



ScamCops  
Your Anti-Scam Force

Advik Atyam



# The Problem

- **2.6 Million** Fraud Reports
- **\$10 Billion** Reported Loss
- **\$7000** Median Loss

**30% increase  
from 2022**

**Older Adults -  
Target for  
impersonation and  
investment fraud  
schemes**

**Cryptocurrency  
payments -  
irreversible  
transactions**



## A Scammy Snapshot of 2023

(based on reports to  
Consumer Sentinel)  
[ftc.gov/data](https://ftc.gov/data)  
[ReportFraud.ftc.gov](https://ReportFraud.ftc.gov)

**REPORT**  
**2.6 million**  
fraud reports

**\$10 billion**  
reported lost

The number of reports  
and the amount lost is up.  
(2022: 2.5 million fraud reports,  
\$9 billion lost)

### ★★★ Reports by Military Consumers ★★★

**Imposters:** Highest # of reports: **42,000**  
Highest total losses: **\$178 million**  
**Investments:** Highest % with loss: **81%**  
Highest median losses: **\$7,000**

Scammers  
contacting people  
by phone or on  
social led to big  
losses.

**Phone calls:**  
Highest **per person**  
reported losses  
**\$1,480**  
median loss

**Social media:**  
Highest **overall**  
reported losses  
**\$1.4 billion**  
total lost

**Email:**  
Highest  
# of reports  
**358,000**  
reports

### Top Payment Methods and Losses

Bank Transfer or Payments	<b>\$1.8 billion</b>
Cryptocurrency	<b>\$1.4 billion</b>
Wire Transfer	<b>\$343.7 million</b>

## Top Frauds







# What is ScamCops?

ScamCops is a 501(c)(3) organization that helps instill knowledge about Scams in local senior homes and community centers.

Create educational information such as:  
Scam Quiz, Ai Chatbot,  
Guide to Scam Awareness

## How Keylogging Works

➔ Hardware-based keyloggers are physical devices that are installed between the keyboard and the computer. They record all keystrokes made on the keyboard and store them on an internal memory chip. The attacker can then retrieve the keylogger and extract the recorded data.

Software-based keyloggers are programs that are installed on a computer or device. They can be installed through various methods, such as downloading a malicious attachment or software from a fake website. Once installed, the keylogger records all keystrokes and sends the data to the attacker's computer or a remote server.

## Types of Keyloggers

There are different types of keyloggers that vary in their level of sophistication and how they operate. Some of these types include:

### Hardware Keyloggers

Hardware keyloggers are physical devices that are attached between the keyboard and the computer. They are small and discreet, making them difficult to detect.



### Software Keyloggers

Software keyloggers are programs that run on a computer or device. They can be disguised as legitimate software, making them difficult to detect.



Advik Atyam · Sep 24, 2023 · 2 min read

## Government Imposter Scams

### How to Spot, Stop, & Report Government Imposter Scams

Consumers reported more than 498,000 imposter scams to the Federal Trade Commission in 2020.

- Nearly 1 in 5 people reported losing money
- Overall, reported losses were nearly \$1.2 billion
- The median loss was \$850
- Almost one-third of the imposter scams reported involved someone posing as a government representative

Image from Century Next Bank

Government imposter scams are a type of fraud in which scammers pretend to be government officials, such as representatives of the Social Security Administration (SSA), the Internal Revenue Service (IRS), or law enforcement agencies, to trick victims into providing personal information or making payments. These scams can take many forms and can be conducted over the phone, through email, or in person.

## How Government Imposter Scams Work

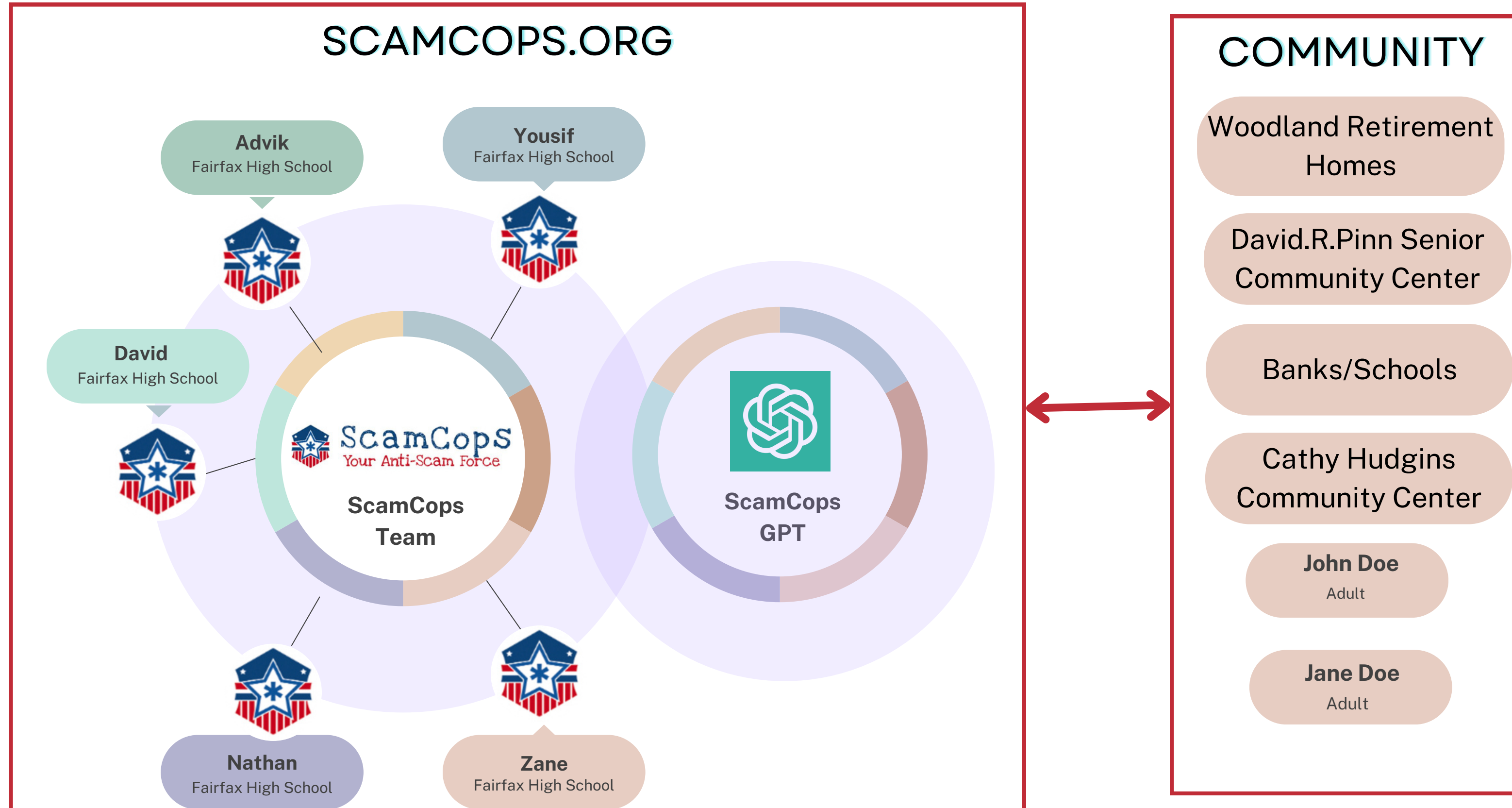
Government imposter scams typically involve the scammer contacting the victim and posing as a government official or law enforcement agent. The scammer may use scare tactics to convince the victim that they are in trouble and need to take immediate action. They may threaten the victim with arrest, fines, or other legal consequences if they do not comply with their demands.

The scammer will then ask the victim to provide personal information, such as their Social Security number, bank account information, or credit card details. They may also ask the victim to make a payment using a prepaid debit card, gift card, or wire transfer. In some cases, the scammer may ask the victim to download and install software that allows them to take control of the victim's computer or access their personal information.

## ## How to Protect Yourself from Government Imposter Scams

Here are some tips to help protect yourself from government imposter scams:

# The Product







ScamCops



OAI-Assistant

ScamCops Custom Assistant

You

Someone is requesting me pay \$1000 in unpaid taxes what should I do?

OAI-Assistant

It's crucial to verify the legitimacy of the request. Scammers often impersonate tax authorities, so contact your local tax office directly using official contact details to confirm if you owe any taxes. Do not provide personal information or payment until you verify the claim.

Scam Confidence Rate: 9/10

Welcome! Avoid scams with me!



Question 1 / 25

**Incorrect**

What should you do if you receive a suspicious email or call?

- ☐ Click on all links to investigate
- ☒ Provide requested information immediately (Your Answer)
- ☐ Verify the sender's legitimacy independently (Correct Answer)
- ☐ Engage in a lengthy conversation

Feedback

- Don't Click or Respond: Do not click on any links, download attachments, or respond to the email or call immediately, especially if it seems suspicious.
- Verify the Sender: Independently verify the identity of the sender or caller. Look up the official contact information for the organization or individual and reach out to them through official channels.
- Check for Red Flags: Be cautious of common red flags, such as a sense of urgency, requests for personal or financial information, poor grammar or spelling, and unsolicited offers.
- Report It: Report the suspicious email or call to relevant authorities or organizations. If it's a phishing attempt, report it to the Anti-Phishing Working Group, the Federal Trade Commission (FTC), or your email provider.

#### How to Protect Yourself from Government Imposter Scams

Here are some tips to help protect yourself from government imposter scams:

##### Know How the Government Operates

Be aware of how the government operates and how they typically communicate with citizens. For example, the SSA will never call or email you to request your Social Security number or ask you to pay money to avoid losing benefits.



##### Don't Provide Personal Information

Never provide personal information, such as your Social Security number, bank account information, or credit card details, unless you are certain of the legitimacy of the request. If you are unsure, hang up and call the government agency directly using a phone number from their official website.



##### Don't Make Payments with Gift Cards or Wire Transfers

Government agencies will never ask you to make a payment using a prepaid debit card, gift card, or wire transfer. If a caller or email asks you to make a payment using one of these methods, it is likely a scam.

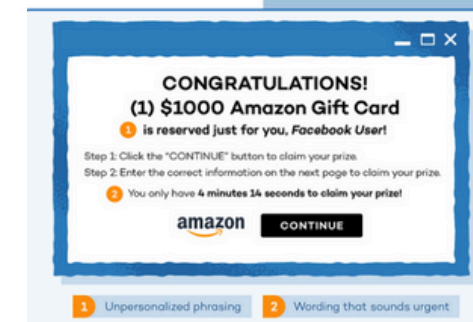


##### Be Wary of Unsolicited Calls or Emails

If you receive an unsolicited call or email from someone claiming to be from a government agency, be cautious. Do not provide personal information or make a payment until you have verified the legitimacy of the request.



#### Door to Door Scams:



Door-to-door scams are fraudulent schemes in which a scammer goes door-to-door, usually targeting elderly or vulnerable individuals, to convince them to purchase fake products or services, or to make a donation to a fake charity. Door-to-door scams can be carried out by a single individual or a group of scammers working together. Here are some common types of door-to-door scams:

##### Home Improvement Scams

Home improvement scams involve a scammer offering to perform home repairs or improvements at a discounted rate. The scammer may claim to be a contractor, but in reality, they may perform shoddy work or use subpar materials. Home improvement scams can also involve advance payment for work that is never completed.

##### Fake Charity Scams

Fake charity scams involve a scammer soliciting donations for a fake charity or non-profit organization. The scammer may use a name that sounds legitimate or may claim to be raising money for a specific cause, such as disaster relief. The donations never reach the intended charity, and the scammer pockets the money.

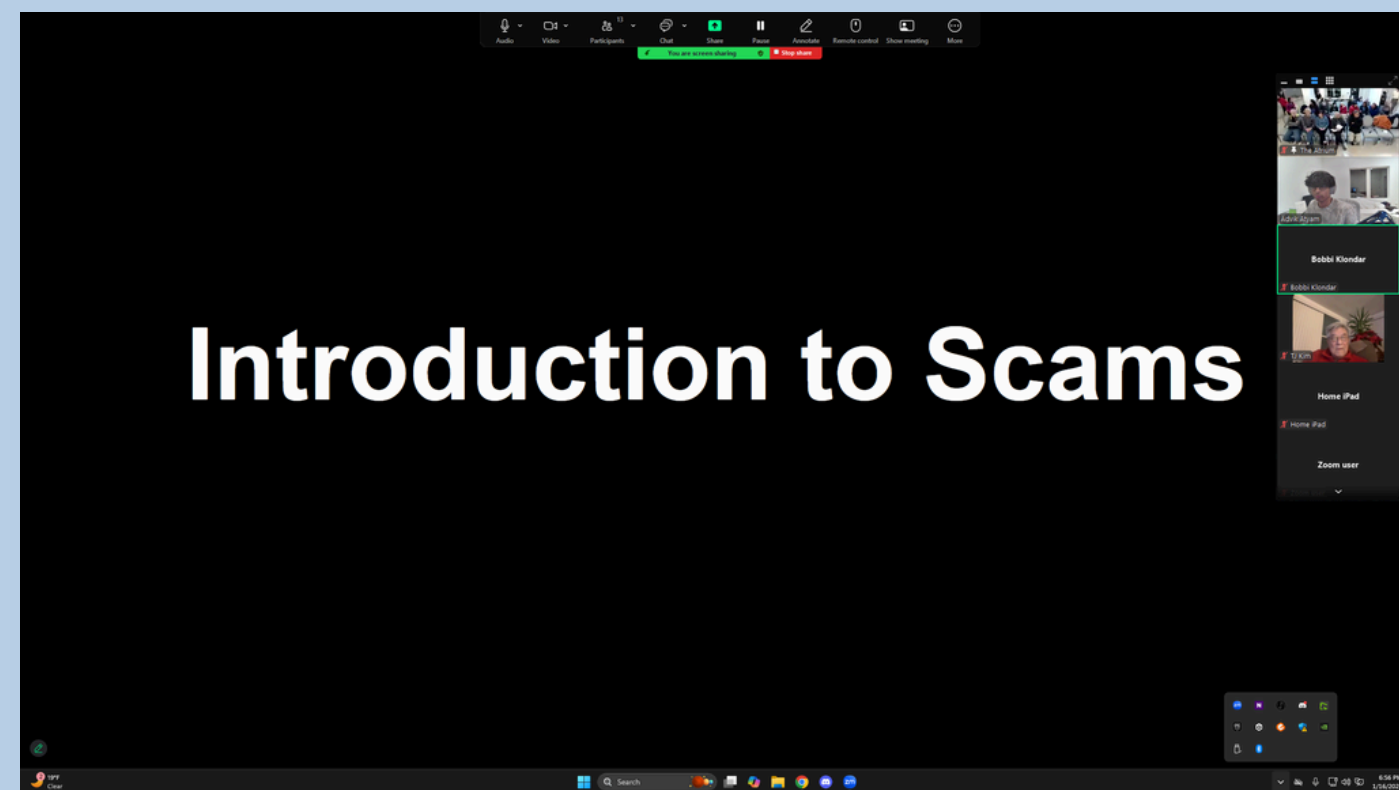
##### Energy Scams

Energy scams involve a scammer claiming to be a representative from a legitimate energy company, offering to save the homeowner money on their energy bill by installing new equipment or making repairs. The scammer may ask for payment upfront or may offer to finance the work at an exorbitant rate.

##### Magazine Subscription Scams

Magazine subscription scams involve a scammer offering magazine subscriptions at a discounted rate. The scammer may claim to be raising money for a school or charity. Once the victim has paid for the subscription, the magazines never arrive, or the subscription is canceled shortly after.

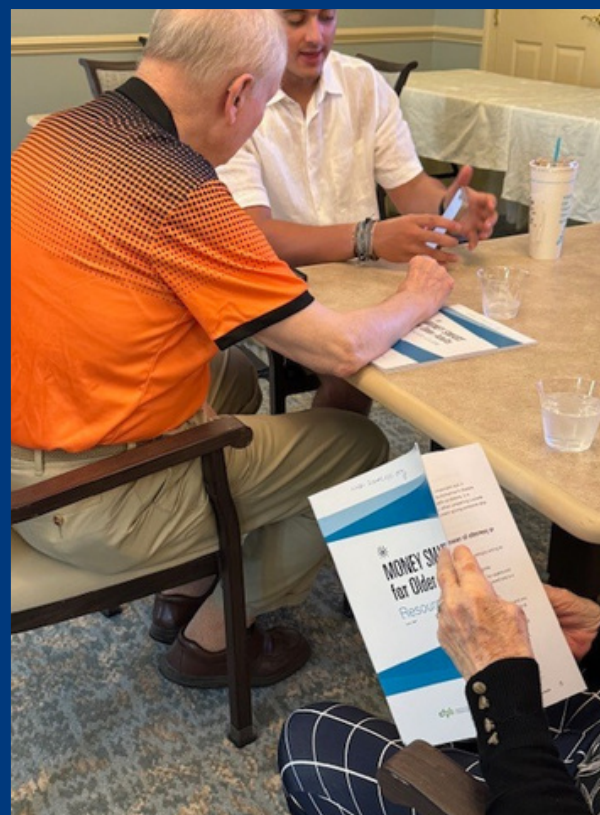
## Online



## In-person









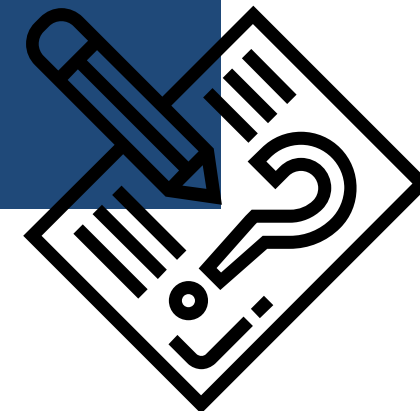
## WEBSITE INTERACTIONS

- Analyzed website data to identify popular content
- Infographics and materials based on insights



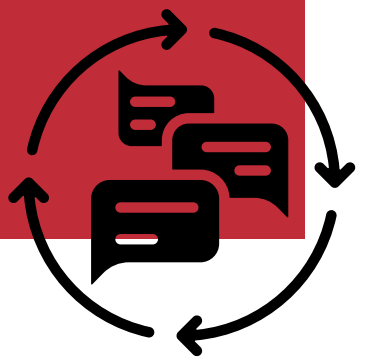
## POST-TEST

- Attendees take a post-test after events to measure understanding.
- Consistent improvement has been observed after each session.
- Results indicate the effectiveness of our project.

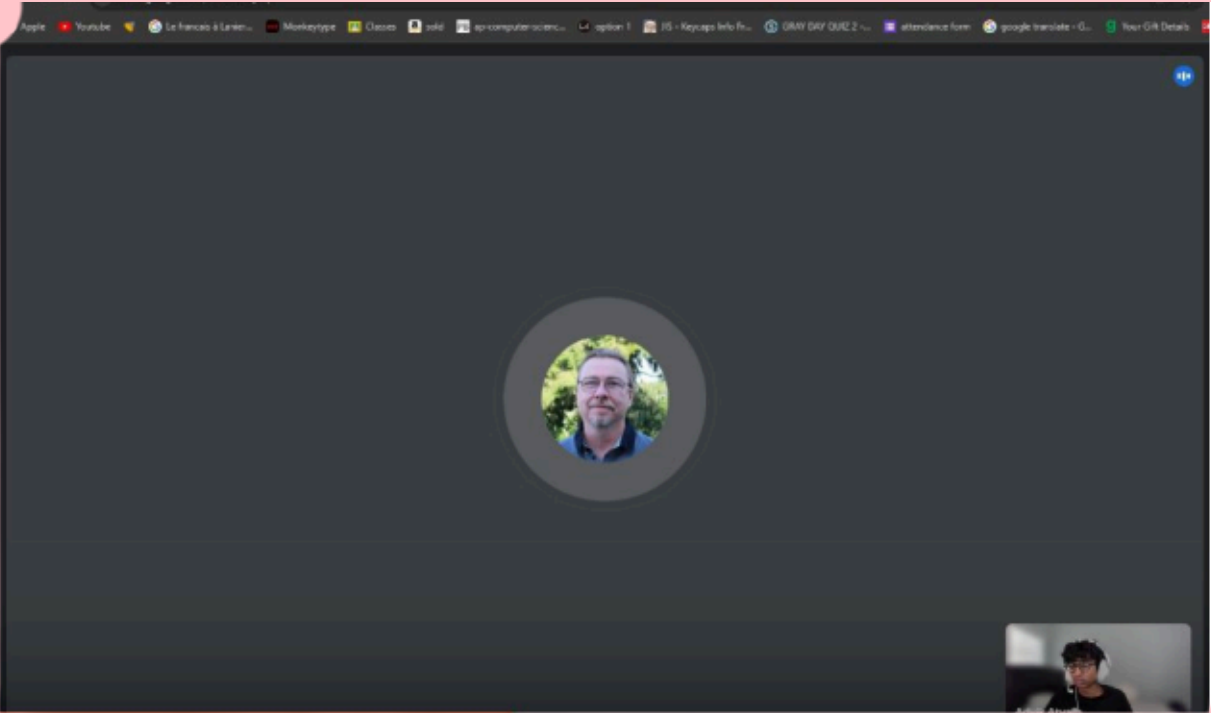
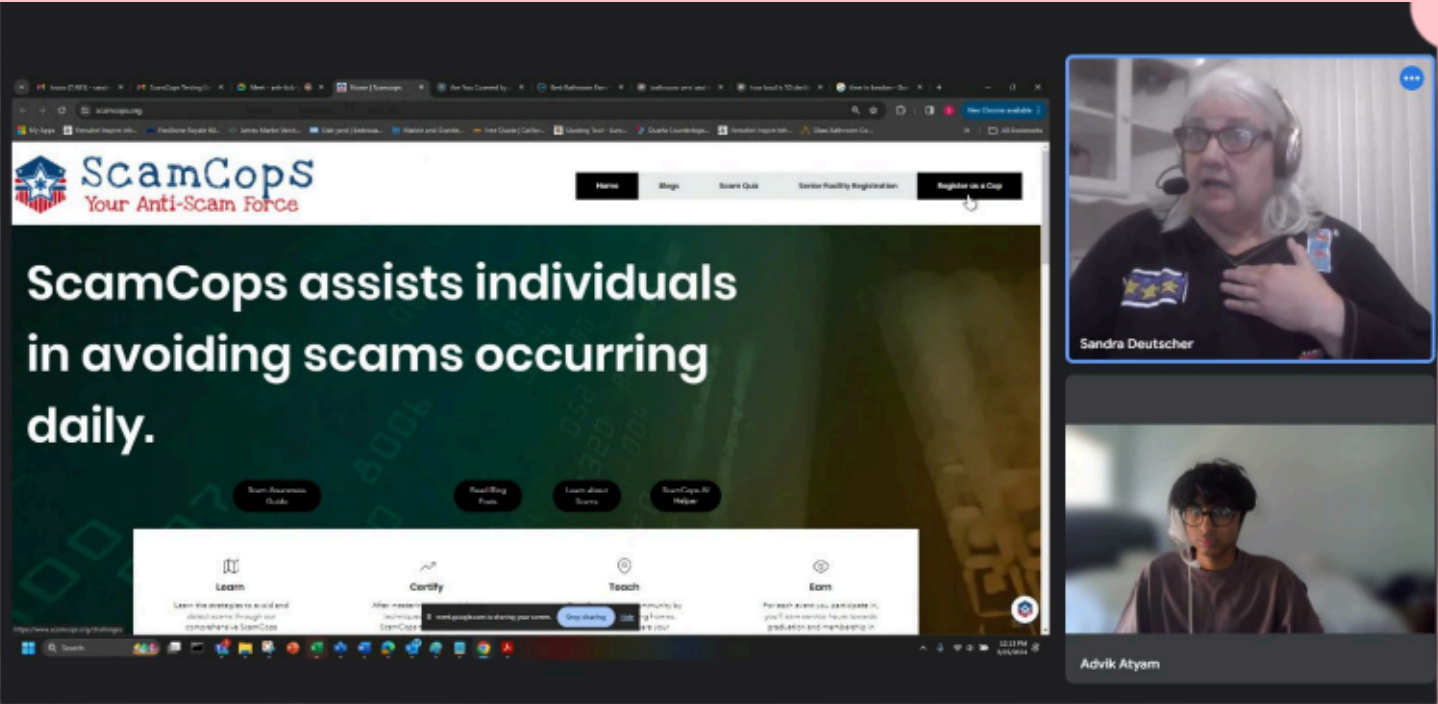


## FEEDBACK

- Feedback is crucial to our project.
- We ask users what they enjoy and dislike
- This helps us ensure a great experience for everyone.



# User Testing - Online and In-Person



Test Video



# USER FEEDBACK

## Pros

“No sign-up required”

“The certification questions prove invaluable in evaluating our understanding of scams.”

“The scam guide can be used as a reference”

“Chatbot and Scam Confidence Rate – This indicator serves as a valuable indicator for gauging the severity of scams”

## Improvements

“Improve the visual experience of Scam Quiz”






















“Seniors requested a more concise quiz.”

“Include videos explaining scams and measures to avoid”





# SCAMCOPS VS. COMPETITION

Features	AARP	FTC	ScamCops
Scam Awareness Content			
Scam Knowledge Assessment			
24/7 AI GPT Chatbot			
Proactive Knowledge Camps			
Downloadable Material			
Volunteer Network			
Age friendly			

# Collaborations



# Cops Training



Completed

Register as a Cop

58%

Overview

Introduction

0/1 steps

Section 1 - Identifying Basic Scams

6/6 steps

Section 2 - How to Avoid Proper Scams

5/6 steps

Section 3 - How to escape a Scam?

2/2 steps

Quiz

0/2 steps

17 Steps

About

This course is designed and created for those who would like to become a cop.

Rewards

You received this program's certificate. [Get Certificate](#)

Instructors



 Advik Atyam

Completed

Register as a Cop

58%

Overview

Introduction

0/1 steps

Introduction

Section 1 - Identifying Basic Scams

6/6 steps

Section 1 - Identifying Basic Scams

Section 1 - Identifying Basic Scams

Step 1: What are Scams?

What is the purpose of Scams?

Example Scenario

Step 2: Too good to be true

"Too good to be True"?

Section 2 - How to Avoid Proper Scams

5/6 steps

Section 2 - How to Avoid Proper Scams

Step 1: How information can affect us

How to Avoid Scam Emails

scamcops.org

CERTIFICATE OF COMPLETION





Proudly presented to

Advik Atyam

This is to certify the successful completion of this program and the fulfillment of all its requirements. The recipient demonstrated dedication and commitment and acquired a wealth of knowledge and skills through the program. May this serve as a testament to their hard work and future success.

Program

Avoid Scams By ScamCops

Completion Date

September 23, 2023

Advik Atyam

President





[Home](#) [Contact Us](#) [Scam Quiz](#) [Senior Facility Registration](#) [Register as a Cop](#) [Blogs](#)

Facility Registration

First name

Last name

Email \*

Message

Address

Submit



## Contact Us

If you are not affiliated with any senior facility, you can reach out to Advik Atyam (Founder) at [advik.atyam@scamcops.org](mailto:advik.atyam@scamcops.org).

For iOS App Support, [support@scamcops.org](mailto:support@scamcops.org)

Contact Us

Scamcops(Forward Thinkers Foundation) is a 501(c)3 charitable organization to work for the greater good; thus, donations are tax deductible



**3000+**

Individuals reached in 36  
countries

**\$5000+**

Protected  
and more

**30+**

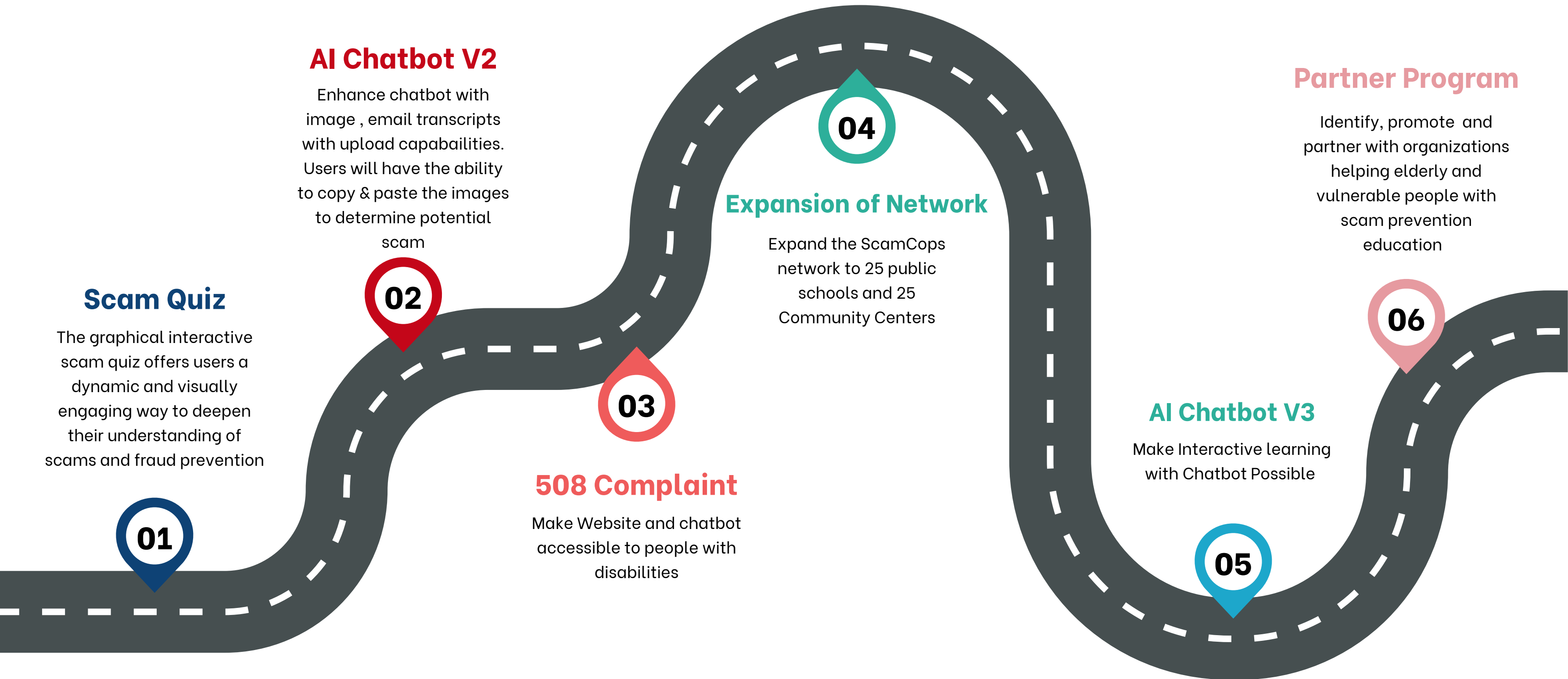
Volunteers  
Recruited

**8**

Retirement Homes  
and Centers

# Community Impact

# Future Enhancements RoadMap





# Achievements



**First Place in Fairfax County  
Shark Tank**



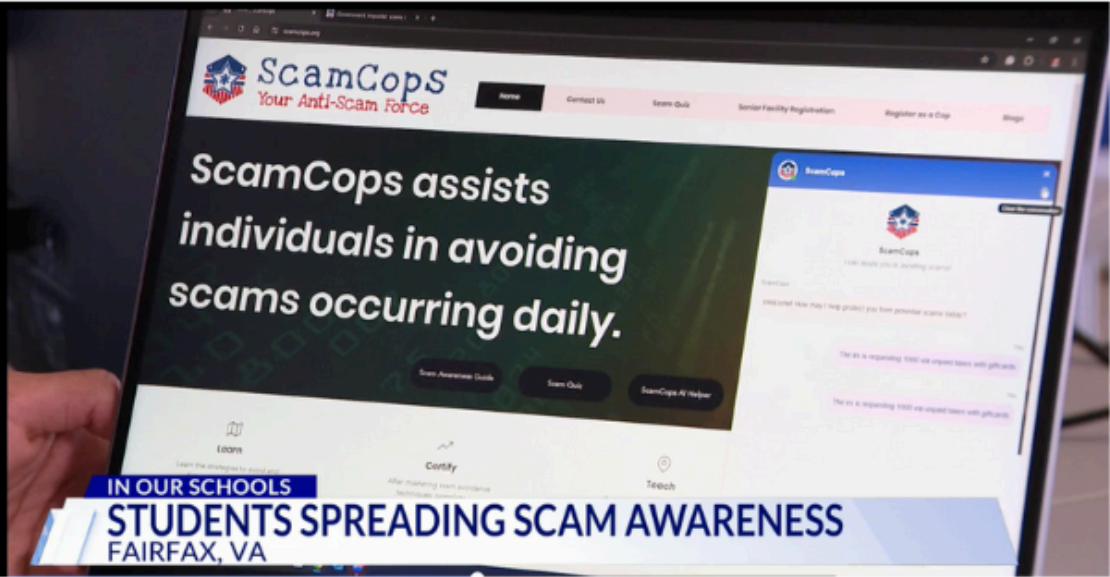
**Featured on WUSA  
Live Studio in  
Georgetown**



**Met Congressman  
Gerry Connelly**



**Featured on WTOP**



**Featured on DC  
News Now**



W

Woodlands Activities <activities@thewoodlandscrc.com>  
to me ▾

Tue, Oct 29, 2024, 9:21 AM ☆ ↶

Hi Advik,

Wow! Time flew by. I hope you enjoyed your summer.

The residents are asking for a smartphone tutorial in December. Do you have availability in December? If so, please let me know what day.

I look forward to hearing from you!

Lisa Smith  
Life Enrichment Department  
The Woodlands Independent Living Community  
4320 Forest Hill Drive  
Fairfax, VA 22030  
(703) 667-9800, X 4032

H

Hernandez-Giblin, Linda <Linda.Hernandez-Giblin@fairfaxcounty.gov>  
to me, To: ▾


Tue, Jul 16, 2024, 11:50 AM ☆ ↶ ⋮

THANK YOU Advik, Yousif and David as well as Sowmya!!! You all did a fabulous job presenting and answering questions! You engaged well with the members! I was so impressed! I hope that some of the connections will lead to many more opportunities. Thanks so much for your willingness to attend this meeting and present.


One of the members, Cherie LeJuene started a FB page for NVAN: (9) Facebook which she and a few others have managed through the years. Would it be OK if she posted the one page from your presentation today? We completely understand if you prefer not posting. We can manage asking her to take it down. She let us know she posted but we want to make sure we have your permission to have it up.

Thank you,

Linda



Linda Hernández-Giblin  
Pronouns: She/Her/Hers  
Legislative Supervisor  
Area Agency on Aging  
12011 Government Center Parkway  
Fairfax, VA 22035



Ken Westbrook <kennethwestbrook@gmail.com>  
to me ▾

Fri, Aug 2, 2024, 2:44 PM ☆ ↶ ⋮

Dear Advik,  
I love what you're doing with Scamcops!

I'm the CEO of Stop Scams Alliance, which is based in Vienna VA. We are a nonprofit that was formed after my mom was scammed. Our motto is "Protecting consumers by stopping scams at the source." We don't focus on education like you do, instead, we focus on preventing the scam phone call, text message, or pop-up ad in the first place.

Check out my website. If it's OK with you, how about if I put your logo on our Members page. You can list me as a supporter on your website, too, if you like.

Best,  
Ken Westbrook  
Founder and CEO, Stop Scams Alliance

Thank you! External Inbox x



demetria lco <denisoulsister612@gmail.com>  
to me ▾

Sat, Aug 24, 2024, 6:01 PM ☆ ↶ ⋮

Hi! My name is Demetria I. from Arlington, VA. I am 72 years old and retired from Fairfax County. I was a victim of a scam 4 times. The first and second was around September 2010-2012. I noticed the unfamiliar amount withdrawal from my paper bank statement. I called my bank (Penfed) and they told me to make a written statement and have it notarized. They returned my money back. I was busy taking care of my ill mother and working with Fairfax County at that time so I did not get a chance to call them back for follow-up.

The third one was on August 21, 2023 (big time hacked) and May 10, 2024 continuation of August 21, 2023 scam. I am sad and embarrassed of what happened to me but I tried to embrace my imperfections. Sometimes I thought about killing myself but I have faith in God and asked all the time for strength to keep moving.

I reached out to the following agencies: FBI, FTC, Police, Atty General, Federal REserve, etc. To date I have not recovered any amount of my big chunk lost.

I'm looking forward to sharing with you what happened to me. I'm hoping you could give me some tips or advice on what else to do to recover even some of my money.

Thank you so much for your help. Stay safe.

Demetria I.  
571-574-2366  
571-641-5977

thank you! External Inbox x



demetria lco <denisoulsister612@gmail.com>  
to me ▾

Thu, Aug 29, 2024, 7:26 AM ☆ ↶ ⋮

Good morning Advik!  
Thank you for the response.I've all your recommendations. The sad part is, I lost the "battle" with PenFed, my bank for 25 years. I just received a 25-year coin from my bank yesterday for being a loyal member.  
Even though a hacker claimed to be an employee of Penfed to make me believe the first time was true then denied it. I wrote a letter to the Chairman of The Board and the CEO/President of the bank but they refused to help me because I initiated the transactions.  
I fully understand and admit I initiated the transactions per Dorothy Barnes (claimed to be an employee of PenFed) and Michael Henderson (claimed to be a Manager of Federal Reserve) advice as to what possibly happened to me. Some have already happened. They strongly warned me that the following would happen if I do not follow their advice: (1) Fear of identity theft (dark web). (2) They informed me that my Social Security, passport and other personal profile were already stolen by scammers and being used by a 12-year old child who is a victim of child trafficking, Scammers got all my personal information from my bank statement when my computer was hacked and being used for child trafficking. (3) Sold my house 612 S. Barton St., Arlington, VA 22204 hurriedly within 4 weeks, according to Dorothy Barnes the FBI will come to interrogate me and might associate me with because according to them my home address was used for child trafficking. (4) Fear of staying with my family, relatives and friends because the FBI will involve them during the investigations and interrogations. (5) Fear of cloning my voice. We seldom talk over the phone because of cloning my voice. (6) Fear of retaliation as the scammers knew where I live including my family and friends. Michael Henderson even told me he would call a law enforcement friend superior to report her/him interfering with investigations of my hacking case.  
And in my journal, I also included the 5 or 6 reasons why I believe (for the first time) Dorothy Barnes is an employee of the bank.  
You were right, the scammers might be just around the corner. She knew everything about me. I'm trying to close my account from PenFed. I'm sure the scammers know that I opened a new account. She knows where.

Have a good Advik. Stay safe.

As always,  
Demetria

# End Statement

"The most effective safeguard against falling victim to scams is prevention."

## SCAMMER'S TOOLS

Fear and Urgency  
Vulnerable Adults  
Impersonation  
Untraceable Money Transfers  
Cryptocurrency  
Gift Cards

## SCAMCOPS TOOLS

Prevention  
Knowledge and Education  
Awareness  
Constant Dialogue  
24/7 Help  
Artificial Intelligence  
Community Outreach

