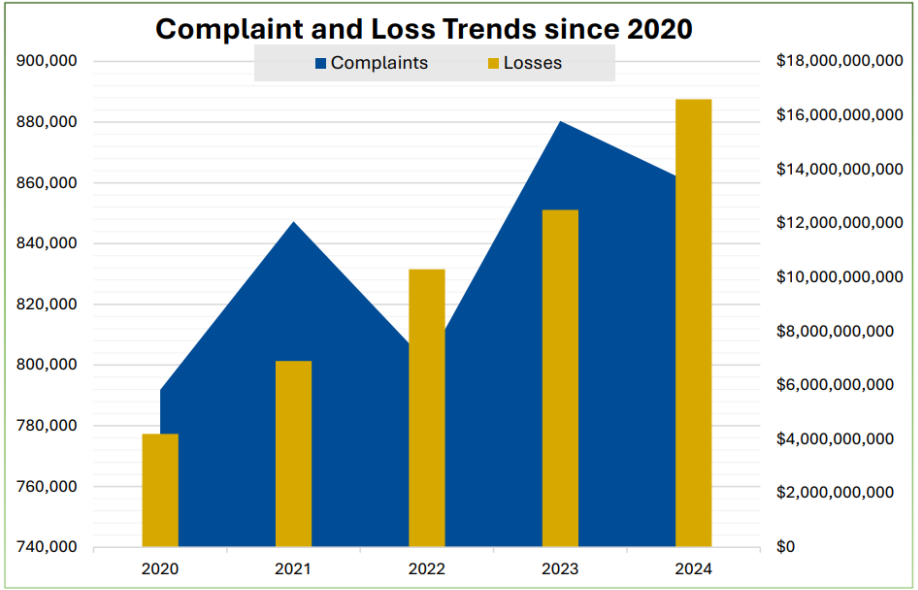
Cyber Fraud Literacy

AUTHORS: BRIAN GIBLIN & ED BASSETT

Agenda

- How bad is the problem
- Common types of Fraud/Theft
- What you can do about it NOW
- What can you do after it happens

How bad is it?



IC3 COMPLAINTS - PAST FIVE YEARS

4.2 Million Complaints	$50.5 Billion in Losses	836,000 Average

Since 2000, the IC3 has received more than 9 million complaints.

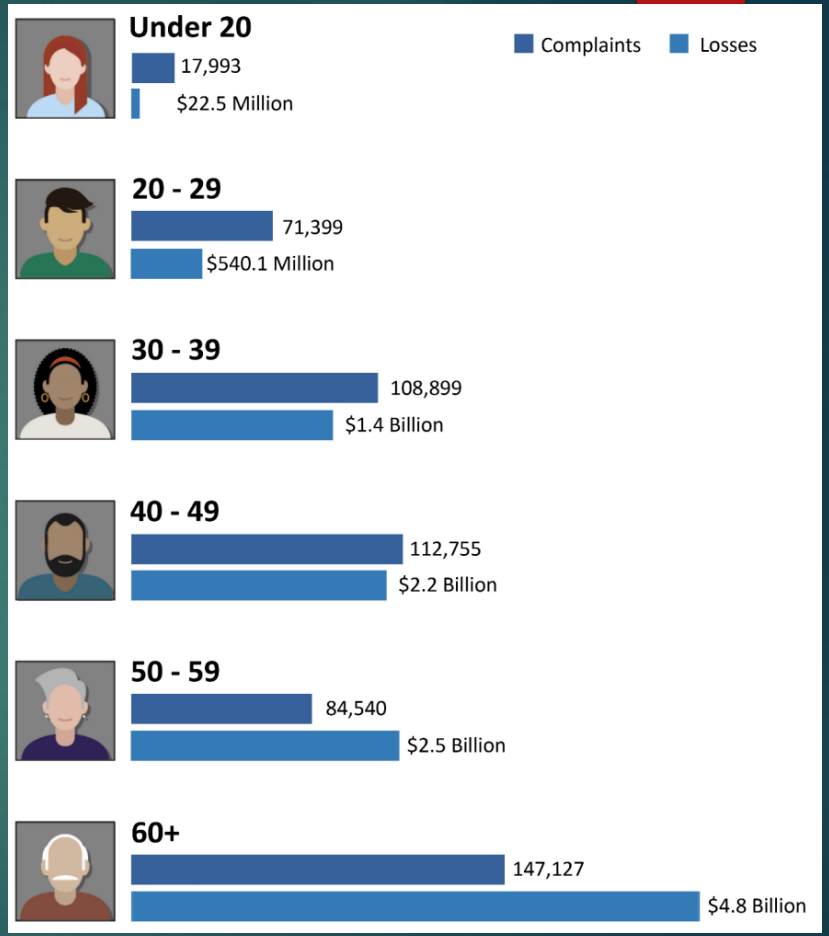
Source: FBI

Seniors targeted more…

Victims over age 60

- 147,127 complaints
- $4.9B in losses
- 43% YoY increase
- Avg loss: $33,915

- 7.500 people lost >$100k!



Source: FBI

…and suffering the greatest losses!

Types of fraud

Common Scams Targeting Seniors

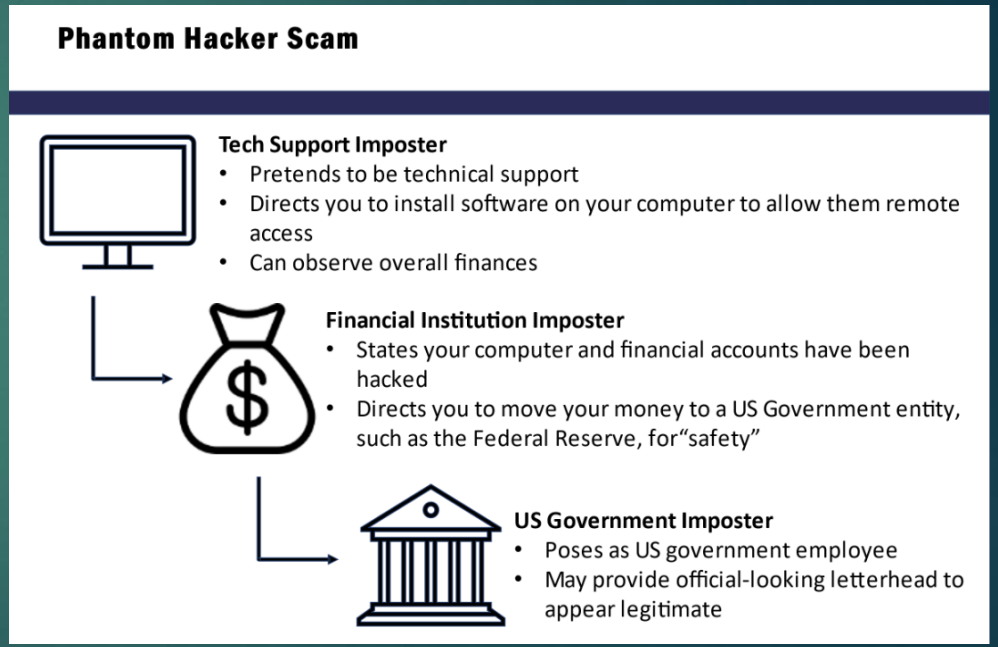
- **Tech Support Scam**
  Perpetrators pose as technology support representatives and offer to fix non-existent computer issues—gaining remote access to victims' devices and, thus, their sensitive information
- **Government Impersonation Scam**
  Perpetrators pose as government employees and threaten to arrest or prosecute victims unless they agree to provide funds or other payments
- **Grandparent Scam**
  Perpetrators pose as a relative—usually a child or grandchild—claiming to be in immediate dire financial need
- **Romance Scam**
  Perpetrators pose as interested romantic partners through dating websites to capitalize on their victims' desire to find companions

Common Scams Targeting Seniors (cont.)

- **Sweepstakes/Charity/Lottery Scam**
  Perpetrators claim to work for legitimate charitable organizations to gain victims' trust. Or they claim their targets have won a foreign lottery or sweepstake, which they can collect for a "fee"
- **Home Repair Scam**
  Perpetrators appear in person and charge homeowners in advance for home improvement services that they never provide.
- **TV/Radio Scam**
  Perpetrators target potential victims using illegitimate advertisements about legitimate services, such as reverse mortgages or credit repair
- **Family/Caregiver Scam**
  Perpetrators are relatives or acquaintances of the elderly victims and take advantage of them or otherwise get their money

Phantom Hacker Scam

- This Phantom Hacker scam is an evolution of more general tech support scams, layering imposter tech support, financial institution, and government personas to enhance the trust victims place in the scammers and identify the most lucrative accounts to target
- Victims often suffer the loss of entire banking, savings, retirement, or investment accounts under the guise of "protecting" their assets



Source: FBI

Common Traits/Themes

Common Traits/Themes

- In most cases, criminals use very social techniques to convince their victims to participate willingly
- Scammers initiate the contact: pop-up, email, text, or phone
- Scams may unfold over several calls – taking days or even weeks
- Much less reliance on technical "hacking" and computer/account takeover than most people think.

Common Traits/Themes (cont.)

- The criminal pretends to be someone the victim either fears or trusts, preferably both
  - IRS, FBI, Bank Fraud Department, Computer Support
  - Offer help, built trust
- Scammers instill fear and urgency
  - Adrenaline suppresses judgement, common sense, and hesitation
  - Do not hang up, do not tell anyone
  - Family member at risk; computer/accounts hacked; money at risk; can lose your house; jail threats
- Guide victims to pay or move money, often to protect the money, family, or property
  - New accounts, cryptocurrency, ACATS transfers, gift cards, Zelle, payment app (Venmo, PayPal), cash, gold

What can you do NOW?

What can you do NOW/BEFORE?

- Become aware of these scams
- Exercise caution in interactions (phone call, text, email, pop-up) you did not initiate
- Protect your financial accounts
- Decide who you would call if you receive a warning or threat
- Discuss this topic with your family and friends

Things to do every day

Safety precautions we all should practice everyday:

- Don't answer phone calls from unknown numbers
- Don't click on links in texts, emails or pop-up messages
- Assume people and companies aren't who they say they are
- Reach out to the person or company through a secondary contact to verify
- Ask a friend or family member about suspicious messages
- Slow down, breath, and trust your gut

Password Strategies

Do

- Different passwords for each account
- Use a password generator to randomize
- Make passwords long (12+ characters)
- Make passwords complex
  - Uppercase, lowercase, number, symbols
  - Phrases and quotes
- Store passwords securely
  - Password manager/vault or
  - Write them down… and keep list secure

Don't

- Save your passwords locally in web browsers or a document/spreadsheet
- Re-use passwords
- Use personal info in password
- Use dictionary words or pseudo words
- Try to remember passwords

Recommendation: Bitwarden password manager (free for personal use)

2-step Login

- **Provides an additional layer of protection that makes it much more difficult for hackers or cybercriminals to gain unauthorized access to your account**
- Your password is something you know
- Add a 2nd step:
  - Something you have (e.g., authentication application or a confirmation code from your phone or email)
  - Something you are (e.g., fingerprint or face scan)

Alerts & Notifications

Ask your financial institutions how they protect against fraud

- Prosperion uses voice verification to confirm email/voicemail requests and ACAT transfers
- Financial accounts may offer a "Trusted Contact" option for notices of suspicious activity
- Set up alerts and notifications:
  - Low balance
  - Transfers/Charges/Withdrawals
  - Unusual activity
  - Large Purchases

Alerts can come as text messages or email

Tip: Familiarize yourself with YOUR alerts, so you don't fall victim to alert scams

Freeze credit

- A credit freeze, or security freeze, keeps the sensitive data in your credit files from being accessed without your consent

- How to contact credit bureaus:
  - Equifax: Call 800-349-9960 or go online
  - Experian: Go online to initiate, or for information call 888-397-3742
  - TransUnion: Call 888-909-8872 or go online

- You can unfreeze anytime, which you should do when you are applying for new credit

Set up a Buddy system

- Pick someone you trust implicitly (spouse, family member, close friend, advisor, care giver)
- Discuss Cyber Fraud
- Ask them to be your Fraud Prevention Buddy and/or offer to do this for them
- Agree that you will ALWAYS talk before sending money (>$XX) to anyone for any reason
- Set the person up as a Trusted Contact on financial accounts (where available)
- Consider sharing Alerts & Notifications
- Buddy should offer/agree:
  - "I will go to jail for you" (pro tip: no one will actually go to jail)
  - "Even if you're afraid for me, you can always call me"

Create a call sheet

- Personal Contact/Fraud Prevention Buddy: XXX-XXX-XXXX
- Bank 1: XXX-XXX-XXXX, xxxxx@xxx.com
- Bank 2: XXX-XXX-XXXX, xxxxx@xxx.com
- Tech Support: XXX-XXX-XXXX, xxxxx@xxx.com
- Financial Account: XXX-XXX-XXXX, xxxxx@xx.com

- Do not accept help from a stranger

- Do not call a number or send a text or email to a contact that you didn't look up yourself

What to do if it happens to you?

If a scammer calls…

Post Fraud Response Priorities

1. Password lists – vault application, browser cache, spreadsheet
2. Bank accounts – checking, savings, CDs
3. Investment accounts – brokerage, retirement, life insurance
4. Direct deposit Income sources – employers, social security, pensions, annuities, trusts, government benefits
5. Phone accounts – Apple ID for iPhone, Google for Android
6. Computer/cloud/email accounts – Microsoft, Google, ISP, cloud backup
7. Credit bureaus (credit freeze)
8. If they've lost money:
    a) FBI/police
    b) Insurance
    c) Tax accountant (especially if retirement funds were lost)

Points to Remember

- Scammers are professional criminals - they do this all day every day, using sophisticated social cons that exploit fear and trust
- Do not engage with them
  - Even out of curiosity
  - Even if they threaten arrest or jail
  - Even if they offer to save you from a crime
  - Even if they offer to make your life exciting by helping stop criminals
- As soon as you feel suspicious or scared, call a trusted contact

Helping fraud victims

- Reassure them - scammers are highly skilled, and victims should not feel guilty
- Ensure they have fully terminated contact with the scammers
  - Modern schemes can last days or weeks using many phone calls, building trust and escalating the theft
- Advise or assist in locking the scammers out
  - Check transactions, change passwords, verify contact/recovery options, set up 2-step login
- Share the story with others so they don't get scammed
- Advise them to report it to the FBI or other law enforcement: complaint.ic3.gov/

Resources

Report a crime

- FBI Denver Field Office
  8000 E 36th Ave
  Denver, CO 80238
  https://www.fbi.gov/contact-us/field-offices/denver
  (303) 629-7171

- Internet Crime Complaint Center (IC3)
  complaint.ic3.gov

FBI Announcements

- Brochure
  www.ic3.gov/Outreach/Brochures/Elder_Fraud_Tri-fold.pdf

- Public Service Announcements
  Grandparent Scams: www.ic3.gov/PSA/2023/PSA231117
  Phantom Hacker Scams: www.ic3.gov/PSA/2023/PSA230929
  Instant Payment Scams: www.ic3.gov/PSA/2022/PSA220414
  Government Impersonation: www.ic3.gov/PSA/2022/PSA220307
  Elder Fraud methods: www.ic3.gov/PSA/2019/PSA190919

- Annual Report
  https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

Resources (cont.)

- Microsoft support.microsoft.com/en-us/topic/avoid-and-report-microsoft-technical-support-scams-392515fa-c630-b41d-2039-a637d5eaaec2
- Bitwarden Password Manager (recommended) bitwarden.com/products/personal/
- Two-step Login www.cisa.gov/MFA
- How to Freeze Credit www.nerdwallet.com/article/finance/how-to-freeze-credit

  consumer.ftc.gov/articles/what-know-about-credit-freezes-fraud-alerts
- More on the techniques www.wired.com/story/what-is-pig-butchering-scam/

  consumer.ftc.gov/articles/how-avoid-government-impersonation-scam

  www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/romance-scams


What are your questions?