



Cybersecurity for Seniors: Protecting Our Elderly

Presented by:

Shriyanka Hiremagalur

Senior, Notre Dame High School, San Jose

Aarini Naskar

Senior, Notre Dame High School, San Jose

Sahana Shyam

Junior, Notre Dame High School, San Jose

FBI RELEASE INFOGRAPHIC ON DEEPFAKE SCAMS

DEEPFAKE MEDIA SCAMS

Scams targeting Americans are surging.



Since 2020, the FBI has received
4.2 million+ reports of fraud.
That's **\$50.5 billion in losses.**



Imposter scams in particular are on the rise in the age of artificial intelligence (AI). Criminals are using deepfakes, or media that is generated or manipulated by AI, to gain your trust and scam you out of your hard-earned money.

Deepfakes can be altered images, videos or audio. They may depict people you know — including friends and family — or public figures including celebrities, government officials and law enforcement.

FBI RELEASE INFOGRAPHIC ON DEEPFAKE SCAMS

HOW TO DETECT A DEEPFAKE



LOOK FOR INCONSISTENCIES:

- Are any of the facial features blurry or distorted?
- Does the person blink too much or too little?
- Do the hair and teeth look real?
- Are the audio and video out of sync?
- Is the voice tone flat or unnatural?
- Does the visual show odd or unnatural shadows or lighting?

RED FLAGS OF A DEEPPFAKE SCAM



Unexpected requests for money, passwords, personal information or secrecy.



Emotional manipulation involving fear or urgency.



Uncharacteristic communication from someone you know, especially over text, phone or video.

REPORT SCAMS



To **your** local police



To the **FBI** at **IC3.Gov**



To **your bank** if you sent money

FBI ALERT: SCAMMERS IMPERSONATING AGENCY'S CYBER-CRIMES WEBSITE

- Scammers are spoofing the website of the agency's Internet Crime Complaint Center, or IC3, to trick consumers into turning over financial information.
- A spoofed website is designed to impersonate a legitimate website and may be used for personal information theft and facilitating monetary scams.



TIPS TO AVOID THIS SCAM

- ❑ The FBI recommended that consumers type the IC3's web address – www.ic3.gov – directly into their browser address bar to ensure they are going to the correct address.
- ❑ The agency recommended against clicking on “sponsored” results in web searches for the IC3 as those may be spoofed sites, and instead to check that the address ends in “.gov” and matches the IC3 address.
- ❑ Potential victims should report any interactions with websites or individuals impersonating IC3 to their local FBI field office or the IC3 through its official web address, the agency said.



FEDERAL TRADE COMMISSION (FTC) WARNS CONSUMERS ABOUT SOCIAL MEDIA CHECK FRAUD SCAM

Social media posts sharing an alleged checking account “hack” is actually a scam that could lead to financial and legal trouble.

How it works:

- ❑ The supposed hack involves writing a check for more money than you have, depositing it into a different account of yours, and then withdrawing the money before the (bad) check is fully processed.
- ❑ What the video or post might not tell you is that could leave you on the hook for paying back all the money, kicked out of your bank, and in serious legal trouble for bank fraud.



TIPS TO AVOID THIS SCAM:

Before you jump onboard a viral trend:

- **Do some research.** Search the trend along with terms like “scam” or “fraud” to see what others are saying about it. Talk to friends and family to see what they think.
- **Think about the source.** What do you know about the person or account that makes them trustworthy?
- **Compare advice from a variety of well-known sources.** Don’t just trust what one person or account says.

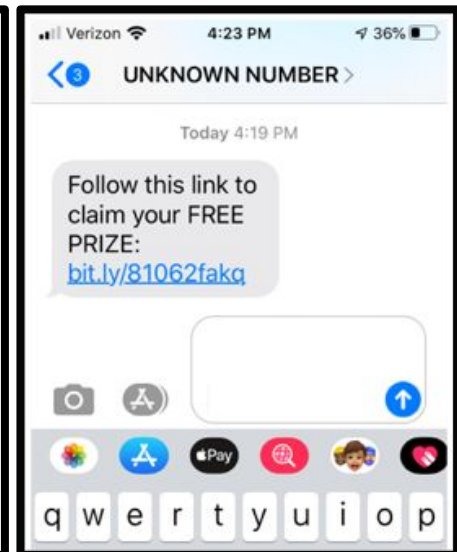
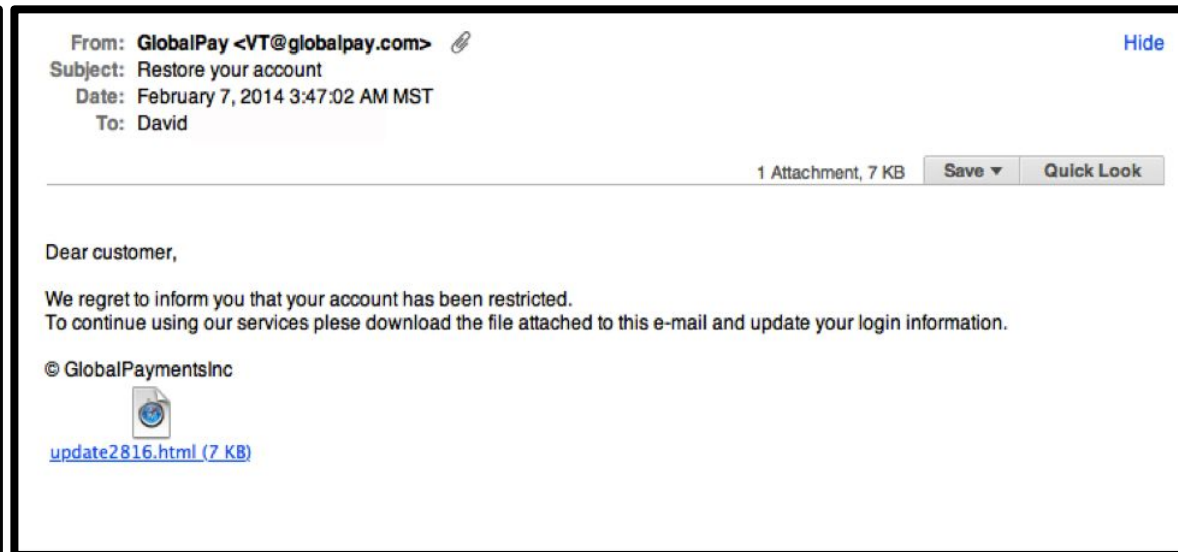
What is Cybersecurity?



Cybersecurity is the practice of protecting internet-connected systems, including hardware, software, and data, from digital attacks and unauthorized access.

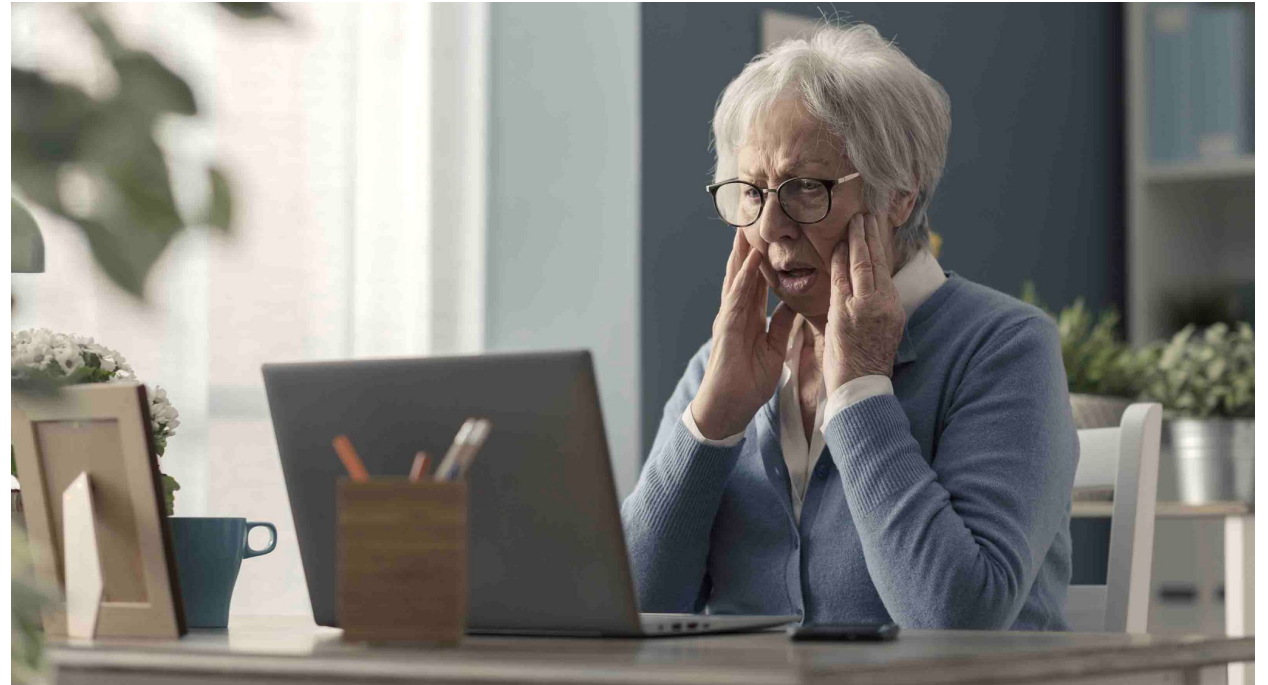
Please note: The cybersecurity tips provided in this presentation is intended to be informative and helpful, but it is not a substitute for professional advice or guidance.

Question: How many of you here have received a suspicious phone call, email or text?



Why Are Elders Targeted?

- More likely to have more money.
- May hesitate to report scams for fear of losing their independence.
- Often perceived as not tech-savvy, making them easy targets for phone and social media scams.
- May have cognitive or physical impairments that hinder their judgment.





Losses to Seniors from Cyber Crimes in 2023



TDM	729.89	915.51	185.62	▲25.43%	FLR	660.27	745.28	85.01	▲12.88%
HUM	749.73	924.29	174.56	▲23.28%	UVD	155.59	181.57	25.98	▲16.70%
DMW	833.72	1004.01	170.29	▲20.43%	QUV	440.55	540.21	99.66	▲22.62%
YZJ	903.49	1127.46	223.97	▲24.79%	HZT	285.51	344.98	59.47	▲20.83%
GLY	982.07	1219.39	237.32	▲24.17%	PCW	811.44	1029.66	218.22	▲26.89%
VDA	113.74	143.41	29.67	▲26.09%	AIK	361.77	451.39	89.62	▲24.77%
UVV	468.08	535.41	67.33	▲14.38%	ZJJ	858.36	994.57	136.21	▲15.87%
HJS	545.49	659.05	113.56	▲20.82%	RHJ	894.79	1046.68	151.89	▲16.97%
EQC	556.96	664.69	97.73	▲17.24%	VGV	425.08	509.95	84.87	▲19.97%

PPJ	912.63	1038.36	125.73	▲13.78%	ZGK	391.59	491.48	99.89	▲25.51%
UAQ	1309.55	1655.62	346.07	▲26.43%	BNY	969.21	1130.65	161.44	▲16.66%
DAQ	1295.17	1641.66	346.49	▲26.75%	SDM	735.44	913.39	177.95	▲24.20%
PNR	654.33	775.84	121.51	▲18.57%	TQQ	1323.91	1646.42	322.51	▲24.36%
ZTM	1111.11	1377.78	266.67	▲23.96%	OIS	543.42	667.91	124.49	▲22.73%

**Which State do you think
has the highest number of
complaints/loss reported
by individuals over 60?**

Tops Losses by State:

2023 OVERALL STATE STATISTICS, COM

COMPLAINTS FILED BY INDIVIDUALS OVER 60

Rank	State	Loss	Re
1	California	\$643,230,534	3
2	Florida	\$293,817,911	3
3	Texas	\$278,320,107	3
4	New York	\$203,437,635	3
5	Illinois	\$137,940,620	3
6	Arizona	\$127,977,700	3
7	Pennsylvania	\$117,427,238	3
8	New Jersey	\$104,087,085	3
9	Virginia	\$94,037,054	3
10	Georgia	\$92,422,609	3

Top Complaints by State:

2023 OVERALL STATE STATISTICS

COMPLAINTS FILED BY INDIVIDUALS OVER 60

Rank	State	Count
1	California	11,622
2	Florida	8,138
3	Texas	7,035
4	Arizona	5,003
5	New York	4,328
6	Ohio	3,299
7	Pennsylvania	3,020
8	Colorado	2,905
9	Illinois	2,887
10	Washington	2,873

**What are some
of the most
prevalent fraud
scams
affecting the
elderly?**



**Let's watch this short video
from Federal Trade
Commission:**

IRS Imposter Scams | Federal
Trade Commission (ftc.gov)

Common Government Impersonation Scams

1. IRS imposter Scams

2. Medicare Imposter Scams

3. Social Security Administration Imposter Scams



IRS IMPOSTER SCAM:



- ☐ You receive a call or voicemail warning that authorities will arrest you if you don't pay money owed to the IRS.
- ☐ The caller claims you have unpaid taxes and threatens jail time or other penalties.
- ☐ They may demand immediate payment to avoid arrest or legal action.
- ☐ Scammers often use caller ID spoofing to appear legitimate.
- ☐ **The IRS will never contact you by phone for immediate payment; they always send written notifications first.**

MEDICARE IMPOSTER SCAM

Scammers **call, email, text, or send social media messages** claiming to:

- ☐ “alert” you that your new Medicare benefits card is ready.
- ☐ offering to help you sign up for or change your plan.
- ☐ that you’re eligible for a medical device you didn’t realize you needed.



SOCIAL SECURITY ADMINISTRATION IMPOSTER SCAMS

You get a call, email, text, or social media message warning that:

- ☐ your Social Security benefits are about to expire.

OR

- ☐ that they will be suspended because you owe money for a reason you previously weren't aware of.





Please Remember:

"If someone you don't know immediately starts pressuring you—on the phone, in a text, or another way—that's a **"HUGE RED FLAG"**

Common Tactics that Indicate a Scam:

**Establishing
Credibility**

Building Rapport

Threatening You

**Demanding
Payment**

**Never trust the
number on your
caller ID, or the
email address in
your inbox**

How do I Avoid Government Imposter Scams?

Hang up

Whether you recognize the number on the caller ID or not, immediately end any call from someone you don't know.

Delete

Even if the sender's address appears to be from a government agency, don't open it. Instead, send it directly to your Trash folder.

Ignore

If you receive a text or direct message on social media from the IRS, SSA, Medicare, FTC, or other government account, don't reply.

REMEMBER...

Be proactive

If you're concerned that a government agency is legitimately trying to reach you, be proactive.

Look up

Look up the agency's contact information yourself (go to their official website)

Don't rely on

Don't rely on your caller ID or an email you received) and get in touch that way.

What Should I Do if I've Been Scammed by a Government Imposter?

- Report what happened. You may call the **National Elder Fraud Hotline** at 833-FRAUD-11 (833-372-831)
- Alert the Federal Trade Commission (FTC) **online** or by phone at 877-FTC-HELP (877-382-4357).
- Finally, if criminals got their hands on your personal information, your money, or both, the **FTC offers step-by-step advice** on what to do.



Please note:

If the IRS, Social Security Administration, Medicare, or other government agency needs you,
they'll send a letter.

Sweepstake/Lottery Scams



You must pay to claim your prize.



Scammers claim – paying will increase odds of winning.



Asking for financial information.



Scammers will send a fake check and ask you to send some of the money back.



Scammers pressurize you to “act now” to claim the prize.



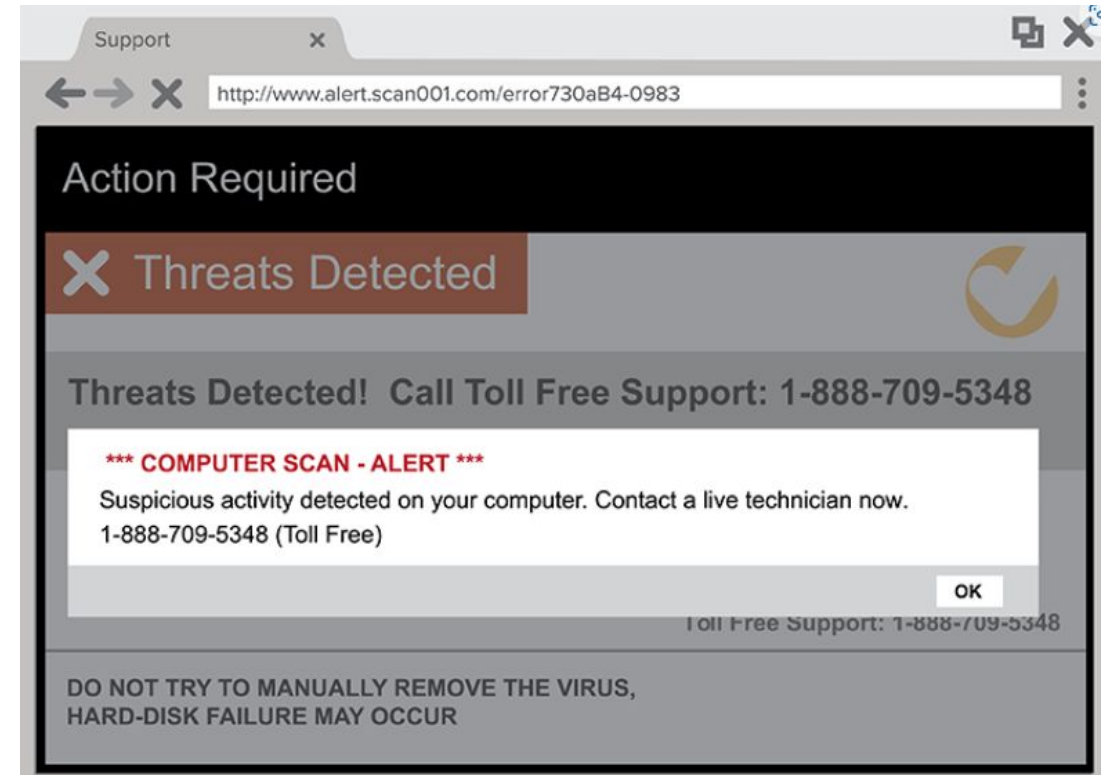
Prevention Tips

Approach	Approach unexpected prize claims with skepticism.
Verify	Verify Legitimacy of the lottery or sweepstake organization independently.
Consult	Consult the organization's website or published information, not the message from the sender.
Don't share	Don't share Personal/Financial Information with unsolicited contacts.
Do not send	Do not send money or make payments to claim a prize.

Tech-Support Scam

Tech support scammers use many different scare tactics to **trick** you into **unnecessary** technical support services to supposedly fix device or software problems that doesn't exist as follows:

- Phone calls
- Pop-up warnings on the computer
- Online ads and listings in search results pages



How to recognize a Tech-Support Scam

Fake security pop up messages asking to call a number

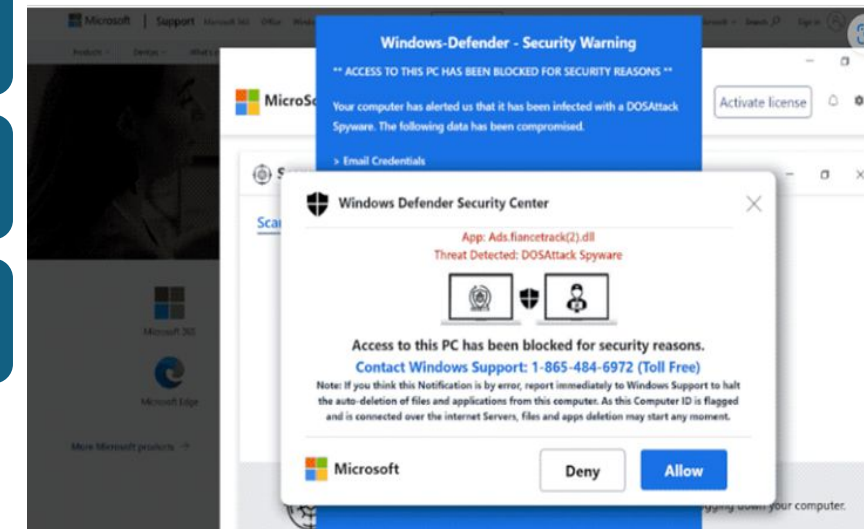
Unsolicited phone calls

Suspicious emails/text messages with malicious links

Requesting remote access

Creating a sense of urgency

Requesting immediate payments



Prevention Tips

Do not click

- Do not click any links or call a number that pops up on your screen warning of a computer problem.

Hang up

- Hang up on unexpected calls from anyone who claims to be tech support.

Don't believe

- Don't believe your caller ID – it can be easily spoofed.

Never Give

- Never give control of your computer or share passwords/ financial information with anyone who contacts you.

Keep

- Keep your security software up to date.

Contact

- If you need help, contact a computer technician that you trust. Don't just rely on an online search.



Romance/Sweetheart Scam

- ❑ Criminals pose as interested romantic partners on social media or dating websites.
- ❑ Establish a romantic relationship, eventually asking for money.
- ❑ This could also be confidence scams luring a victim to be a good friend.



How to Recognize a Romance/ Sweetheart Scam



A stranger
approaching you
online

Establishing a
close connection
very quickly
(texts, emails and
phone calls).

Asking for money
in small amounts
at first, and for
seemingly honest
reasons.

Hesitant to meet
in person.

Requesting
money through
untraceable and
unregulated
money transfers
(gift cards,
money orders,
Cryptocurrency,
cash transfer
apps like Zelle,
Venmo and
CashApp)

Odd/poor use of
grammar and
slang that native
English speakers
will not use.



**NEW: AI PHANTOM
HACKER SCAM**

AI PHANTOM HACKER SCAM

Scam happens in the following three ways:

1. Using AI-powered social eng.
2. Caller ID spoofing
3. **Deepfake voices** for impersonation

How AI is Involved: Deepfake voices are recreated from brief audio samples to impersonate real officials, and there are also AI-generated scripts to craft realistic emails, messages, etc.



Prevention Tips

Ask	*Ask questions, spot inconsistencies that might reveal an imposter.
Discuss	*Discuss your new love interest with family and friends; heed their concerns.
Be wary	*Be wary of flirtatious and overly complimentary emails.
Cut Contact	*If suspecting a swindler, cut contact immediately.
Report	*Report the scammer to the dating platform.
Stay	*Stay cautious even if you initiate contact; scammers lurk everywhere.
Share	*Share minimal personal info in your dating profile or online chats.
Never Send	*Never send money or gift cards to online-only contacts.

Question: If you think you are a victim of an online scam or cyberattack, what do you need to do?

- ❑ Be vocal.
- ❑ Don't feel embarrassed about what happened.
- ❑ Report the incident to **Internet Crime Center (IC3) at the "Internet Crime Complaint (IC3)" Home Page**, the Federal Bureau of Investigation (FBI) nearest field office using the **Electronic Tip Form**, and **Federal Trade Commission (FTC)**.
- ❑ Contact your local law enforcement agency to file a report and notify your financial institutions.
- ❑ Install a trusted antivirus software on your computer and update it on a regular basis.

Thank You!

