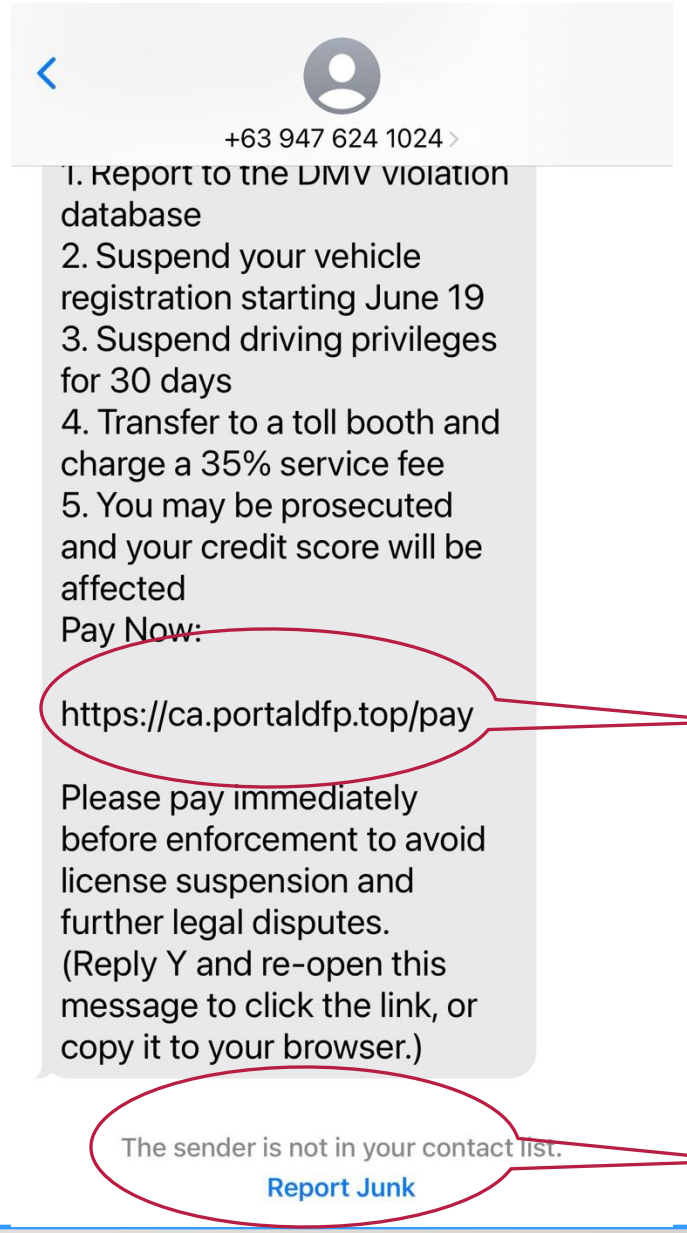
HOW TO STAY SAFE

- Text messages with links or phone numbers that elicit an emotional response (e.g. threat)
  - Never call or respond to phone numbers with international extensions (e.g. +63 is the Philippines)
  - Never click on a web link provided from an unsolicited communication
  - Search for the official website following the instructions from the previous slide
  - Let's run through an example where a text message with an international code of +63 stating that the CA DMV says you have unpaid tickets and they will suspend your auto registration in 2 days.



International phone extension

Immediate emotional action

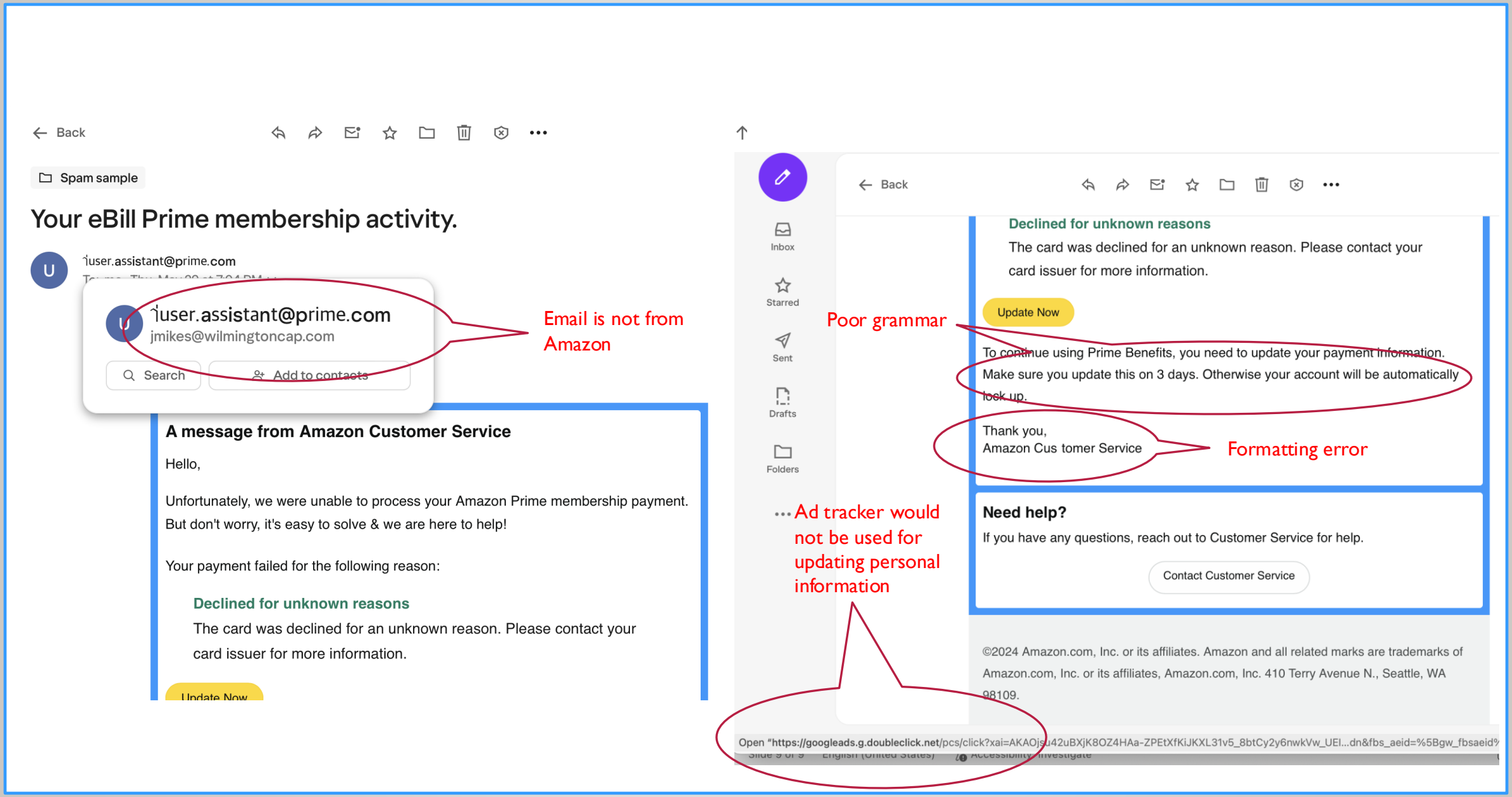


Not a DMV domain

Unknown contact

HOW TO STAY SAFE

- An email from a corporation requests personal information via a website link
  - Legit corporations will not directly request you to enter personal information into a third party website
  - Look at the "From" email address as to the business domain to see if it does match the corporation
  - Verify that the action link (Update for information) goes to the company's website domain (e.g. bankofamerica.com/??)
  - Use AI to inspect the contents and ask if it's a scam. Copy the email text into an AI tool like ChatGPT and ask if it's a scam.
  - Contact the company directly using an official phone number or email address to inquire about the issue
- Let's run through an example email from Amazon says your Prime payment membership payment failed


Back
Spam sample
Your eBill Prime membership activity.
user.assistant@prime.com
user.assistant@prime.com
jmikes@wilmingtoncap.com
Search
Add to contacts
Email is not from Amazon
A message from Amazon Customer Service
Hello,
Unfortunately, we were unable to process your Amazon Prime membership payment. But don't worry, it's easy to solve & we are here to help!
Your payment failed for the following reason:
Declined for unknown reasons
The card was declined for an unknown reason. Please contact your card issuer for more information.
Update Now
Inbox
Starred
Sent
Drafts
Folders
Poor grammar
Declined for unknown reasons
The card was declined for an unknown reason. Please contact your card issuer for more information.
Update Now
To continue using Prime Benefits, you need to update your payment information. Make sure you update this on 3 days. Otherwise your account will be automatically lock up.
Thank you,
Amazon Cus tomer Service
Formatting error
Need help?
If you have any questions, reach out to Customer Service for help.
Contact Customer Service
Ad tracker would not be used for updating personal information
©2024 Amazon.com, Inc. or its affiliates. Amazon and all related marks are trademarks of Amazon.com, Inc. or its affiliates, Amazon.com, Inc. 410 Terry Avenue N., Seattle, WA 98109.
Open "https://googleads.g.doubleclick.net/pcs/click?xai=AKAOjsu42uBXjK8OZ4HAa-ZPEtXfKiJKXL31v5_8btCy2y6nwkVw_UEI...dn&fbs_aeid=%5Bgw_fbsaeid%

HOW TO STAY SAFE

- You get a call from someone that sounds like your grandson asking for help
  - Scammers can use AI clips from social media to construct a voice and then have the AI voice say what they type
  - Caller ID phone numbers can be spoofed so that caller may not be who Caller ID says it is
  - Be wary of voices that sound ”like” a family member, but don’t come from their known phone or don’t come across with the same personality traits
  - Have family members use a security word to “authenticate” themselves if asked for

WHO IS REALLY CALLING YOU?!

AI IS THE ROOT OF ALL THIS SCAM?!?

- AI is being used by scammers, but what works for the scammer can work for you!
- AI websites and phone apps can be used to inspect any digital communication (email, text messages) that seems suspicious
- Let me show you how…

IS THIS A SCAM?

Dear Customer,

Your Microsoft 365 subscription is confirmed. USD 430.56 will debit within 12 hours.

Unauthorized? Call 1 818 867-8131 now.

Details:
Subscription: qbzg-6089-ibc
Email: RUSSOC01532@YAHOO.COM
Customer ID: Jpka-5330-Dkc
Service: MaxSecurity
Term: 4-Year
Start: Saturday, June 21, 2025
Devices: 2
Payment: Auto
Amount: USD 430.56

Thank you!,
Microsoft 365 Customer Care
Bridggett Solesbee
1 818 867-8131

Auto-generated. ©2025

WHAT TO DO IF YOU SUSPECT FRAUD

- Cut off immediate communication with the scammer
- Gather evidence of fraudulent transactions and communications with scammers, and any information that might possibly help to identify the criminals
- Report fraud to the Federal Trade Commission. It won't help you recover your losses, but reported information is used to help with investigations. Call toll-free 1-877-FTC-HELP (1-877-382-4357) or visit reportfraud.ftc.gov
- Contact the Attorney General's Public Inquiry Unit to report a complaint about a business or if you have questions or comments. https://oag.ca.gov/consumers/alerts
- Flag emails and text messages as fraud/spam

WHAT STEPS YOU CAN TAKE?

- Pause, reflect and protect!
- Sign-up for AARP's fraud alerts https://www.aarp.org/money/scams-fraud/landing/
- Get text messages from your credit cards for any charge over a certain threshold (I set mine to $0)
- Have a list of people you trust to contact if you are unsure if you are being scammed
- To help cut down on robocalls, add your phone numbers to the National Do Not Call Registry, operated by the FTC. It won't stop fraudulent calls, but it will make them easier to spot because most legitimate telemarketers won't call numbers on the registry. Register your numbers at 1-888-382-1222 or donotcall.gov

WHAT STEPS YOU CAN TAKE?

- Prevent unauthorized new accounts (e.g. credit card) by freezing your credit
  - Blocks access to your credit report
  - Prevents new account openings
  - Doesn't affect your credit score
  - Requires temporary lifts for certain actions (e.g. a new car loan)
  - Its free!!
  - Credit bureaus are Equifax, Experian, and TransUnion.

CREDIT ORGANIZATIONS

Equifax	Experian	TransUnion
Manage your Equifax credit freeze: **Online** Call 888-298-0045 Equifax Info Services LLC P.O. Box 105788 Atlanta, GA 30348-5788	Manage your Experian credit freeze: **Online** Call 888-397-3742 Experian Security Freeze P.O. Box 9554 Allen, TX 75013	Manage your TransUnion credit freeze: **Online** Call 800-916-8800 TransUnion P.O. Box 160 Woodlyn, PA 19094

Equifax credit freeze: https://www.equifax.com/personal/help/article-list/-/h/a/place-lift-remove-security-freeze/
Experian credit freeze: https://www.experian.com/help/credit-freeze/
TransUnition credit freeze: https://www.transunion.com/credit-freeze

WHAT STEPS CAN YOU TAKE?

- Customer Service Numbers for Commonly Impersonated Organizations
  - IRS (Treasury Inspector General): 800-366-4484
  - Social Security Administration: 800-772-1213
  - Medicare (HHS Office of Inspector General): 800-447-8477
  - Amazon Customer Support: 888-280-4331
  - Google: To report Google scams, visit support.google.com/faqs/answer/2952493
- Have a list of phone numbers for banks, investment, government and other institutions that you regularly use in a secure location for easy access

QUESTIONS?