



# 2022 TRENDING SCAMS

# FBI and IC3

**MORE** FILE A COMPLAINT CONSUMER ALERTS INDUSTRY ALERTS BEC RANSOMWARE ELDER FRAUD SCAMS

 **FEDERAL BUREAU OF INVESTIGATION**  
**Internet Crime Complaint Center IC3** 

## Elder Fraud

The mission of the FBI is to protect the American people and uphold the Constitution of the United States. This mission includes our efforts to combat financial crimes targeting seniors. The FBI, in alignment with the Department of Justice Elder Fraud Initiative and the efforts of our internal and external partners, is committed to this mission. It is from this commitment to the American people that the FBI provides the public an avenue to report fraud through the IC3.

The IC3 receives and tracks thousands of complaints daily, reported by victims of fraud. Any person aged 60 or older could be considered a victim of Elder Fraud. IC3 reporting is key to identifying, investigating, and holding those responsible accountable for their actions.

Each year, millions of elderly Americans fall victim to some type of financial fraud or internet scheme.

If you, or someone you know, is a victim of a fraud or scam, file a complaint with the IC3.

[File an Elder Fraud Complaint](#)



Elder Fraud Report

[Perpetrators Use Various Methods to Deceive and Defraud Elderly Victims For Financial Gain](#)

[Thu, 19 Sep 2019](#)

[FBI Warns of a Grandparent Fraud Scheme Using Couriers](#)

[Thu, 29 Jul 2021](#)



[Elder Fraud Brochure on IC3.gov](#)

<https://www.ic3.gov/Content/PDF/ElderFraudBrochure.pdf>

# Reports from Older Coloradoans in 2022

1. Imposter Business
2. Identity Theft
3. Tech Support/Computer Virus
4. Home Repair/Improvement
5. Online Dating/Romance
6. Imposter Government (SSA, IRS)
7. Fraudulent Sales
8. Sweepstakes/Prize/Lottery
9. Phishing
10. Non-Stranger Exploitation

# 2022 Scam Trends

- ID Theft
- Tech Support/Computer Virus
- Romance Scams
- Payment Methods
- Communications Methods

# FBI - IC3 Statistics

## Top 3 Frauds by Victim (Over 60) Loss for September 2022 In Colorado

Crime Type	Number of Victims	Total Loss
Tech Support	51	\$1,417,274
Government Impersonation	16	\$412,202
Investment	5	\$398,000

# Identity Theft

## What's New or Trending

- Still fallout from the unemployment fraud, tax fraud issues (preparation/imposter/etc.)

## Recognize

- Fraudulent charges on your credit card, unauthorized accounts opened in your name, unauthorized use of any personal information, etc.
- Unemployment fraud
- Can cost you time and money and destroy your credit/ruin your good name

## Refuse

- Keep personal and financial information private
- Monitor accounts regularly, check your annual credit report, don't share personal or financial information with unknown callers/entities

## Report

- FTC, [identitytheft.gov](http://identitytheft.gov), CBI, Colorado Dept. of Labor



# Tech Support/Computer Virus



## What's New or Trending

- More aggressive, posing as Norton/McAfee, sending false invoices, greater focus on accessing bank accounts once remote on your computer, attempts to take over phones/other devices

## Recognize

- Unsolicited calls and pop-windows informing you of a computer virus
- Ask for payment and/or access to your computer

## Refuse

- Microsoft or any other major computer company is not going to call you
- Hang up/shut down your computer/contact trusted support
- Avoid future attempts at contact

## Report

- FTC, AG, AARP, ic3.gov, etc.

# Romance/Blackmail



## What's New or Trending

- Fallout from “relationships” during COVID, increasing amount of blackmail scam attempts, greater losses including false investments

## Recognize

- Contacted on a dating site by someone who wants to move the conversation to Facebook, text, email, WhatsApp, etc. Eventually asks for money.
- Contacted on a social media site or app by a stranger who shows interest in you. Eventually asks for money.

## Refuse

- Never send money to someone you have not met in person, no matter how convincing (often an emergency, travel funds, business venture, charity, etc.)

## Report

- Dating site, social media site, ic3.gov, other appropriate authorities



# Payment Methods

- Increase interest in payment with cryptocurrency
  - More accessible
  - Not widely understood
  - Lots “buzz” around it
- Peer-to-Peer (Venmo, Zelle, Cash App)
  - Fast and accessible
  - More comfortable for people
- Gift Cards
- Accessing Bank Accounts Directly



# Communication Methods

- Text Messages
  - Increased usage and accessibility
  - Posing as businesses (phones company, banks, etc.)
- Social Media
  - Widely used by scammers
  - Avoid contact from strangers
- Better Phishing Emails
- Apps with Social Components
  - Words with Friends, Gambling Apps, Games, etc.



# Summary: Ways to Avoid Scams

- Do your own research and conduct independent verification
- Protect your personal and financial information
- Manage your phone calls
- Avoid contact with any unknown entities (it's OK to be skeptical or rude)
- Don't rush to act (THINK!) and talk to others
- Consider unusual payment options a “red flag”
- Be cautious if you are asked to send cryptocurrency
- Does it sound too good to be true?
- Actively seek information about trending scams/fraud
- Report to the authorities!

# Resources

- AARP ElderWatch – 800.222.4444, Option 2  
[www.stopfraudcolorado.gov](http://www.stopfraudcolorado.gov)
- AARP ElderWatch Facebook  
[www.facebook.com/AARPElderWatch](http://www.facebook.com/AARPElderWatch)
- FBI Internet Crime Complaint Center  
[www.ic3.gov](http://www.ic3.gov)
- FTC Identity Theft  
[www.identitytheft.gov](http://www.identitytheft.gov)

# Questions

