# Cybercriminals Are Out to Get Us

## How Seniors Can Stay One Step Ahead




**October 8, 2026**




# This presentation is brought to you by your group's membership in

apcug

(An International Association of Senior Technology and Computer User Groups)

Presented by

**Judy Taylour**

Speakers Bureau Member

# 2025 Florida Scam Rankings

| Rank | State | 2025 Losses | 2024 Losses | YoY |
|---|---|---|---|---|
| 1 | California | $3,674,716,305 | $2,539,041,635 | +44.7% |
| 2 | Texas | $1,825,636,181 | $1,351,598,183 | +35.1% |
| 3 | **Florida ←** | **$1,596,138,595** | $1,071,909,632 | +48.9% |
| 4 | New York | $1,226,307,877 | $903,975,003 | +35.7% |
| 5 | New Jersey | $660,411,901 | $434,856,424 | +51.9% |

# 2025 - 7 Florida metro  areas in top 50 for per-capita fraud complaints

| National Rank | Metro Area |
|---|---|
| #1 | Miami-Fort Lauderdale-West Palm Beach, FL |
| #5 | Orlando-Kissimmee-Sanford, FL |
| #9 | Tampa-St. Petersburg-Clearwater, FL |
| #11 | Palm Bay-Melbourne-Titusville, FL |
| #13 | Lakeland-Winter Haven, FL |
| #14 | Jacksonville, FL |
| #31 | Deltona-Daytona Beach-Ormond Beach, FL |

# Why This Matters in 2026

The numbers are large — and the scams are becoming more convincing.

**201,266**

Complaints from people age 60+ reported to the FBI's IC3 in 2025.

**$7.75 billion**

Reported losses by people age 60+ in 2025.

**SENIOR TIP**

A reported loss is not always recovered — report quickly.

Source: FBI 2025 IC3 / FBI elder fraud update. Complaints rose 37%; reported losses rose 59% from 2024.

# Artificial Intelligence Is Changing Scams

## AI makes scams easier to create

- More convincing phishing emails and text messages
- Personalized messages with fewer obvious mistakes
- Voice cloning and deepfake video can imitate trusted people
- Criminals can automate and scale scams

## What to remember

- A familiar voice does not prove the caller is real
- A polished message can still be a scam
- Urgency is a warning sign
- Verify using a phone number or website you already know

FBI and FTC continue to warn about impersonation, voice-cloning, and AI-assisted scams.

# AI + Impersonation = A More Convincing Scam

- Scams may begin with an unexpected call, text, email, or social media message.
- A cloned voice may sound like a child, grandchild, friend, bank employee, or government official.
- The scammer may create fear: “Act now,” “Keep this secret,” or “Your money is in danger.”
- Verify through a separate channel — not the number, link, or contact information supplied by the caller.

**SENIOR TIP**

Create a family code word for emergencies.

# New Scams to Watch in 2026

Fake Toll, Jury Duty & Government Messages

## Fake Toll Messages

- "You owe an unpaid toll."
- A text threatens a late fee, license problem, or other penalty.
- A link takes you to a payment page designed to steal information.

## Fake Jury Duty

- "You missed jury duty."
- The caller says there is a warrant or fine.
- You are told to pay immediately by phone, gift card, wire, or cryptocurrency.

## Government Imposters

- Scammers may pretend to be law enforcement or another government agency.
- Caller ID and official -looking documents can be faked.
- Hang up and contact the agency using a number you find yourself.

Sources: FTC consumer alerts, June 2026; FBI IC3 government-impersonation guidance.

# New Scams to Watch in 2026

## The Scam After the Scam — Recovery & Fake IC3

### How it works

- You have already lost money to a scam.
- Someone contacts you claiming they can recover your money.
- They may pretend to be the FBI, IC3, a lawyer, or a recovery company.
- They ask for money, cryptocurrency, or personal information.

### Protect Yourself

- IC3 does not use social media to contact victims or recover lost money.
- Do not pay a “recovery fee.”
- Do not give account information to an unexpected recovery service.
- Report the original scam through official channels — not through a link sent by the scammer.

Source: FBI IC3, “FBI Warns of Scammers Impersonating the IC3,” July 20, 2026.

# New Scams to Watch in 2026

## AI Can Fake More Than a Voice

### What AI Can Fake

- The voice of someone you know.
- Photos and videos of people who look real.
- A government official, company leader, or family member in a video.
- Some scammers use AI to create fake video during live conversations.

### Your New Rule

- Seeing or hearing someone does not prove the person is real.
- Be especially careful when the request involves money, passwords, or personal information.
- Verify using a separate phone number, website, or trusted contact.
- Take a moment before responding to anything that creates fear or urgency.

Sources: FBI 2025 IC3 Annual Report; FBI IC3 PSA, July 20, 2026.

# Common Scams

**Know the names — then learn the warning signs.**

- Identity theft
- Phishing
- Vishing (voice phishing)
- Spoofing
- Grandparent/family scams

- Technical support scams
- Subscription/renewal scams
- Investment & “pig butchering” scams
- House stealing/deed fraud
- Money mule scams

# Identity Theft & Phishing

## Identity Theft

- Criminals steal personal information to open accounts or access money.
- Common sources include data breaches, stolen mail, and phishing.
- Warning signs: unfamiliar bills, credit inquiries, or missing mail.

## Phishing

- Fake emails or messages try to steal passwords or financial information.
- Scammers may impersonate banks, Medicare, Social Security, or delivery services.
- Red flags: urgency, suspicious links, or unexpected attachments.

# Vishing & Spoofing

## Vishing

- A phone call pretending to be a bank, government agency, or technology company.
- Common tactics: fear, urgency, threats, or account-closure warnings.
- Hang up and call the organization using a number you know is real.

## Spoofing

- Caller ID or an email address is disguised to look familiar.
- A scam can appear to come from “your bank” or a local number.
- Caller ID is not proof that a call is legitimate.

# Grandparent & Family Scams

## The story

- Someone pretends to be your grandchild or another family member.
- They claim there has been an accident, arrest, emergency, or another crisis.
- They ask for money by gift card, wire transfer, cryptocurrency, or another fast method.
- They may insist that you keep the situation secret.

## Your response

- Slow down.
- Call the family member directly.
- Use a family code word.
- Tell someone you trust.

# Technical Support Scams

## Typical setup

- A scary pop-up says your computer has a virus.
- It may pretend to be Microsoft, Apple, or another trusted company.
- A phone number tells you to call immediately.
- The scammer wants remote access or payment.

## Remember

- A real security warning will not tell you to call a phone number in a pop-up.
- Never give remote control of your computer to an unexpected caller.
- If you need help, contact a trusted technician using known contact information.

Source: FTC guidance on tech-support scams.

# Pig Butchering: The “Super Scam”

## The name

“Pig butchering” is a nickname for a long-term scam in which criminals build trust and gradually steer victims into a fake investment.

**SENIOR TIP**

Never invest because an online stranger tells you to.

Source: AARP, September 2026; investment scams reported $8.6 billion in losses in 2025.

# Investment Fraud & “Pig Butchering”

## Warning signs

- Promises of guaranteed or “risk-free” returns.
- A stranger builds trust over weeks or months.
- The conversation moves to cryptocurrency or a private investment website.
- You are told to keep the investment secret.

## The trap

- A fake website can show impressive “profits.”
- You may be allowed to withdraw a small amount at first.
- Later, you are asked for more money, taxes, or fees.
- When you try to cash out, the money — and the scammer — disappear.

Source: AARP, updated September 2026; FBI/FTC fraud guidance.

# House Stealing / Deed Fraud

## How it works

- Criminals may use forged documents or stolen personal information to transfer or misuse property ownership.
- Homeowners who own their homes outright can be attractive targets.
- Victims may not discover the problem until they receive an unexpected bill, lien, foreclosure notice, or other property-related document.

## Protect yourself

- Monitor property records.
- Create a Hillsborough County Property Fraud Notice-.
- Open and review property notices.
- Report anything suspicious promptly.

# Money Mule Scams

## What is a money mule?

- Someone who is asked to move money or packages for another person.
- The request may come through romance, friendship, tech support, or another trusted relationship.
- The scammer may promise easy income or claim the transfer is urgent.
- For some reason, they can't do it themselves.

## Why it is dangerous

- The money may come from another victim.
- Your bank account or identity may become part of a criminal operation.
- You can face serious legal consequences even if you did not understand the entire scheme.

# Shop Safely Online

## Before buying

- Do your homework on the seller.
- Check the website address carefully.
- Ask: Do they really need all the information they are requesting?
- Be suspicious of deals that are far too good to be true.

## Pay carefully

- A credit card generally provides stronger dispute protections than a debit card.
- Use reputable payment services when appropriate.
- Review bank and credit card statements regularly.
- Set a charge limit on your credit cards so you are notified when charges occur.

# Medicare Scams: Protect Your Medicare Number

## Common Medicare Scams

"Your Medicare card is expiring" or needs to be replaced.

Someone asks for your Medicare Number or Social Security number.

A caller offers free medical equipment, services, or gifts.

A scammer threatens to cancel your benefits unless you act now.

## Protect Yourself

Medicare will NOT call you unexpectedly to sell you something.

Don't give your Medicare Number to an unsolicited caller, email, or visitor.

Check your Medicare claims and compare them with services you actually received.

Hang up and contact Medicare using an official number.

## Remember

Your Medicare Number is valuable personal information.

If something looks wrong, don't ignore it—check it.

Report suspected Medicare fraud to 1-800-MEDICARE.

Free Medicare counseling is available through SHIP.

SHIP is a federally funded network of local counselors offering free, objective Medicare education and assistance in all states.

Source: Medicare.gov — Reporting Medicare Fraud & Abuse; Your Medicare Card (accessed September 2026)

# Oldie but Goodie: Check Washing

## What is check washing?

- A criminal alters a legitimate check so the payment goes to them.
- The check may contain your bank account and routing numbers.
- Stolen checks can be used for fraud or sold to other criminals.

## Reduce the risk

- Consider electronic bill pay for routine bills.
- If you write checks, use a permanent gel ink pen.
- Mail checks from a secure location and monitor your account.
- Report missing or altered checks to your bank promptly.

# Grandparent / Family Scam: Make a Family Code

## Choose a simple code

- Pick a word or short phrase known only to close family members.
- Use it if someone calls or texts claiming to be a grandchild or relative in trouble.
- If the person cannot provide the code, stop and verify another way.

## Protect family information

- Review social media privacy settings.
- Avoid posting details that reveal birthdays, travel plans, or family relationships.
- Scammers can use public information to make a story sound believable.

# How Criminals Manipulate Victims

### FEAR
“Your account is being hacked.”

### URGENCY
“You must act now.”

### AUTHORITY
“I’m from the government.”

### EMOTION
“I need your help.”

### SECRECY
“Don’t tell anyone.”

### SENIOR TIP
Scammers want you to react — not think.

# The Best Defense: STOP • VERIFY • THEN ACT

## 1 STOP

- Do not click.
- Do not send money.
- Do not give remote access.
- Do not let the caller rush you.

## 2 VERIFY

- Hang up.
- Use a known phone number.
- Type the official website yourself.
- Ask someone you trust.

## 3 ACT

- Only after you verify.
- If it is a scam, report it.
- If money was sent, contact the bank immediately.

# Everyday Prevention

- Let unknown calls go to voicemail; be cautious with unexpected texts.
- Never click unexpected links or open unexpected attachments.
- Use strong, unique passwords and turn on multi-factor authentication.
- Keep your devices, browsers, and apps updated.

- Freeze your credit with the four credit bureaus.
- Shred sensitive documents before throwing them away.
- Review bank and credit card statements regularly.
- Use a trusted patching tool if you need help keeping Windows apps updated.

**Patch My PC**

# If You Think You Are a Victim

**1**

Contact your bank or credit-card company immediately if money or account information was involved.

**2**

Report to local police or sheriff when appropriate.

**3**

Report internet crime to the FBI's IC3.

**4**

Contact the credit bureaus if identity or credit information may be compromised.

# Resources for Seniors

## Keep these resources handy

- AARP Fraud Watch Network
- Federal Trade Commission: ReportFraud.ftc.gov
- FBI Internet Crime Complaint Center: IC3.gov
- State and local consumer-protection agencies

## And remember

- Senior centers and community education programs can help.
- Trusted family members or caregivers can be a second set of eyes.
- Reporting helps authorities identify patterns and protect others.

# TO DO: Create Your Online Government Accounts

## IRS Individual Online Account

- Lets you view tax information, refund status, transcripts, and more.
- Can help you protect your tax identity.
- Create it yourself — before a criminal tries to misuse your information.

## my Social Security

- Lets you review earnings and benefits information.
- Helps you monitor your Social Security account.
- Use only the official SSA.gov website.

Official sites: IRS.gov/account • SSA.gov/myaccount/

# Create an IRS Individual Online Account

## Why create one?

- View key tax-return information and transcripts.
- Check refund or amended-return status.
- Request and access an Identity Protection PIN.
- See digital IRS notices and make or schedule payments.

## Safety reminder

Start at the official IRS website. Do not use an IRS link from an unexpected email or text.

Official source: IRS.gov/account • IRS account uses secure identity verification through ID.me.

# Create a my Social Security Account

## What you can do

- Review your earnings history.
- Check benefits information and estimates.
- Request certain replacement documents and manage account information.
- Help protect your Social Security information by monitoring your account.

## Sign-in options

- Login.gov
- ID.me
- As of June 7, 2025, these are the sign-in options for SSA online services.

Official source: SSA.gov/myaccount/ • SSA FAQ updated 2026.

# USPS Informed Delivery

## A useful free service

- Get a daily email preview of incoming mail.
- See grayscale images of the outside of eligible letter-size mail.
- Track and manage packages.
- Use your USPS.com account and verify your identity and address.

## Why it helps

You can spot mail that you are expecting — and notice when something seems missing or unusual.

Official source: InformedDelivery.USPS.com • USPS says the service is free.

# Password Safety

## Strong passwords

- Longer is better — aim for at least 14–16 characters when practical.
- Use a different password for every important account.
- Avoid names, pet names, birthdays, and information connected to you.
- A password manager can create and remember unique passwords.

## Passphrases

- Use a memorable phrase rather than a short word.
- Mix words with numbers and special characters when required.
- Do not use an example from a presentation as your real password!

# Passkeys, PINs & Biometrics

## PIN

A device PIN can unlock your device and may be used as part of a secure sign-in process.

## Biometrics

Face or fingerprint recognition can make signing in easier while keeping the credential on your device.

## Passkey

A secure digital credential that can replace a password. You may sign in with your device, biometrics, or PIN.

# Read Critically

## Ask yourself

- Is the sender asking for something they normally would not ask?
- Why would a company need information it already has?
- Are there unusual phrases, odd addresses, or unexpected attachments?
- Is there pressure to act immediately?

## When in doubt

Stop. Do not click. Verify through the company's official website or another trusted source.

FTC: Do not let an unexpected message or call rush you into sending money or information.

# Verify to Clarify

### Instead of using the message

- Open your browser yourself.
- Type the company's official web address or use a bookmark you created earlier.
- Log in to your account and look for messages or alerts.
- Call the organization using a phone number from an official statement, card, or website.

### Never verify by

- Clicking the unexpected link
- Calling the unexpected number
- Replying to the message
- Giving the caller information

# To Click or Not to Click?

## Look beyond the display name

- Configure your email so you can see the sender's full email address.
- A familiar name can hide a completely different email address.
- Check the address before clicking a link or opening an attachment.

## Example

- A familiar person may use an AOL address.
- A phishing message may use a Gmail address that looks similar.
- Do not assume the message is safe just because the name looks right.

# When in Doubt, Throw It Out

## A simple rule

Be suspicious of unexpected messages from people or organizations you do not know well. You do not have to answer every email, text, or call.

## Remember

- Scammers can sound friendly.
- Scammers can sound official.
- Scammers can know personal details.
- None of that proves they are legitimate.

# Judy's Tip: Make a Reporting Script

### Write it down before you need it

- Your name and contact information
- What happened and when
- Names, phone numbers, email addresses, websites, and payment information
- Names of banks, companies, or agencies involved

### Why?

When you are upset or embarrassed, it is easy to forget details. A simple script helps you give the same information each time you report the crime.

# How to Report: IC3 — What to Save

## Include

- Names of the scammer or company
- Dates and times of contact
- How the scammer contacted you
- Phone numbers, email addresses, mailing addresses, and websites

## Keep original records

- Emails and text messages
- Screenshots
- Payment records
- Notes or logs of conversations

# How to Report: IC3 — Payment Details

### If money was sent

- Record the payment method.
- Include the financial institution, account information, and transaction details when appropriate.
- Include wire transfers, prepaid cards, cryptocurrency, or other payment methods.
- Contact the bank or payment provider immediately — do not wait for the report.

### Describe the scam

- What were you told?
- What were you instructed to do?
- What did you actually do?
- What happened afterward?

# Report Scams to the FTC

## ReportFraud.ftc.gov

Use the FTC's official reporting site to report scams, fraud, and bad business practices.

### Important

- The FTC will not demand money.
- The FTC will not tell you to move money to "protect it."
- The FTC will not ask you to hand cash or gold to a courier.

Official source: FTC.gov / ReportFraud.ftc.gov

# Your 10-Point Scam Defense

- 1. Slow down.
- 2. Verify independently.
- 3. Never send money to “protect” it.
- 4. Never give an unexpected caller remote access.
- 5. Use unique passwords.
- 6. Turn on MFA or use passkeys.
- 7. Keep software updated.
- 8. Review financial and property records.
- 9. Talk to someone you trust.
- 10. Report scams quickly.

# STOP • VERIFY • THEN ACT

If something makes you afraid, confused, or rushed...

**STOP. Take a breath. Verify. Then decide.**

You do not have to make a decision right now.