



*Keeping
Seniors
Safe*



MONTGOMERY COUNTY DEPARTMENT OF POLICE

**WALTER HOUSER
FINANCIAL CRIMES SECTION
VOLUNTEER**

A SCAM NEAR YOU

2



HOW CAN THIS HAPPEN?

4

- What are the three most dangerous devices in your home?
- Who gets a lot of phone calls from unknown callers?
- Who gets a lot of email?
- Who gets a lot of text messages?
- Who shops online?
- Who banks or invests online?
- Who uses social media?

TOPICS

5

- What are the Numbers?
- Frauds and Scams
- Identity Theft
- Questions

WHAT ARE THE NUMBERS?

7

**Younger people
reported losing
money to fraud
more often than
older people.**

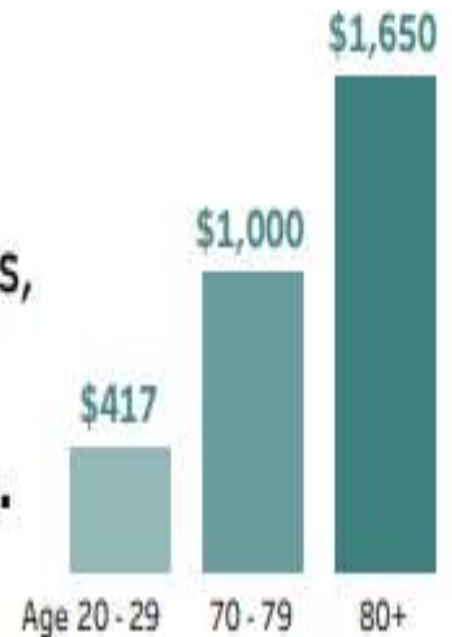


Age 20-29



Age 70-79

**But when people
aged 70+ had a loss,
the median loss
was much higher.**



2024 FTC Consumer Sentinel Network at www.FTC.gov/Sentinel

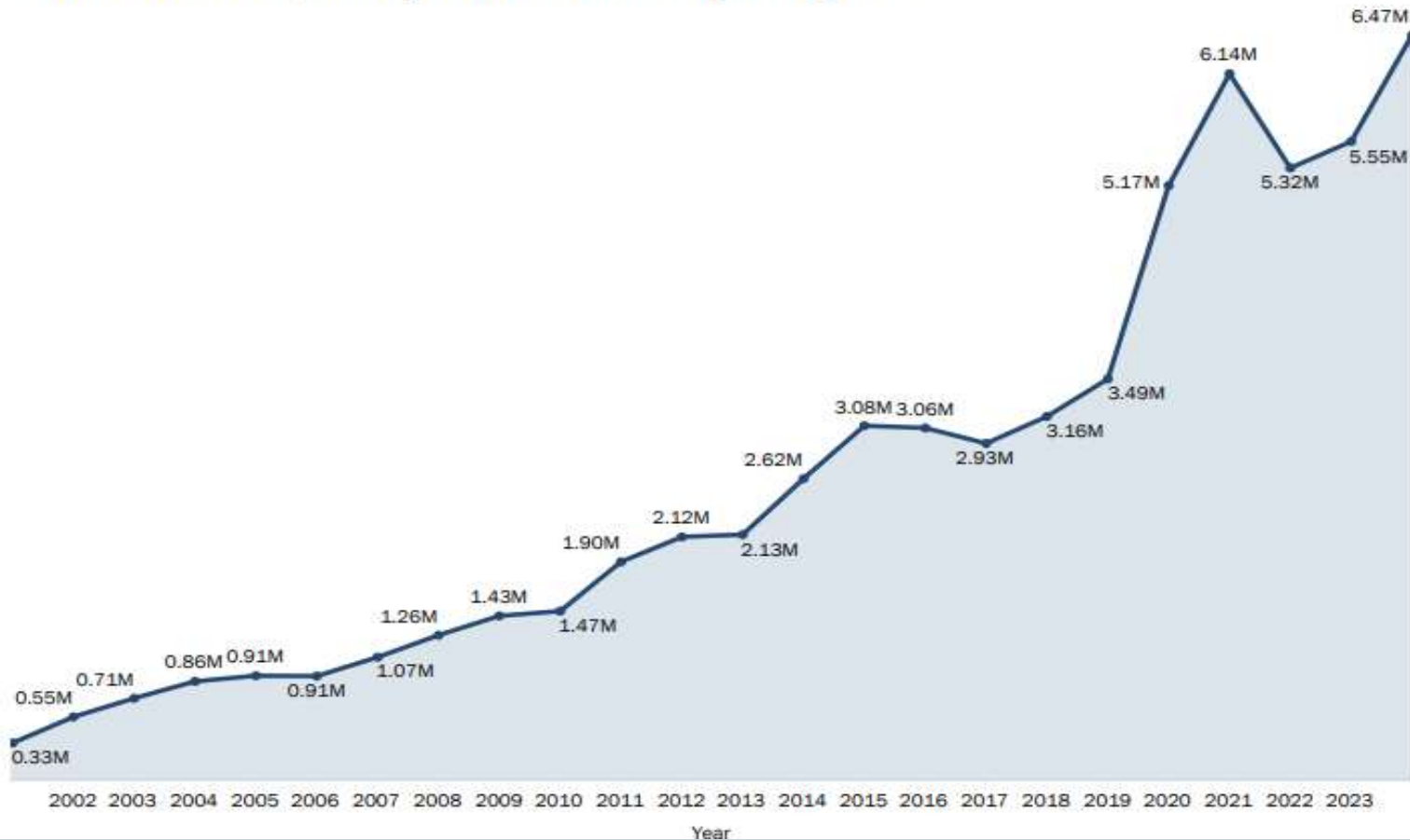
WHAT ARE THE NUMBERS?

9

CONSUMER SENTINEL NETWORK

DATA BOOK 2024

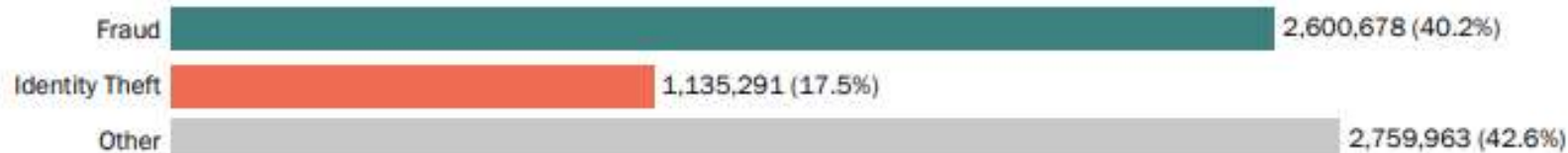
Number of Fraud, Identity Theft and Other Reports by Year



WHAT ARE THE NUMBERS?

10

Report Type



Top 10 Fraud Categories

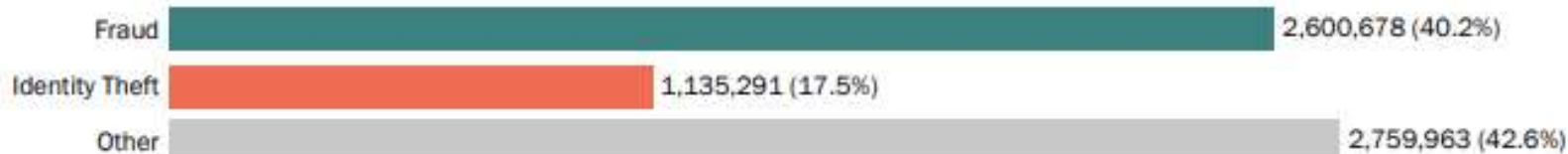
Rank	Category	# of Reports	% Reporting \$ Loss	Total \$ Loss	Median \$ Loss
1	Imposter Scams	845,806	22%	\$2,952M	\$800
2	Online Shopping and Negative Reviews	383,441	76%	\$432M	\$130
3	Business and Job Opportunities	126,217	36%	\$751M	\$2,250
4	Investment Related	118,960	79%	\$5,697M	\$9,196
5	Internet Services	118,261	28%	\$164M	\$300
6	Prizes, Sweepstakes and Lotteries	97,350	22%	\$351M	\$1,000
7	Telephone and Mobile Services	92,520	39%	\$56M	\$240
8	Health Care	78,763	51%	\$80M	\$283
9	Travel, Vacations and Timeshare Plans	58,347	67%	\$274M	\$922
10	Mortgage Foreclosure Relief and Debt Management	34,159	21%	\$82M	\$1,500

2024 FTC Consumer Sentinel Network at www.FTC.gov/Sentinel

WHAT ARE THE NUMBERS?

11

Report Type



Identity Theft Types

Rank	Theft Type	# of Reports
1	Credit Card	449,032
2	Other Identity Theft	358,993
3	Loan or Lease	176,400
4	Bank Account	114,608
5	Employment or Tax-Related	87,470
6	Phone or Utilities	82,626
7	Government Documents or Benefits	70,332

WHAT ARE THE NUMBERS?

12

Number of Reports and Amount Lost by Contact Method

Contact Method	# of Reports	Total \$ Lost	Median \$ Lost
Email	371,651	\$502M	\$600
Phone call	284,659	\$948M	\$1,500
Text	246,784	\$470M	\$1,000
Social Media	186,826	\$1,858M	\$409
Website or Apps	186,663	\$976M	\$200
Other	148,288	\$1,072M	\$633
Mail	42,108	\$90M	\$990
Online Ad or Pop-up	42,023	\$246M	\$180

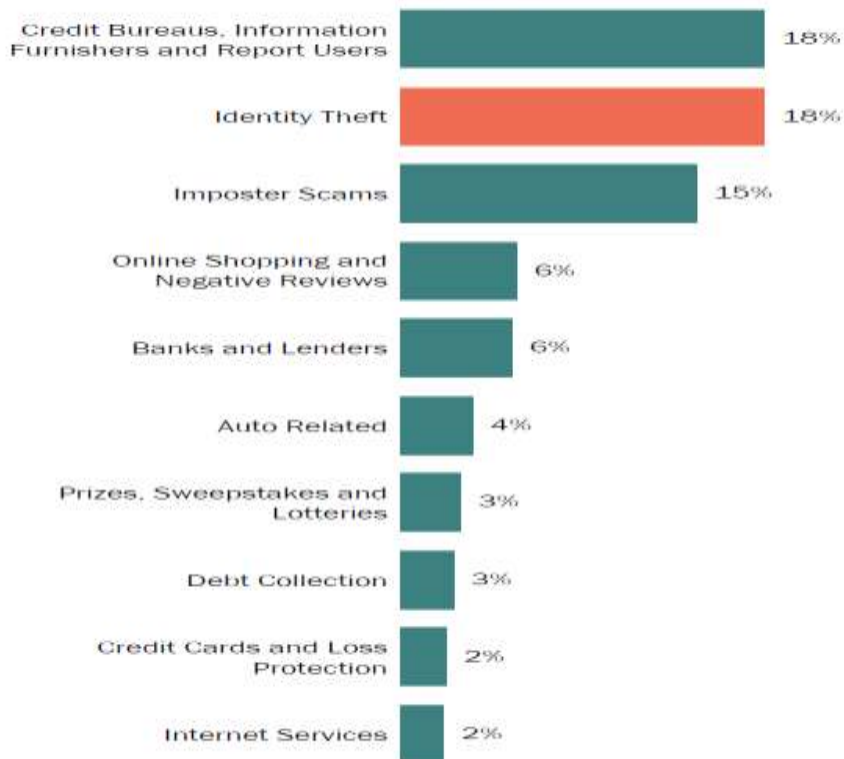
2024 FTC Consumer Sentinel Network at www.FTC.gov/Sentinel

WHAT ARE THE NUMBERS?

13

Maryland

Top Ten Report Categories



2024 FTC Consumer Sentinel Network at www.FTC.gov/Sentinel

Financial Crimes Section

1/28/2026

WHAT ARE THE NUMBERS?

14

Rank	State	Reports per 100K Population	# of Reports
1	Florida	2,163	474,314
2	Georgia	2,108	228,132
3	Delaware	1,876	18,870
4	Nevada	1,867	58,640
5	Maryland	1,799	111,041
6	Texas	1,561	462,667
7	South Carolina	1,536	80,070
8	New Jersey	1,506	139,551
9	Louisiana	1,472	68,025
10	Illinois	1,469	186,426

2024 FTC Consumer Sentinel Network at www.FTC.gov/Sentinel

COMMON PRACTICES

15

- ✓ Urgency – “Act now or your account will be closed.”
- ✓ Fear – Arrest threats, tax penalties, hacked accounts.
- ✓ Authority impersonation – Police, IRS, banks, Microsoft, Amazon.
- ✓ Trust building – Friendly chat, empathy, flattery.
- ✓ Scarcity – “Only one spot left,” “offer expires soon.”
- ✓ Reciprocity – Send you a small “refund” or “bonus” first.
- ✓ Secrecy – “Don’t tell anyone it’s confidential.”

IMPOSTER SCAMS

18

IRS, SSA, FTC, CMS, and other government agencies will initiate contact only in person or in writing.

Gov't agencies will not:

- Call you (out of the “blue”)
- Threaten to send “local cops”
- Ask for payment in gift cards
- Tell you to send money to a third party



IMPOSTER SCAMS

20



- Unsolicited Calls from “Big Tech.”
 - Pop-Up Messages.
 - Fake Websites.
 - Pressure to Act Quickly.
 - Request for Remote Access.
-
- Say No! Hang up!
 - Disconnect the internet.
 - Scan for malware.
 - More at this MCPD QR Code:



ADVANCED FEE/FAKE CHECK

25



CHARITY SCAMS

26

- ✓ Don't be pressured.
- ✓ Don't give info over the phone.
- ✓ Verify that the charity is legit.
- ✓ Do they contract out for fundraising?
- ✓ What percentage raised goes to the recipient?
- ✓ Pay the organization directly with a check or credit card, not gift card, Venmo, Zelle.
- ✓ IRS, BBB Wise Giving Alliance, Charity Navigator, CharityWatch, and GuideStar



ROMANCE SCAMS

27



INVESTMENT FRAUD

28

When considering investment opportunities

- ✓ Verify credentials and licenses.
- ✓ Meet at their office.



- ✓ Understand how they make their money.
- ✓ Are they fiduciary agents?

PHISHING EMAILS

29



Order Confirmation
1 message

Norton-BILLING-TEAM
To: walthouser@gmail.com

Dear walter h

Thank you for connecting
computer security &

Congratulations, you
You have been charged
via Debit/credit card
Kindly reach us im

Norton account :- w

INVOICE ID: #46-78

Description
McAfee Anti-Virus P
Service

This Deduction will
Your order no/Refer
If you have any que

Note- This is a sys
(803) - 233 - 0731



walthouser@gmail.com>

Oct 14, 2021 at 1:32 PM

r membership for your

ship .
n your bank account,

mt.
0

\$9.00

) - 233 - 0731

Customer care.+1

GARY@GARYMCCOY.ORG 12/17 © 2019 Glenn and Gary McCoy/Dist. by Andrews McMeel Syndication

30

to me ▼


<thanhthuy.13091980@gmail.com>

date: Jun 25, 2025, 1:54 PM

mailing list: <ab2a3ccda80e0b4aef15451261ca6944cb5ea@winon.com> **WINON IS LIMITED!**

[Filter messages from this mailing list](#)

signed-by: gmail.com

security:  Standard encryption (TLS) [Learn more](#)

➤: Important according to Google magic.

LIMITED STATEFARM OFFER

GET IT NOW

PHISHING EMAILS

31

Receipt #DHR130



HELP DESK <zampavdc4573@gmail.com>

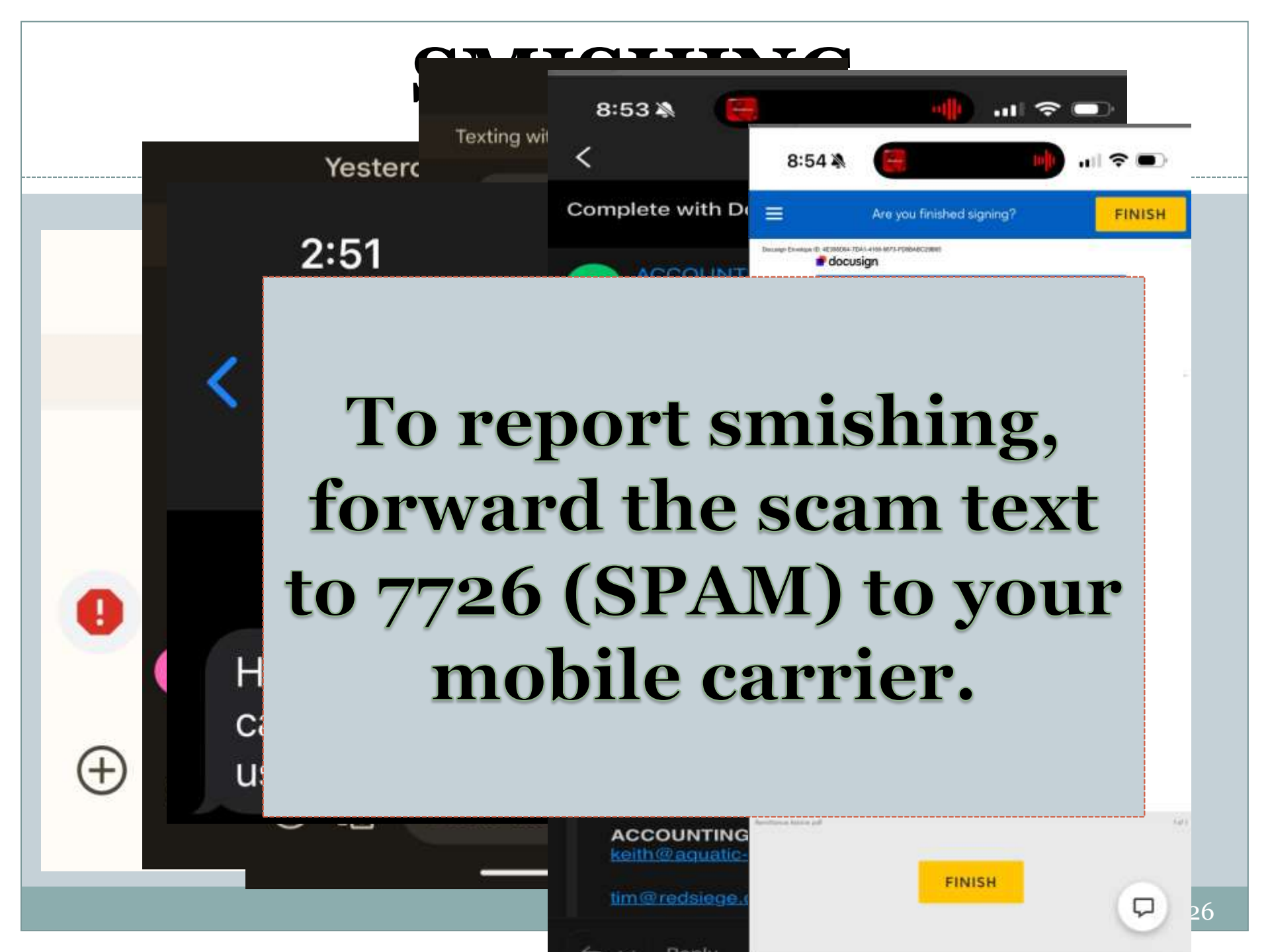
to walkerhalhfbh, bcc: me



← Reply

↩ Reply all

→ Forward



The background features a collage of several smartphone screens. One screen shows a text conversation with a blue arrow icon and a red octagonal warning icon. Another screen displays a 'Complete with DocuSign' message. A third screen shows a 'docusign' email signature. A fourth screen at the bottom right has a yellow 'FINISH' button. The overall theme is mobile communication and security.

**To report smishing,
forward the scam text
to 7726 (SPAM) to your
mobile carrier.**

QUISHING

35



- If the edges aren't sharp and precise, it might be fake.
- Run your fingernail across the QR code. If there's a detectable edge or thickness, it could be hiding the legitimate sticker.
- If the QR code lifts away from the surface, don't use it.

DON'T STEAL THE MAIL

38



FRAUD: ATM SKIMMING

40

- Skimmers
 - Read the magnetic strip
 - Capture your PIN with a camera or keypad overlay
- CHIP cards are safer
- Use the ATM inside the bank

ATM Skimming

Skimming is an illegal activity that involves the installation of a device, usually undetectable by ATM users, that secretly records bank account data when the user inserts an ATM card into the machine. Criminals can then encode the stolen data onto a blank card and use it to loot the customer's bank account.

1 Hidden camera

A concealed camera is typically used in conjunction with the skimming device in order to record customers typing their PIN into the ATM keypad. Cameras are usually concealed somewhere on the front of the ATM—in this example, just above the screen in a phony ATM part—or somewhere nearby (like a light fixture).

2 Skimmer

The skimmer, which looks very similar to the original card reader in color and texture, fits right over the card reader—the original card reader is usually concave in shape (curving inward), while the skimmer is more convex (curving outward). As customers insert their ATM card, bank account information on the card is “skimmed,” or stolen, and usually stored on some type of electronic device.

3 Keypad overlay

The use of a keypad overlay—placed directly on top of the factory-installed keypad—is a fairly new technique that takes the place of a concealed camera. Instead of visually recording users punching in their PINs, circuitry inside the phony keypad stores the actual keystrokes.



OTHER SCAMS

41

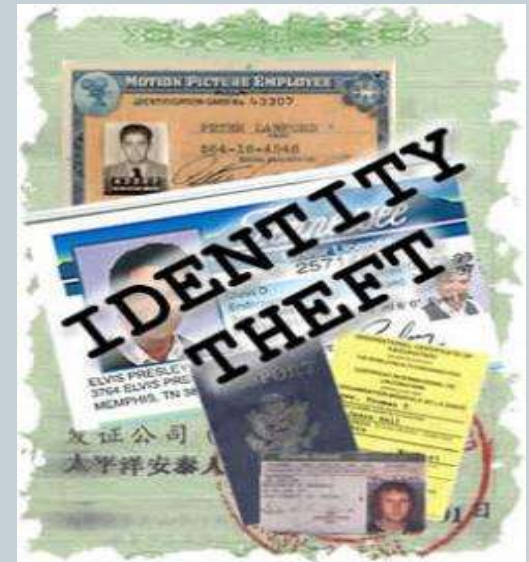
- A family member in jail/injured
- Utility threatens to cut your service
- Lottery
- Romance
- Jury scams
- Jobs
- Zero balance gift cards
- Computer helpdesk
- Scareware
- Package delivery
- Any recent crisis



IDENTITY THEFT

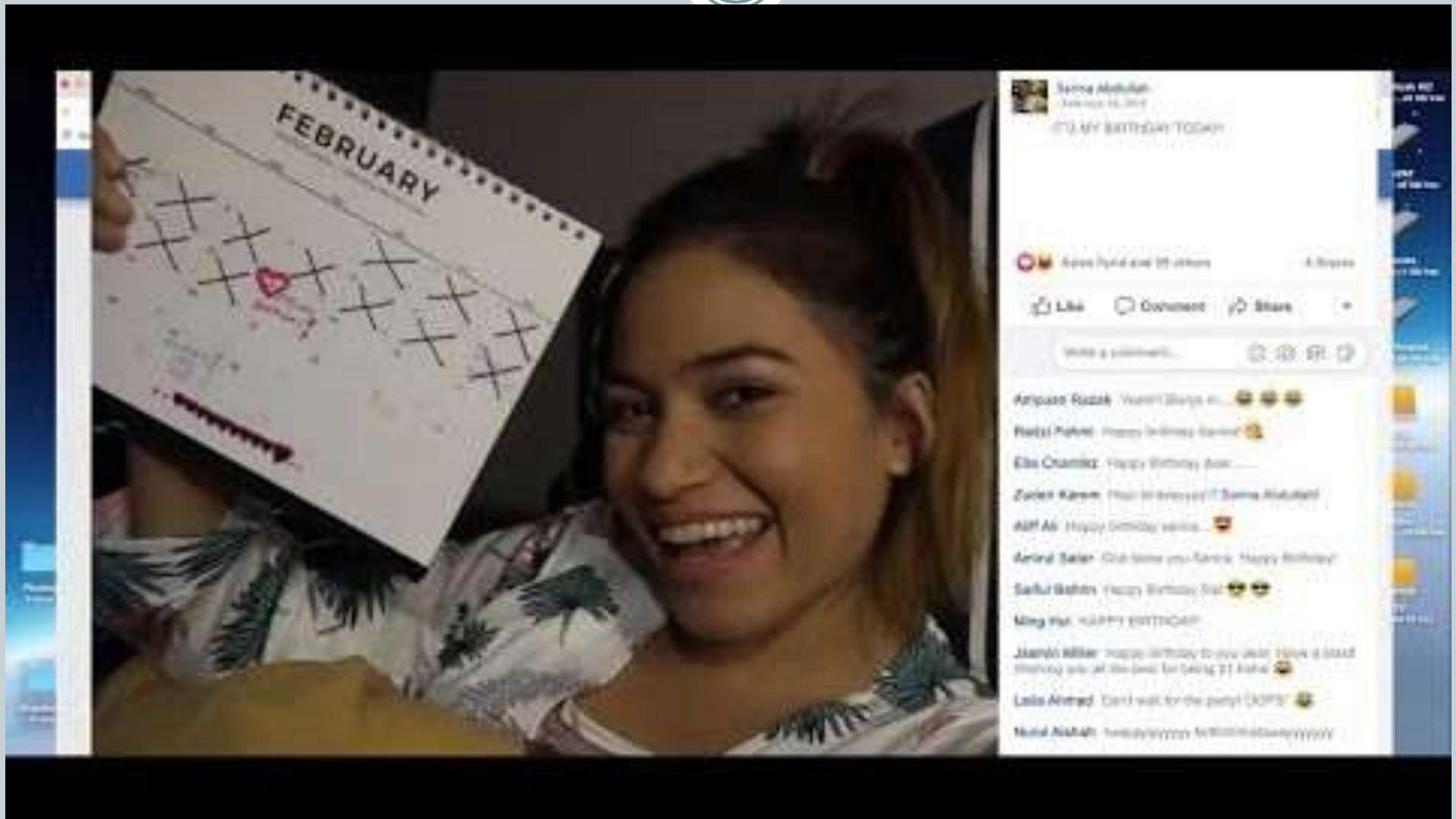
42

- Someone steals personal information in order to pretend to be you so they can:
 - Commit crimes
 - Obtain credit cards
 - Get a tax refund
 - Get a mortgage
 - Stick you with the bill



IDENTITY THEFT

44



Be careful what you share on social media

HOW ID THEFT OCCURS



News ▾ Guides ▾ Property ▾ Insurance, Visas & Legal ▾

Thai hospital fined 1.2 million baht for data breach via snack bags

Medical data mishandling shakes public trust in healthcare



Bright Choomanee · 3 weeks ago Last Updated: Sunday, August 3, 2025

1 minute read

Share this article



Picture courtesy of PDPA Thailand

bsites.

FRAUD PREVENTION

46

- Screen phone calls/solicitations.
 - Don't answer if you don't recognize the number.
 - Legit callers will leave a message.
 - Caller ID can be easily spoofed.
- Don't be pressured or bullied.
- Sounds too good to be true? It probably is!
- If you are interested, take your time, ask questions, and investigate the offer.
- Legit vendors answer questions and put offers in writing.
- Never give out personal information

FRAUD PREVENTION

47

- Use Credit Cards (vs. debit or gift cards)
- Request transaction alerts
- Review statements for suspicious activity
- Shred sensitive docs - Clean Cut Shredding
- Mail checks at the post office
- Freeze your credit at the reporting agencies:
 - *Equifax, Experian, TransUnion*
- Check your credit quarterly
 - *<https://www.annualcreditreport.com/>*

HELP IS AVAILABLE

48

If you have been targeted, remember
IT IS NOT YOUR FAULT!

THESE SCAMMERS ARE PROS!

HELP IS AVAILABLE

49

If you have been a victim of fraud, report it immediately:

- Report crime to MCPD at 301-279-8000
- A report is required for an insurance claim.
- Your bank or credit card company
- Better Business Bureau (BBB) WWW.BBB.COM
- Federal Trade Commission (FTC) WWW.FTC.GOV
- Internal Revenue Service (IRS) WWW.IRS.GOV
- Federal Bureau of Investigation (FBI) WWW.IC3.GOV
- AARP Fraud Watch Network 1-877-908-3360

Here is the TL/DR

66

- ✓ When you get a phone call, email or text message, do you know who it really is?
- ✓ You can be fooled because the scammers know so much about you.
- ✓ This is because of so many data breaches.
- ✓ And so many data brokers sell your information.

Here is the TL/DR

67

- ✓ To avoid a scam... start with the premise that every direct message, link, email, or text is **fake** and work from there.
- ✓ This should be your default response to any contact you did not initiate.
- ✓ Any time you are asked to pay for something with a gift card, wire transfer, or cryptocurrency, **it is a scam.**
- ✓ If you didn't look for it, **don't install it!**

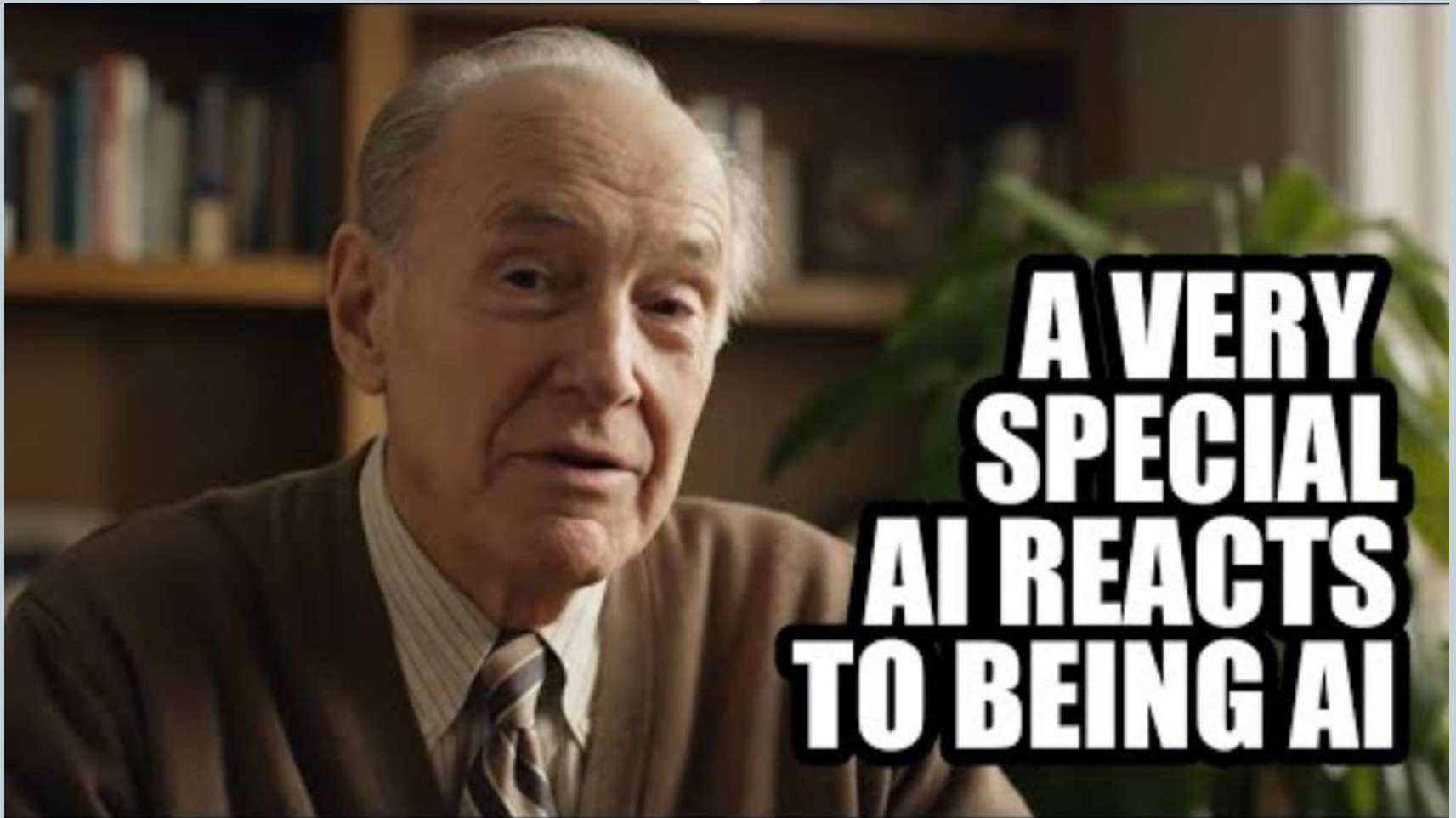
Dept of Police Web Pages

68

- **Keeping Seniors Safe**
<https://www.montgomerycountymd.gov/pol/seniors/index.html>
- **Frauds and Scams**
<https://www.montgomerycountymd.gov/pol/fraud/frauds-and-scams.html>
- **Fraud Reporting**
<https://www.montgomerycountymd.gov/pol/fraud/reporting-fraud.html>
- **Cyber Crime**
<https://www.montgomerycountymd.gov/pol/fraud/cyber-crime.html>
- **Influence and Fraud**
<https://www.montgomerycountymd.gov/pol/fraud/influence.html>
- **Victim Resistance**
<https://www.montgomerycountymd.gov/pol/fraud/resistance.html>
- **Financial Crimes Section**
<https://www.montgomerycountymd.gov/pol/fraud/financial-crimes-section.html>

AI DEEP FAKES

71





Thank you!



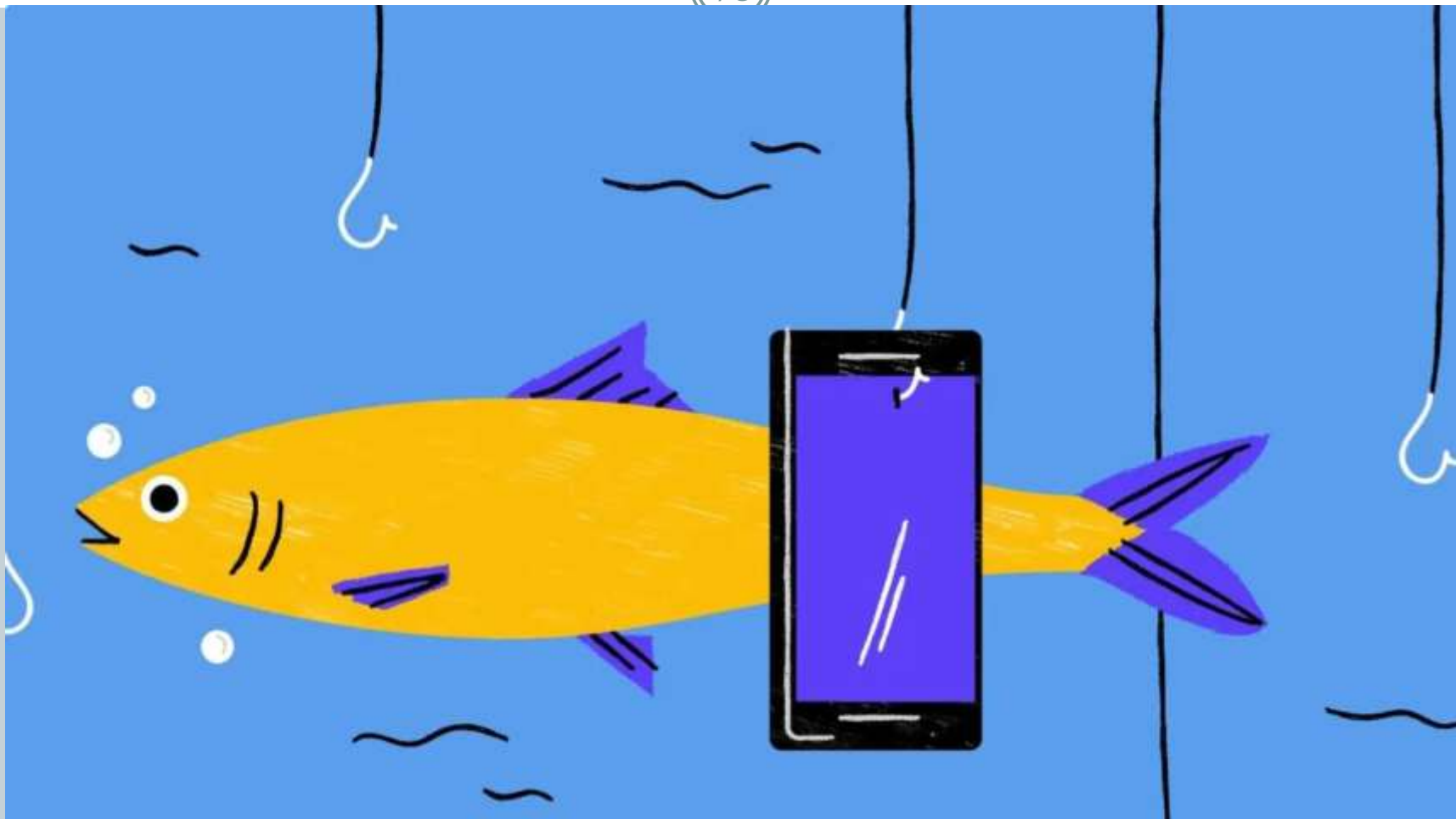
ON BEHALF OF CHIEF MARC YAMADA AND
THE MONTGOMERY COUNTY POLICE
DEPARTMENT, WE THANK YOU FOR THE
INVITATION AND THE OPPORTUNITY TO
SPEAK TODAY.

QUESTIONS OR COMMENTS?

PLEASE CALL KSS AT 240-773-5615 OR VISIT OUR WEBSITE
[HTTPS://WWW.MONTGOMERYCOUNTYMD.GOV/POL/SENIORS/](https://www.montgomerycountymd.gov/pol/seniors/)

PHISHING TEST

73



<https://phishingquiz.withgoogle.com/>