Be Fraud-Free!

Protecting Yourself from Modern Tech Scams

Blending personal stories and current research to help you understand fraud risks.

- Practical advice
- Technical insights
- Strategic guidance
- Steps for Recovery

Presented by
Mark A. Annati, CISSP, SSCP

Tronpilot Technologies LLC

About Mark...

Mark is a seasoned IT and cybersecurity professional with over 20 years of experience in IT and security management, holding key certifications such as Certified Information Systems Security Professional (CISSP) and Systems Security Certified Practitioner (SSCP) through ISC2.

Formerly the Chief Information Security Officer (CISO) with advansappz.com and Extreme Reach (now XR.com). He is currently serving as a board member of the InfraGard Boston Chapter - an FBI private sector partnership focused on protecting critical infrastructure through civilian tech collaboration, and Chief Technology Officer (CTO) of Tronpilot Technologies LLC (IT and Cyber Presentations and Training).

Mark is committed to educating businesses and individuals on reducing their risk, aligning security strategies with organizational goals, and promoting fraud awareness and prevention.

Today he wishes to help at least one of you not fall victim to fraud!

TRONPILOT technologies LLC

What We Will Learn Today...

Awareness, Discernment, Protection, Action

- Awareness: Learn how to spot and avoid scams.
- Discernment: Know how to ignore fake messages and calls.
- Protection: Protect your accounts and devices with simple steps.
- Action: Act quickly and get help if you're scammed.

TRONPILOT technologies LLC

What are some of the top reasons WHY we can easily become a victim of fraud?

TRONPILOT technologies LLC

FEDERAL BUREAU of INVESTIGATION

Internet Crime Report

2023

INTERNET CRIME COMPLAINT CENTER

Complainants Over 60
101,068

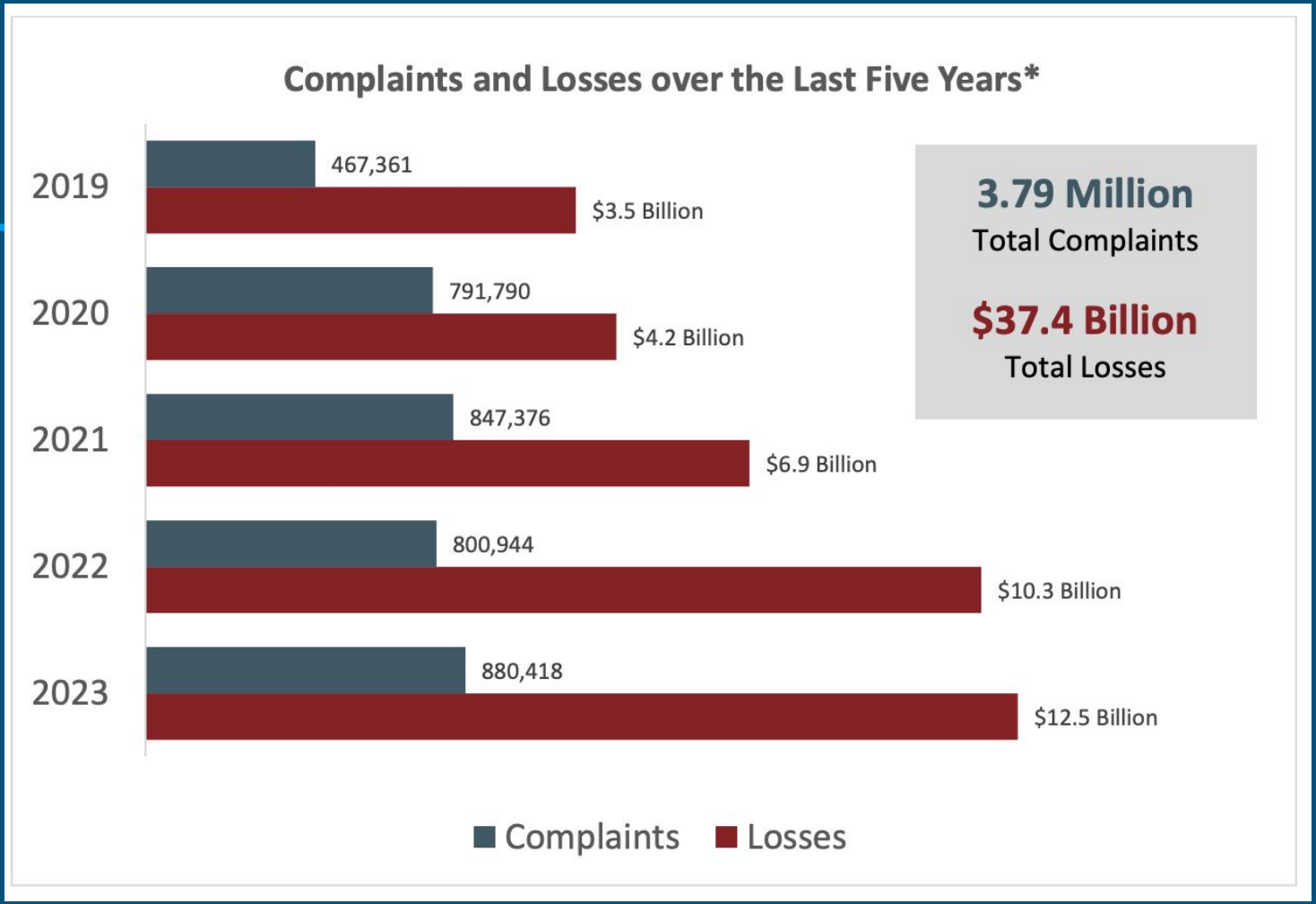
Total Losses
$3,427,717,654

Increase from 2022
11%

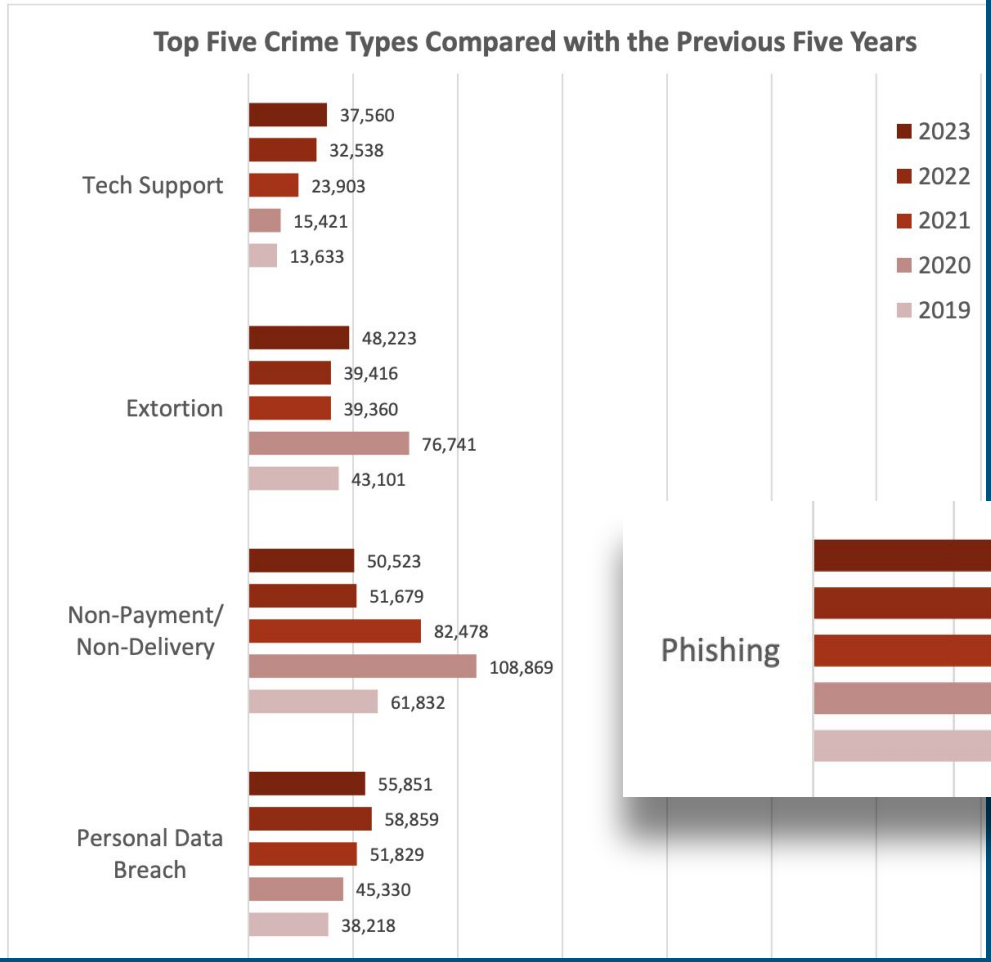
Avg Dollar Loss
$33,915

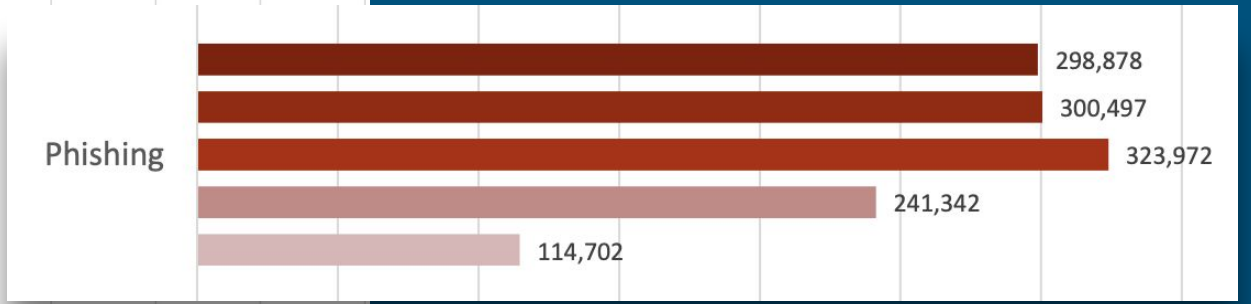
Lost more than $100K
5,920

TRONPILOT technologies LLC



TOP FIVE CRIME TYPE COMPARISON[4]





TRONPILOT technologies LLC

Top 11 Reasons Why We Are Vulnerable

"People are gullible because they want to believe."
- *Anonymous*

1. Lack of Awareness or Knowledge
2. Social Engineering (Fear, Greed, Sympathy)
3. Psychological Vulnerabilities
4. Impersonation and Identity Theft
5. Sophisticated Scams
6. Lack of Security Measures

Top 11 Reasons Why We Are Vulnerable

"People are gullible because they want to believe."
- *Anonymous*

7. Human Error
8. Complexity of Modern Life
9. Overconfidence
10. Financial Incentives
11. Technological Sophistication

What are some common scams targeting us?

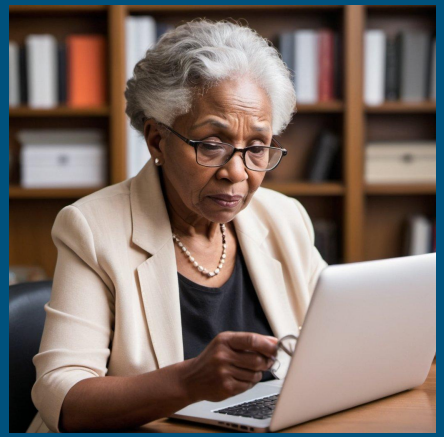
TRONPILOT technologies LLC

Top 16 List of Scams

1. Personal Data Breach & Identity Theft
2. Phishing Emails & Business Email Compromise
3. Medicare, Health Insurance & Government Impersonation Scams
4. Investment & Real Estate Fraud
5. Tech Support Scams
6. Extortion, Stalking, & Threats of Violence
7. Romance & Confidence Scams
8. QR Code Scanning Scams: unsafe site, malware distro, payment hijack

TRONPILOT technologies LLC

Top 16 List of Scams



9. Credit Card / Check Fraud
10. Lottery, Sweepstakes, & Inheritance Scams
11. Phone SIM Hacks - Swap, Clone, Jacking
12. Grandparent Scams
13. Telemarketing & Phone Scams
14. Non-payment / Non-Delivery Scams
15. Advanced Fee & Home Repair Scams
16. Funeral and Cemetery Scams

TRONPILOT technologies LLC

What behaviors should you adopt to help protect yourself from scams?

TRONPILOT technologies LLC

In a world filled with digital noise from spam calls, emails, texts, and social media, focus only on what's familiar and relevant, and simply ignore the rest.

Avoid clicking on unsolicited links, contacting numbers from pop-ups or texts, giving control of your computer to unknown contacts, and sharing personal information over the phone with unsolicited callers.
Beware of scanning QR Codes (QRishing).

Immediately end all communication with scammers, disconnect from the internet if you encounter a suspicious pop-up, and never open email attachments from unknown senders.

Resist the pressure to act quickly; take your time before responding.
Time works against scammers and helps reveal fraud.

Be skeptical of unsolicited contacts and suspicious links; independently verify identities and only use trusted sources for downloads.

If pressured to keep a financial move secret, seek advice from a trusted friend or advisor.
An outside perspective can help identify a scam.

Enable and monitor all alert notifications for transactions and account changes in your online accounts, and verify that you receive alerts for any actions you take.

- Create Unique Usernames for Important Online Accounts
- Use strong, unique passwords and Multi-Factor Authentication (MFA) for each account
- Keep software updated
- Only use Secured Wi-Fi
- Limit online personal info given
- Maintain updated antivirus
- Enable pop-up blockers
- Never leave devices unattended
- Setup Credit Freezes (the big 3)
- Monitor Your Credit Report

Review and tighten privacy settings on devices and accounts, carefully manage personal information, dispose of sensitive documents securely, and pre-authorize access to personal health information when necessary.

Only Allow Necessary or Essential Cookies

EDUCATE

Stay informed on scams and don't get phished by subscribing to newsletters like AARP's Fraud Watch Network, FTC's Consumer Advice, National Council on Aging (NCOA), Consumer Financial Protection Bureau (CFPB), and Fraud.org for updates, tips, and resources on how to protect yourself from fraud. More resources can be found at the end of this presentation.

Report fraudulent activities to the FBI’s Internet Crime Complaint Center at www.ic3.gov, and relevant financial institutions, credit agencies, and law enforcement, while documenting all details like names, communication methods, and transaction information.

How should we prepare to protect ourselves from fraud?

TRONPILOT technologies LLC

Limit Your Risk

- Adopt smart tech behaviors
- Secure your smartphone and online accounts.
- Use a separate, secret email for banking, investments, and sensitive accounts.
- Practice safe computing - like using different passwords, MFA, and Passkeys
- Enable account recovery options
- Note important phone contacts
- Secure copies of important documents
- Establish a trusted go-to person

Follow me as we explore these topics further….

I use checks for my payments, how can I prevent fraud?

TRONPILOT technologies LLC

8 Best Practices for Check Management

1. Secure with Indelible Ink - No Blank Spaces
2. Disguise Checks (Greeting Card or Wrap in Paper)
3. Use Security-Tinted Envelopes
4. Avoid Marking “Check Enclosed” on Envelopes
5. Hand-Deliver or Use Certified Mailing with Tracking
6. Write Restrictive Endorsements (“For Deposit Only”)
7. Securely Store & Limit Access to Checkbooks
8. Regularly Monitor and Reconcile Accounts (balance the checkbook!)

TRONPILOT technologies LLC

What should we do with all those cookie pop-ups and prompts?

TRONPILOT technologies LLC

Best Practices for Managing Cookie Pop-ups

1. Cookies help websites remember info or track you.
   Adjust cookie settings for safer browsing.

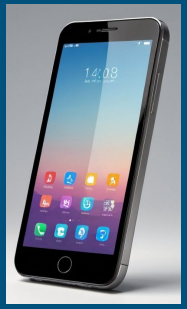
2. Choose “Manage Preferences” or “Settings” instead of “Accept All.”
   Only allow essential cookies.

3. Use “Reject All” if possible, or at least reject marketing/analytics cookies to avoid tracking.

TRONPILOT technologies LLC

How should you secure your smartphone?

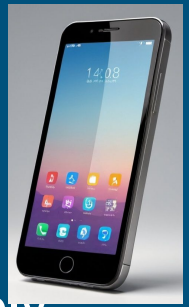
10 Smartphone Features to Enable and Use



1. Use a strong 6-digit or alphanumeric passcode.
2. Enable Touch ID or Face ID for secure access and authentication.
3. Use Tap to Pay Instead of Physical Credit Cards - Apple Pay or Google Pay uses tokenization instead of your CC number
4. Customize your lock screen to control what's visible without unlocking.
5. Enable Two-Factor Authentication (2FA) for added security if your password is compromised.

TRONPILOT technologies LLC

10 Smartphone Features to Enable and Use



6. Set up "Find My" to locate, lock, or erase your device remotely if lost or stolen.
7. Enabling stolen device protection, like iOS's "Stolen Device Protection" and Android's "Theft Detection Lock"
8. Use a password manager to securely store and update passwords, **passkeys**, and more across devices.
9. Enable automatic security updates to fix vulnerabilities.
10. Use cloud backup to keep a secure copy of your data in case your device is lost, stolen, or replaced.

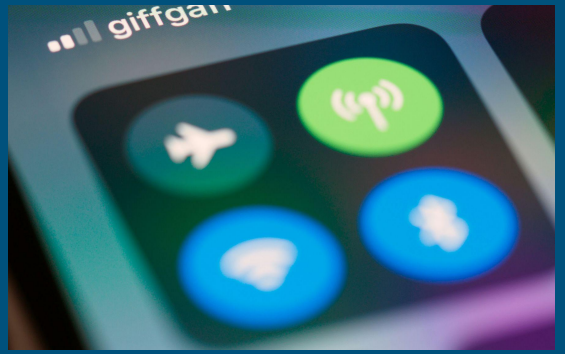
Use Passkeys

A Simpler, Safer Way to Login

- **Passwordless Login:** Uses device-stored cryptographic keys, no need to type passwords.
- **Stronger Security:** Protects against phishing and password leaks.
- **Easy to Use:** Unlock with biometrics (fingerprint, face) or a device PIN.
- **Works Across Devices:** Syncs securely via cloud for seamless access everywhere.

TRONPILOT technologies LLC

Why You Should Turn Off Bluetooth & Wi-Fi When Not in Use



- **The Danger:**
  Leaving Bluetooth or Wi-Fi ON means that they are always LOOKING for a connection. Active connections can be used to eavesdrop on your data and communications. This can allow hackers to break into your device and steal data.

- **Reduce Your Risk:** Turning Wi-Fi/Bluetooth OFF lowers the chances of someone finding weak spots to attack. This can be tuned using Location automation.

- **Solution:** Use mobile data or secure personal hotspots for sensitive transactions.

TRONPILOT technologies LLC

How do you protect your Cloud Accounts?
(Apple iCloud, Google, Microsoft)

TRONPILOT
technologies LLC

8 Ways to Protect Your Phone's Cloud Account

1. Remove unused or outdated devices from your account to reduce risk.
2. Validate or update your email address for essential account recovery.
3. Add an alternate email for account access if your primary email is unavailable.
4. Set up an additional trusted phone number for receiving verification codes if your primary device is inaccessible.

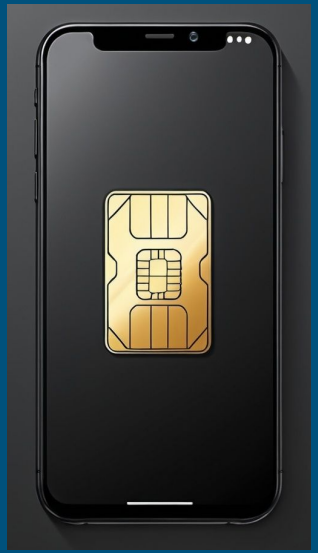
8 Ways to Protect Your Phone's Cloud Account

5. Validate or update your recovery info, like birth date, for security questions.
6. Create and securely store a recovery key for account access.
7. Add a rescue email for important security notifications.
8. Update your security questions and answers.

*How do you protect your actual **phone number** with your cell provider?*

TRONPILOT technologies LLC

5 Ways to protect your phone number



1. Enable a PIN or passcode on your mobile phone carrier account, to authorize any changes to your account, including number transfers.
2. Use two-factor authentication (2FA) on all accounts.
3. Enable alert notifications for any account changes, including SIM card changes.
4. Regularly review your phone account activity.
5. Avoid sharing your phone number publicly.

TRONPILOT technologies LLC

What should you do if your phone is lost or stolen?

TRONPILOT technologies LLC

Act QUICKLY! 9 Steps to Take

1. Use "Find My" to locate your misplaced phone.
2. Change passwords for your phone's cloud account and critical apps.
3. Notify your mobile carrier to secure your number and assist with transfer.
4. Inform financial institutions if using financial apps on the phone.
5. Place a fraud alert with Equifax, Experian, and TransUnion.
6. Report the loss or theft to the police.
7. Consider remotely erasing your device to protect data.
8. Remove the device from your cloud account to lock it out.
9. File a claim if you have theft and loss insurance.

TRONPILOT technologies LLC

What if you need to move your phone number to a new or replacement phone?

TRONPILOT technologies LLC

5 Tips in restoring your backup to a new phone

1. Follow your carrier's specific instructions for the process.
2. Apple and Google offer simple ways to restore data to your new phone.
3. Keep your device connected to Wi-Fi and plugged in during the restore.
4. The restore may take hours, depending on backup size and internet speed.
5. After restoration, complete additional steps to update your device, apps, and services.

What if I've been hacked and I don't know where to begin?

TRONPILOT technologies LLC

Starting Fresh: 8 Key Steps for a Secure Digital Reset

1. Obtain New, Secure Devices
2. Create New Email Accounts with Strong Passwords & MFA
3. Get a New Phone Number from a Different Carrier
4. Set Up Antivirus and VPN on New Devices
5. Change Passwords for Important Accounts
6. Use New Email & Phone for Account Recovery
7. Avoid Using Old Devices for Sensitive Access
8. Be Vigilant: Don’t Reinstall Potentially Compromised Files

TRONPILOT technologies LLC

Thank you for attending.

I hope you feel empowered!

Questions?

TRONPILOT
technologies LLC

Resources

And References

TRONPILOT
technologies LLC

References 1 of 4

- Scam susceptibility may signal risk for cognitive decline https://www.nia.nih.gov/news/scam-susceptibility-may-signal-risk-cognitive-decline
- PLOS Research: Predictors of cognitive functioning trajectories among older Americans: A new investigation covering 20 years of age- and non-age-related cognitive change https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0281139
- Share of those 65 and older who are tech users has grown in the past decade https://www.pewresearch.org/short-reads/2022/01/13/share-of-those-65-and-older-who-are-tech-users-has-grown-in-the-past-decade/
- Older Adults Embrace Tech but Are Skeptical of AI https://www.aarp.org/pri/topics/technology/internet-media-devices/2024-technology-trends-older-adults.html
- Uber driver who was shot and killed by 81-year-old Ohio man after both received scam calls https://www.cbsnews.com/news/uber-driver-killed-scam-phone-call-william-brock-loletha-hall-clark-county-ohio/
- Elder Fraud Prevention Network Development Guide https://www.consumerfinance.gov/consumer-tools/educator-tools/resources-for-older-adults/elder-protection-networks/
- Form to advise Medicare of person(s) to access your personal health information - https://www.cms.gov/cms10106-authorization-disclose-personal-health-information#:~:text=11%2F30%2F2025-,1%2D800%2DMEDICARE%20Authorization%20to%20Disclose%20Personal%20Health%20Information,to%20someone%20other%20than%20you

References 2 of 4

- Unclaimed Property - check your state site to see if there are items in your name and claim: https://unclaimed.org/search/
- Used for Image Creation - https://openart.ai/create
- Photos and Images Used
    - Glen Carrie on Unsplash
    - George Prentzas on Unsplash
    - Brett Jordan on Unsplash
    - Money Knack on Unsplash

TRONPILOT technologies LLC

References 3 of 4 (Gov)

- FBI Elder Fraud https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/elder-fraud
- FBI Field Offices https://www.fbi.gov/contact-us/field-offices
- FBI - submit a tip online - https://tips.fbi.gov/
- Internet Crime Complaint Center at ic3.gov - https://www.ic3.gov/
- IC3 2022 Elder Fraud Report - https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3ElderFraudReport.pdf
- IC3 Public Service Announcement on "Phantom Hacker" Scams - https://www.ic3.gov/Media/Y2023/PSA230929
- IC3 Public Service Announcement for Older Americans (Video) - https://www.justice.gov/elderjustice/video/ic3-public-service-announcement-older-americans
- IC3 2021 Elder Fraud Report - https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3ElderFraudReport.pdf
- IC3 Elder Fraud Page - https://www.ic3.gov/Home/EF
- IC3: A Warning About Technical and Customer Support Fraud - https://www.ic3.gov/Media/Y2022/PSA220316
- IC3: FBI Warns of a Grandparent Fraud Scheme Using Couriers - https://www.ic3.gov/Media/Y2021/PSA210729
- IC3: Perpetrators Use Various Methods to Deceive and Defraud Elderly Victims for Financial Gain - https://www.ic3.gov/media/2019/190919.aspx
- Victim Support: Older Adult Financial Exploitation Brochure (pdf) - https://www.fbi.gov/file-repository/vsd-older-adult-financial-exploitation-brochure-2019.pdf/view
- Department of Justice: Elder Justice Initiative - https://www.justice.gov/elderjustice

References 4 of 4 (YouTube)

- 6 Scams Targeting Seniors - https://www.youtube.com/watch?v=B_Y-kN7uO0w
- Online Scams Against The Elderly - Stay Safe Online - https://www.youtube.com/watch?v=QSL-nEClLRk&t=0s
- Top 5 Tips to Avoid Senior Scams - https://www.youtube.com/watch?v=muHXmMclyoq
- Here are the top scams targeting older adults - https://www.youtube.com/watch?v=30KqBqzqEIQ
- What is Elder Fraud? How To Prevent Senior Citizen Scams | Aura - https://www.youtube.com/watch?v=tu15WGh9jXq
- Avoiding Scams and Fraud for Older Adults - https://www.youtube.com/watch?v=ar2MOvn2aDc
- Senior Scams and Frauds - protection and prevention - https://www.youtube.com/watch?v=7JCpkP7JVJ4
- What is Elderly Exploitation | Financial Exploitation of the Elderly | Elderly Abuse | Prevention - https://www.youtube.com/watch?v=UbDJYiUVR3E
- How To Avoid Becoming A Victim Of Scams That Target Older Adults - https://www.youtube.com/watch?v=KIYQQoj5IPE
- Webinar: New resources for Elder Fraud Prevention and Response Networks — consumerfinance.gov - https://www.youtube.com/watch?v=i2zVsouBznI
- Webinar: Free elder fraud prevention tools for financial institutions — consumerfinance.gov - https://www.youtube.com/watch?v=E-MJNZxNvTU
- Chase bank blames woman for not protecting her account after scammers stole $160,000 - https://www.youtube.com/watch?v=jt6UDAYrf9I
- Scams Targeting Seniors - https://www.youtube.com/watch?v=qOQvGCQJupY
- Fraud and Scams Prevention - https://www.youtube.com/watch?v=1iFzn8OI6ds
- Elder Abuse Prevention Frauds & Scams - https://www.youtube.com/watch?v=Dkaryj-ook8
- UPSTATE ELDER ABUSE CENTER AT LIFESPAN ON FRAUD PREVENTION - https://www.youtube.com/watch?v=NBKy5ZPlFeQ
- Webinar: Promising practices from Elder Fraud Prevention Networks Part 1 — consumerfinance.gov - https://www.youtube.com/watch?v=1TIy2pIKy10
- How Seniors Can Prevent Scams and Financial Exploitation | JPMorgan Chase & Co. - https://www.youtube.com/watch?v=bpktlUqfy4k
- New Scams to Watch Out For (2023) - https://www.youtube.com/watch?v=jxTsI5XvM-c
- Financial Elder Abuse - Detection, Intervention & Prevention - https://www.youtube.com/watch?v=yBAg37jxyK0
- Elder Fraud - https://www.youtube.com/watch?v=JyjyypBtWeA
- The Fraud Investigation Process - https://www.youtube.com/watch?v=T0LUyg20MgE
- The Guide to Elder Financial Abuse | RMO Lawyers - https://www.youtube.com/watch?v=UbuSHUPsAXU

TRONPILOT technologies LLC