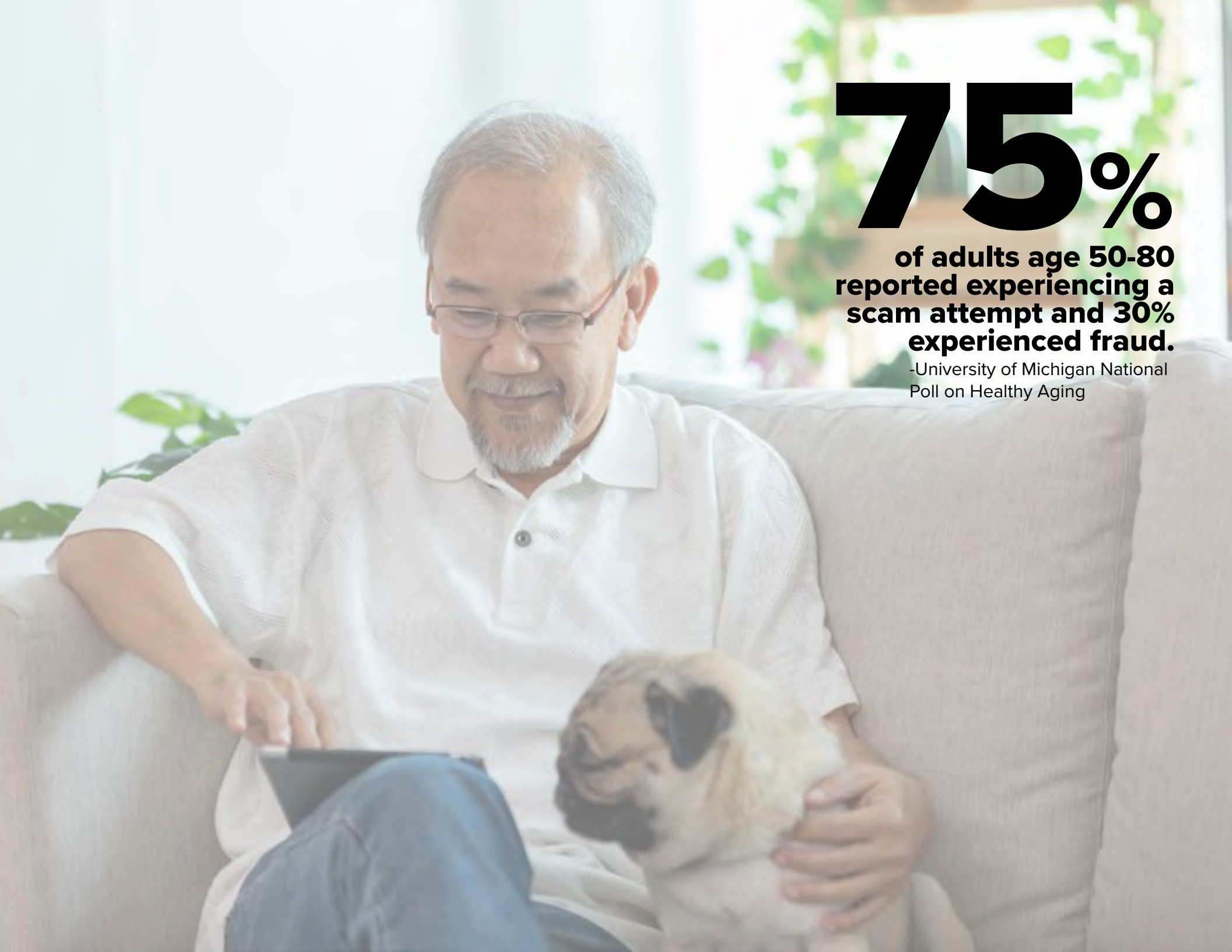
NEW YORK STATE OF OPPORTUNITY. Office for the Aging

Don't Get SCAMMED

A Comprehensive Guide for Avoiding Fraud and Theft



75%

of adults age 50-80 reported experiencing a scam attempt and 30% experienced fraud.

-University of Michigan National Poll on Healthy Aging

800k

cybercrime-related complaints were filed in 2022, with an estimated $10.3 billion in damages

-FBI

Scam Spotting, Scam Stopping
What TO DO and What NOT TO DO

Background
According to the FBI, cybercrime cost Americans 50 and older nearly $5 billion in 2022. More broadly, AARP estimates that financial exploitation costs victims 60 years and older an astonishing $28.3 billion annually. Financial scams all have one thing in common: they prey on an individual's trust to obtain information that can be used to steal money, property, and other assets. But trusted organizations – banks, government agencies, legitimate businesses, charities – don't call, email, or text "out of the blue" to ask for your personal information.

Always verify independently with a trusted source whenever receiving such requests: by using a website or phone number you know to be legitimate.

In recent years, scammers have used increasingly sophisticated methods to get you to act on their ill intent. This guide provides some basic information to help you spot the signs of a scam. We also highlight some tactics that scammers might use, so you know what to do – and what not to do – when you encounter a red flag that raises your suspicion.

Four Signs
According to the Federal Trade Commission (FTC), there are four clear signs of a scam:

- Scammers pretend to be from an organization (or representing a person) you know.
- Scammers say there's a problem or prize that they want you to act upon.
- Scammers pressure you to act immediately.
- Scammers tell you to pay in a specific way.

Any one of these signs – no matter what the source – should be a red flag.

112m

In 2023, approximately 112 million people were affected by healthcare data breaches reported by more than 540 organizations.

-U.S. Department of Health and Human Services

Common Types of Scams

Experts have identified the following most common scams that target older adults.

- **Romance Scams:** Scammers create fake online profiles to establish a relationship with victims and steal their money.

- **Prizes, Sweepstakes and Lotteries:** Scammers will call, email, text, or send a letter notifying you that you've won a prize in exchange for money, financial, or other identifying information.

- **Business or Government Impostors:** People make contact pretending to be a government agency (like the IRS, Medicare, Social Security), a charity, or tech support.

300k

phishing cases were reported to the FBI in 2022.

-FBI

- '**Grandparent Scams':** Scammers call and impersonate a grandchild – or another close relative – in a fake crisis situation, asking for immediate financial assistance. In other cases, a caller may pretend to be a lawyer or emergency first-responder calling on behalf of a family member "in trouble" asking for money or personal information.

- **Investment Scams:** Investment scams claim you'll likely make a lot of money quickly or easily with little to no risk. You may encounter these scams on social media, infomercials, or online ads claiming big returns if you invest in financial markets, cryptocurrency, real estate, precious metals and coins, and other areas.

- **Online Shopping:** Scammers often pose as real companies online — or they make up fake companies — to try to get your money or personal information. They may post fake ads for things on social media or other websites, and even use a real company's logo to try to seem legitimate. But then they take your money, and don't send what you ordered.

- **Gift Card Scams:** You receive a call or text message asking you to buy gift cards or other prepaid cards and share the card access information with the scammer.

- **Health Care Scams:** A scammer will try to sell you health insurance plans that aren't real, or push a product claiming to prevent, treat, or cure diseases or other health conditions. The scammer's real intent is to steal insurance information, money, or both by getting you to provide personal information.

Scam Tactics

- Text message from a stranger
- A text or email that one of your accounts was suspended
- A fake business email
- Social media friend requests
- Pop-up ad, infomercial, or ad on social media
- Phone calls from seemingly familiar numbers
- QR codes directing you to a cryptocurrency ATM
- Robocalls

What To Do

- Ignore phone numbers you don't recognize. You don't need to pick up.

- Ignore unsolicited links in emails, texts, and social media. Don't click.

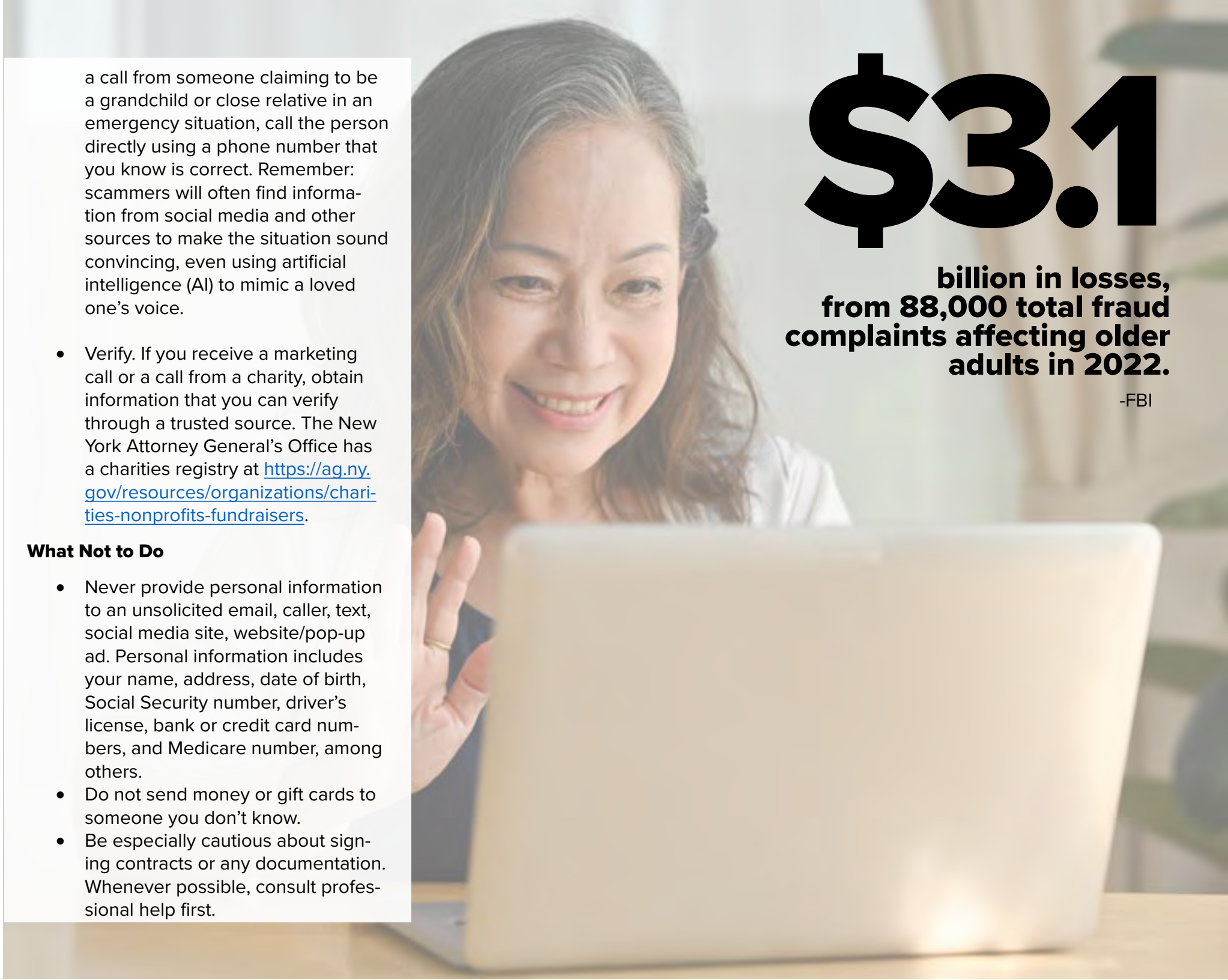
- Hang up. If you receive a call from an unknown number asking for personal information, simply hang up. If it's a company or government agency, contact the source directly through a trusted phone number. If you receive

a call from someone claiming to be a grandchild or close relative in an emergency situation, call the person directly using a phone number that you know is correct. Remember: scammers will often find information from social media and other sources to make the situation sound convincing, even using artificial intelligence (AI) to mimic a loved one's voice.

- Verify. If you receive a marketing call or a call from a charity, obtain information that you can verify through a trusted source. The New York Attorney General's Office has a charities registry at https://ag.ny.gov/resources/organizations/charities-nonprofits-fundraisers.

What Not to Do

- Never provide personal information to an unsolicited email, caller, text, social media site, website/pop-up ad. Personal information includes your name, address, date of birth, Social Security number, driver's license, bank or credit card numbers, and Medicare number, among others.
- Do not send money or gift cards to someone you don't know.
- Be especially cautious about signing contracts or any documentation. Whenever possible, consult professional help first.



$3.1

billion in losses, from 88,000 total fraud complaints affecting older adults in 2022.

-FBI

Real-Life Examples

Romance Scam

A 66-year-old woman met a man on a gaming website. The man began chatting with her on a regular basis, developing a romantic connection over time. The man eventually explained to her that his fortune had changed dramatically for the better: he now possessed over one million dollars in gold. She was told to assist the man with moving this large sum of gold, which would, in turn, financially help her. This involved sending money to her new "friend" – over $90,000 – through apps and other money transfers.

Tech Scam/Bank Impersonator Scam

A 77-year-old woman who lives alone received a fraudulent alert on her computer. The message said that the computer had been infected with a virus and she needed to call a number and speak to "tech support." The imposter took remote control of her computer and told her it would be a one-time fee to fix the problem. She paid for it.

Within a day or two, another imposter called and told her that he was an employee at the bank she used. He had "inside information" that her bank was about to fold. The imposter stated he could help move all of her money to the "Federal Reserve System" for safekeeping. She went to two separate branch locations of her bank, withdrawing $42,000 in cash that she was instructed to place in a cardboard box on her front porch.

Government Impersonator Scam

A 76-year-old man, who lives alone, received a call from an imposter claiming to be from the Social Security Administration. The person announced that his monthly Social Security check was going to increase by an additional $1,000 dollars monthly starting the following month. All he had to do was confirm his personal information, including his Social Security number. He did so. Shortly after the call ended, the man realized he had made a mistake.

Grandkid and Family Scams

A 73-year-old man received a phone call from his "daughter," who was getting married in Connecticut in two days' time. The scammers had used voice cloning and the voice sounded exactly like his daughter. The "daughter" indicated that she had gotten a DWI and was in jail and needed $15,000 bail money to be released. Another two imposters spoke to this father, claiming to be lawyers who were trying to help his daughter. The father arrived at the rehearsal dinner in Connecticut, approached his daughter and expressed his relief that she had gotten out of jail in time for the wedding. His daughter, of course, had no idea what he was talking about. He explained what had happened and then realized that the scammers had used voice cloning to acquire his money.

Stop and consider what is happening before taking any action!

70k

the number of older adults that reported a 'romance scam' in 2022. These scams resulted in $1.3 billion in losses.

-Federal Trade Commission

Resources

Federal Trade Commission (FTC)

Avoiding and reporting scams: https://consumer.ftc.gov/scams

Attorney General's Office

Phone scams: https://ag.ny.gov/publications/phone-scams

Filing a complaint: https://ag.ny.gov/file-complaint/consumer

Elder Abuse Helpline for Concerned Persons

https://elderabuse.weill.cornell.edu/programs/elder-abuse-helpline

844-746-6905

Department of Financial Services

https://www.dfs.ny.gov/consumers

Division of Consumer Protection

https://dos.ny.gov/consumer-protection

(800) 697-1220

Upstate Elder Abuse Center at Lifespan

https://www.lifespan-roch.org/upstate-elder-abuse-center

1-866-454-5110

NYS Office of Victim Services

https://ovs.ny.gov/help-crime-victims

New York State Office for the Aging

https://aging.ny.gov/

https://aging.ny.gov/programs/elder-abuse

NY Connects

https://www.nyconnects.ny.gov/

1-800-342-9871

Adult Protective Services

https://ocfs.ny.gov/programs/adult-svcs/aps/

1-844-697-3505

Common Scams and Crimes — FBI

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

Kathy Hochul, Governor
Greg Olsen, Director

www.aging.ny.gov