STOP • VERIFY • THEN ACT

A Senior's Everyday Scam Prevention Guide

WORLD ELDER ABUSE AWARENESS DAY
Building Strong Support for Elders

Protecting Yourself from Today's Most Common Scams

apcug
An International Association of Technology & Computer User Groups

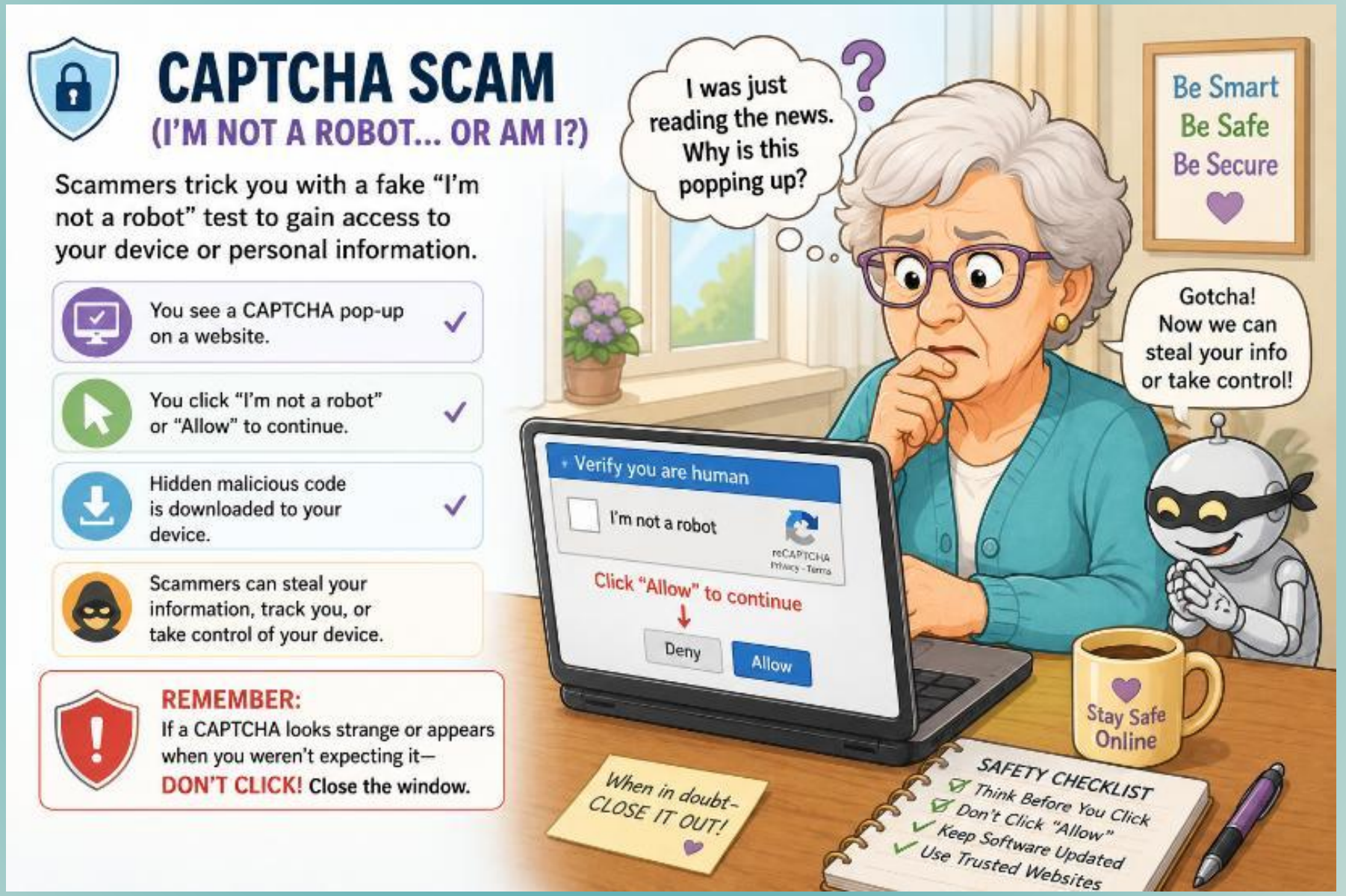

IMPOSTER SCAMS
When Scammers Pretend to Be Someone You Trust
THE HALL OF IMPOSTERS
BANK REPRESENTATIVE
GOVERNMENT AGENT
TECH SUPPORT TECHNICIAN
UTILITY COMPANY
MEDICARE REPRESENTATIVE
CELEBRITY
GRANDCHILD
ROMANCE INTEREST
BANK
IRS
TECH SUPPORT
MEDICARE
VERIFY
STOP
VERIFY
THEN ACT
Scammers wear masks.
Don't be fooled!
Look. Think. Verify!
Knowledge is your best protection.
STOP • VERIFY • THEN ACT

CAPTCHA Safety Scams

HOW IT WORKS	RED FLAGS	WHAT TO DO
• A box appears on a website asking you to prove you are not a robot	• The CAPTCHA appears on a website you did not intentionally visit	• Close the browser tab immediately if CAPTCHA instructions seem unusual
• On fake or hacked sites, clicking it secretly installs harmful software	• It asks you to press unusual keyboard combinations	• Real CAPTCHAs only ask you to click a checkbox or identify photos
• Some fake CAPTCHAs ask you to copy and paste a command into your computer	• It asks you to copy and paste text or a command into your computer	• Never copy and paste commands into your computer from a website
• Following the instructions gives scammers access to your device and files	• You are asked to download a file to 'complete verification'	• Keep your computer's security software and browser updated

STOP • VERIFY • THEN ACT

CAPTCHA Safety Scams



STOP • VERIFY • THEN ACT

Celebrity Scams

HOW IT WORKS	RED FLAGS	WHAT TO DO
• Scammer creates a fake social media account impersonating a celebrity • They message you: you have been selected for a special prize or gift • They ask for a small fee or your personal info to claim the prize • They may use AI-generated voice or video to seem like the real celebrity	• A celebrity contacts you directly out of the blue via social media • They ask for money, gift cards, or your personal information • Account name has a slight variation, extra letter, or odd spelling • Promises of money, a prize, a personal friendship, or romance	• Real celebrities do not contact fans to give away money or gifts • Check the account carefully — look for a verified blue checkmark • Never pay any fee to receive a prize or gift from a celebrity • Report the fake account to the social media platform

STOP • VERIFY • THEN ACT

Celebrity Scams

STOP • VERIFY • THEN ACT

Fake Bank & Credit Card Fraud Calls

HOW IT WORKS	RED FLAGS	WHAT TO DO
• Caller claims to be from your bank or credit card company	• Pressure to act immediately or your money will be lost	• Hang up immediately — do not stay on the line
• Says suspicious activity has been detected on your account	• Caller already knows some of your info to seem legitimate	• Call the number on the back of your bank card yourself
• Asks you to verify your account number, SSN, or PIN	• Asks for your full card number, CVV code, or PIN	• Banks never ask you to move money to a ‘safe account’
• May ask you to transfer money to a ‘safe’ account	• Requests payment via wire transfer or gift card	• Report the call to your bank’s fraud department

STOP • VERIFY • THEN ACT

Fake Bank & Credit Card Fraud Calls

STOP • VERIFY • THEN ACT

Fake Government Calls

HOW IT WORKS	RED FLAGS	WHAT TO DO
• Caller claims to be from the IRS, Social Security, or law enforcement	• Caller demands immediate payment over the phone	• Hang up — government agencies do NOT demand instant phone payment
• Says you owe back taxes or there is a warrant for your arrest	• Insists on payment by gift card, wire transfer, or cryptocurrency	• The IRS contacts taxpayers by mail first — never by phone
• Demands immediate payment to avoid arrest or loss of benefits	• Threatens arrest, deportation, or license suspension	• Call the agency directly from their official website
• Caller ID may show a real government number — this can be faked	• Tells you not to tell anyone about the call	• Report the call to the FTC at ReportFraud.ftc.gov

STOP • VERIFY • THEN ACT

Fake Government Calls

STOP • VERIFY • THEN ACT

Grandparent's Scam

HOW IT WORKS

- A scammer calls pretending to be grandchild, relative, or friend.
- They claim there is an emergency such as an accident, arrest, or medical crisis.
- The caller begs for secrecy and says not to tell anyone.
- They ask for money immediately through gift cards, wire transfers, or payment apps.

RED FLAGS

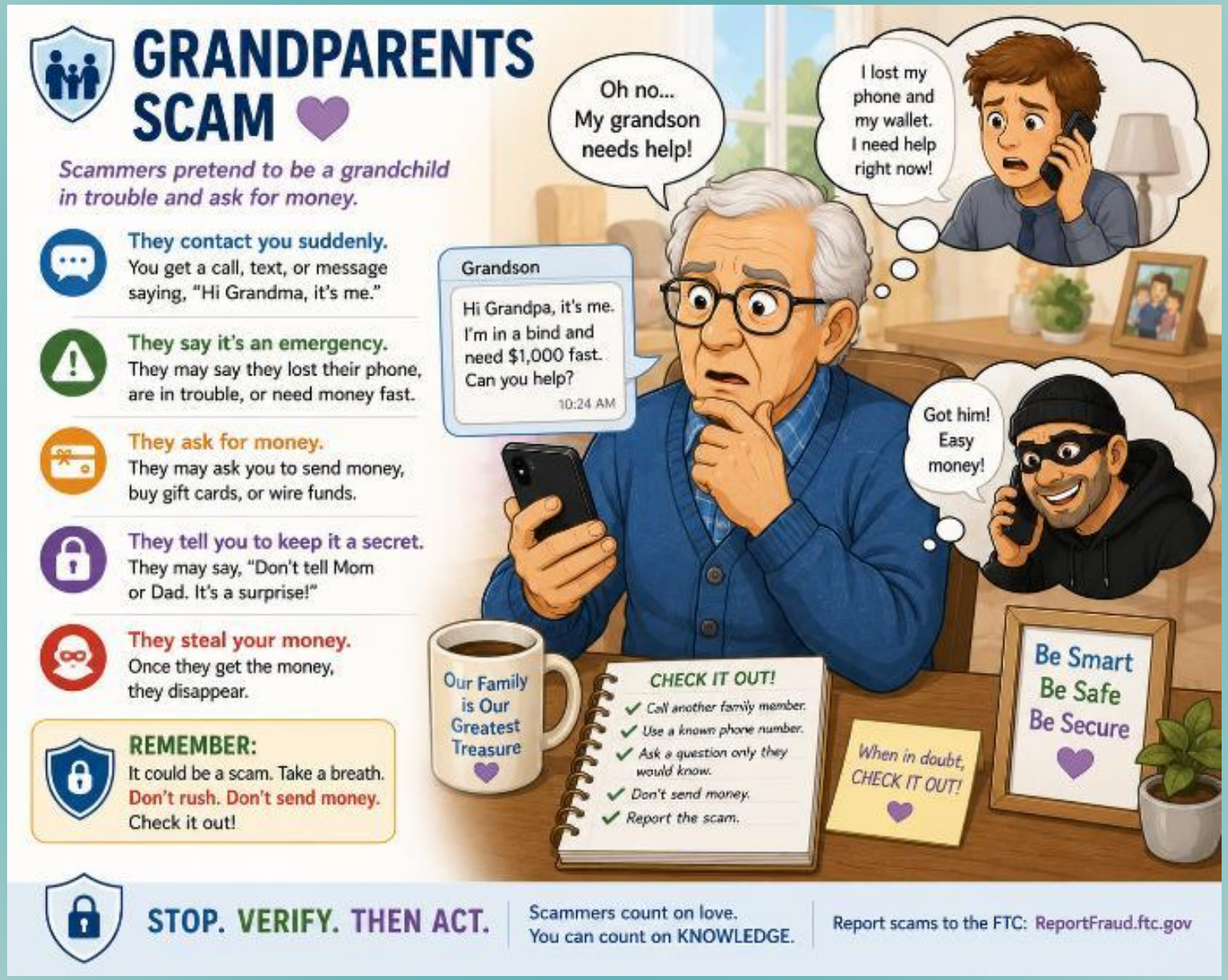
- Caller demands immediate payment over the phone
- Insists on payment by gift card, wire transfer, or cryptocurrency
- Threatens arrest, deportation, or license suspension
- Tells you not to tell anyone about the call

WHAT TO DO

- Stop and verify the story before sending money.
- Call the grandchild or another family member directly.
- Ask questions only your relative would know.
- Never send money until you independently confirm the emergency.
- Have a family safe word; if isn't used in the call you know it is a scam.

STOP • VERIFY • THEN ACT

Grandparent's Scam



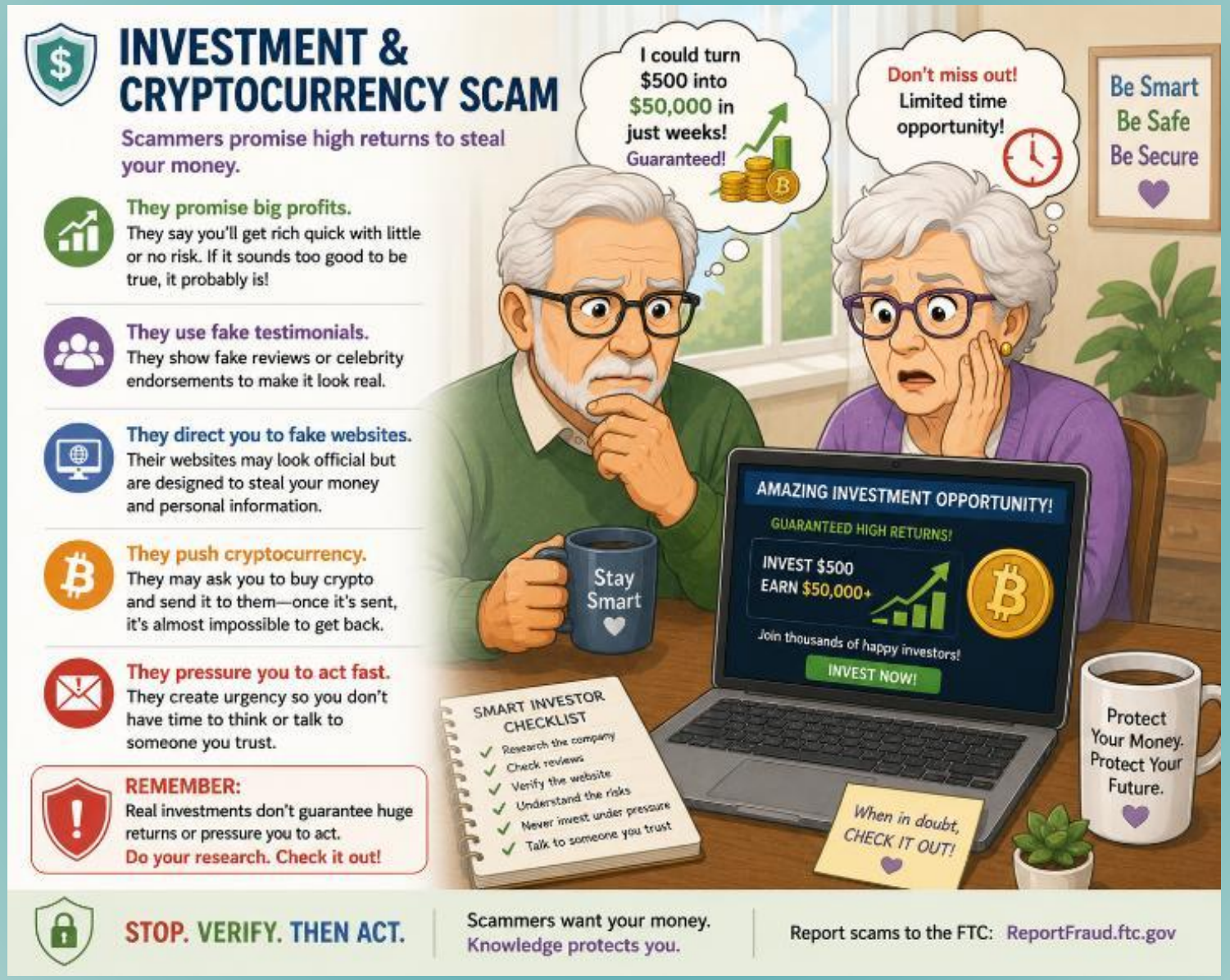
STOP • VERIFY • THEN ACT

Investment & Cryptocurrency Scams

HOW IT WORKS	RED FLAGS	WHAT TO DO
• Someone promises guaranteed high returns on stocks or cryptocurrency	• Guaranteed returns with no risk — this does NOT exist in real investing	• Never invest based on an unsolicited call or online relationship
• They show you fake account screens with impressive growing profits	• Pressure to invest quickly before the ‘opportunity closes’	• Check any investment at investor.gov (the SEC’s official site)
• They encourage you to invest more money as your ‘balance’ grows	• You are asked to invest through an app or platform they control	• Talk to a trusted family member before moving any money
• When you try to withdraw, your money is gone	• Promises of secret tips or insider knowledge	• Report suspected investment fraud to the FTC and the SEC

STOP • VERIFY • THEN ACT

Investment & Cryptocurrency Scams



STOP • VERIFY • THEN ACT

Lost Pet Scam

HOW IT WORKS

- Scammer posts a fake ‘found pet’ ad or responds to your lost pet post
- Claims your pet is far away and demands money for shipping or vet bills
- May send a stolen or fake pet photo to seem convincing
- Keeps demanding more fees each time you pay

RED FLAGS

- Caller refuses a live video call showing the pet
- Demands payment by gift card, wire transfer, Zelle, or Cash App
- Story keeps changing or seems inconsistent
- Extreme urgency — ‘Pay now or I can’t hold the pet’

WHAT TO DO

- Never pay before seeing the pet in person
- Call your local animal shelter to report the missing pet
- Report fake ads to the website or platform immediately
- Contact local police if you have already sent money

STOP • VERIFY • THEN ACT

Lost Pet Scam

STOP • VERIFY • THEN ACT

Lottery, Sweepstakes & Prize Scams

HOW IT WORKS	RED FLAGS	WHAT TO DO
• You receive a call, letter, or email: you have won a large prize!	• You must pay any amount of money to receive a prize	• Legitimate sweepstakes NEVER require you to pay to collect a prize
• You may be told you won a lottery you never entered	• You won a lottery or sweepstakes you don't remember entering	• Hang up the phone or throw away the letter
• To collect your prize, you must pay taxes, fees, or customs upfront	• Payment required by wire transfer, gift card, or money order	• Never send money, gift cards, or personal info to claim a prize
• Once you pay, the scammer disappears — there is no prize	• Caller urges secrecy: 'Do not tell your family yet'	• Report the scam to the FTC at ReportFraud.ftc.gov

STOP • VERIFY • THEN ACT

Lottery, Sweepstakes & Prize Scams

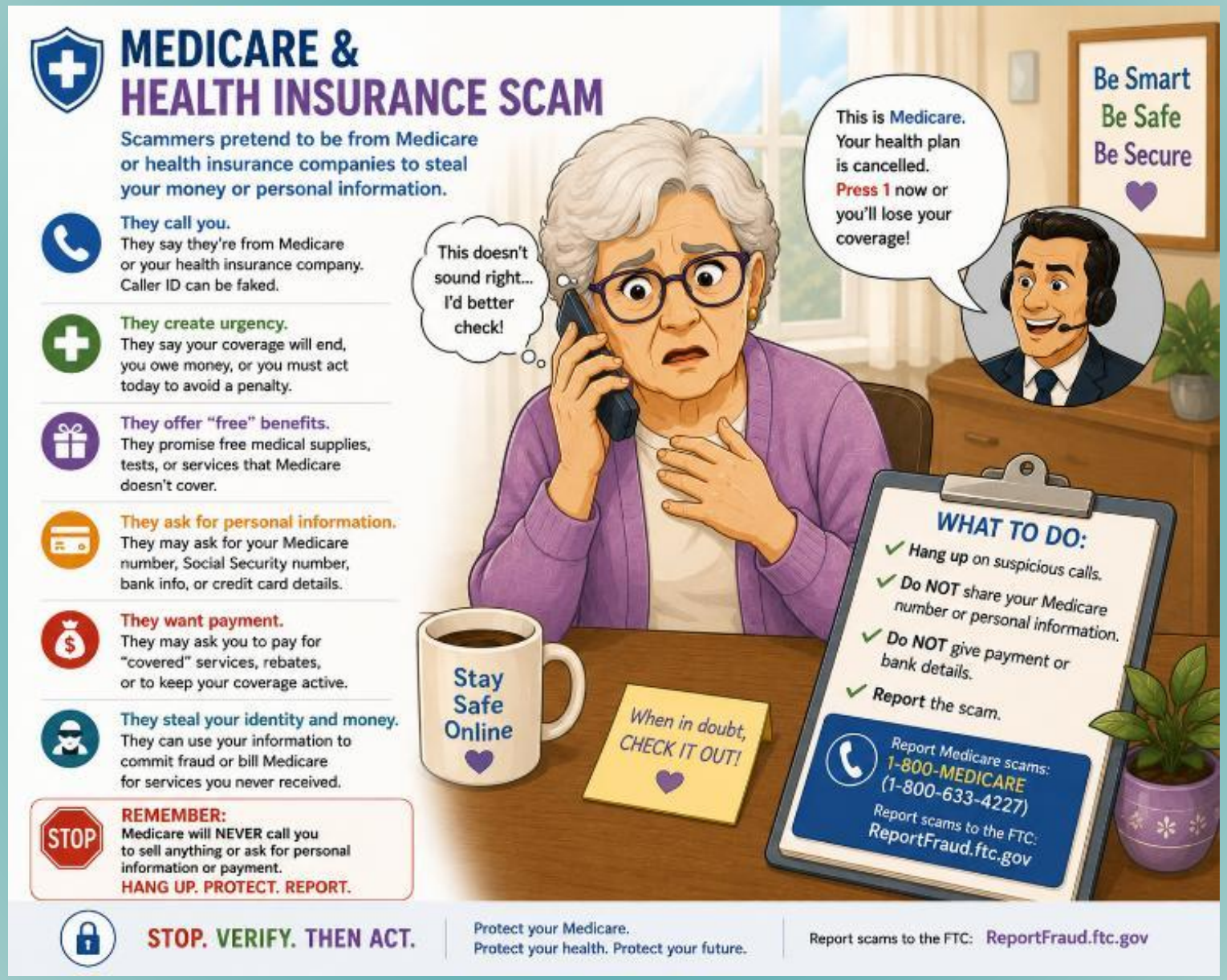
STOP • VERIFY • THEN ACT

Medicare & Health Insurance Scams

HOW IT WORKS	RED FLAGS	WHAT TO DO
• Caller claims to be from Medicare or your insurance company	• Unsolicited call about your Medicare coverage or benefits	• Hang up immediately on all unsolicited Medicare calls
• Offers free equipment, genetic testing kits, or a new Medicare card	• Request for your Medicare ID number over the phone	• Call Medicare directly: 1-800-MEDICARE (1-800-633-4227)
• Asks for your Medicare number or Social Security number	• 'Free' offers that require personal or insurance information	• Never give your Medicare number to an unsolicited caller
• Uses your number to bill for services you never received	• Threats that your Medicare coverage will be cancelled	• Report Medicare fraud: 1-800-HHS-TIPS (1-800-447-8477)

STOP • VERIFY • THEN ACT

Medicare & Health Insurance Scams



STOP • VERIFY • THEN ACT

Online Pet Scams

HOW IT WORKS

- Scammer posts a convincing ad selling puppies or kittens at a great price
- After you pay, they claim the pet needs fees for shipping, crates, or insurance
- Every time you pay, a new fee appears — and the pet never arrives
- The pet does not exist — scammer used stolen photos from real breeders

RED FLAGS

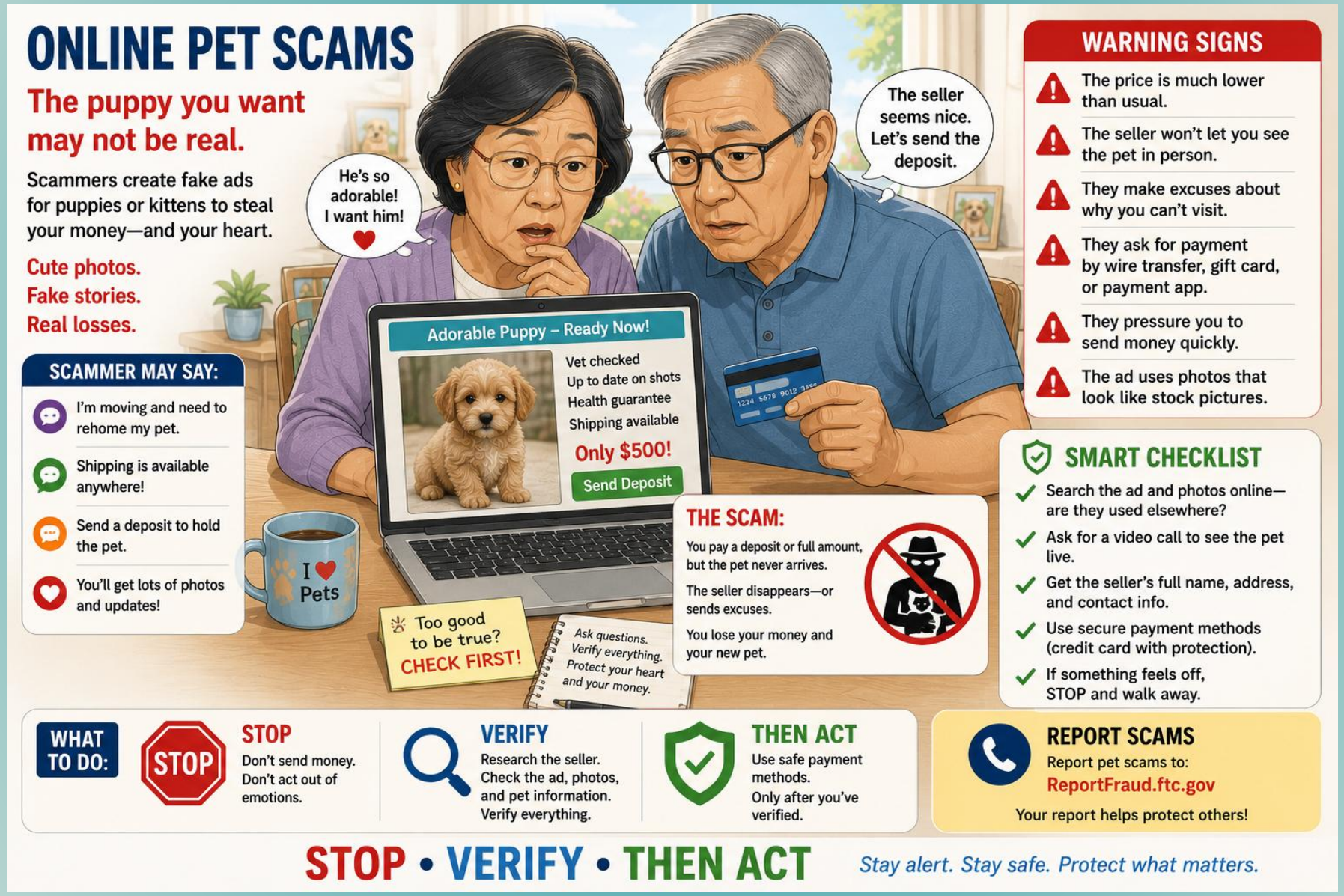
- Price is significantly lower than typical for that breed
- Seller is far away and says the pet must be shipped to you
- Payment by gift card, wire transfer, Zelle, or Cash App only
- Seller refuses a live video call showing you the actual pet

WHAT TO DO

- Only buy pets locally where you can meet the animal and seller in person
- Search the pet's photos online (images.google.com) for stolen images
- Never pay for a pet using gift cards, wire transfer, or money orders
- Report online pet scams to the FTC at ReportFraud.ftc.gov

STOP • VERIFY • THEN ACT

Online Pet Scams



STOP • VERIFY • THEN ACT

Password Reset & Email Security Scams

HOW IT WORKS	RED FLAGS	WHAT TO DO
• You receive an email or text saying your password must be reset now	• Urgent language: 'Act now or lose access permanently'	• Delete the email or text — do not click any links
• Message warns your account will be locked or deleted if you don't act	• Email sender address looks slightly off or misspelled	• Type the company's website address directly in your browser
• The link leads to a fake website that looks like the real company	• The link URL does not match the company's real website	• Enable two-step verification on all important accounts
• You enter your login — now the scammer has your account	• You did not request a password reset	• Call the company's official customer service if unsure

STOP • VERIFY • THEN ACT

Password Reset & Email Security Scams

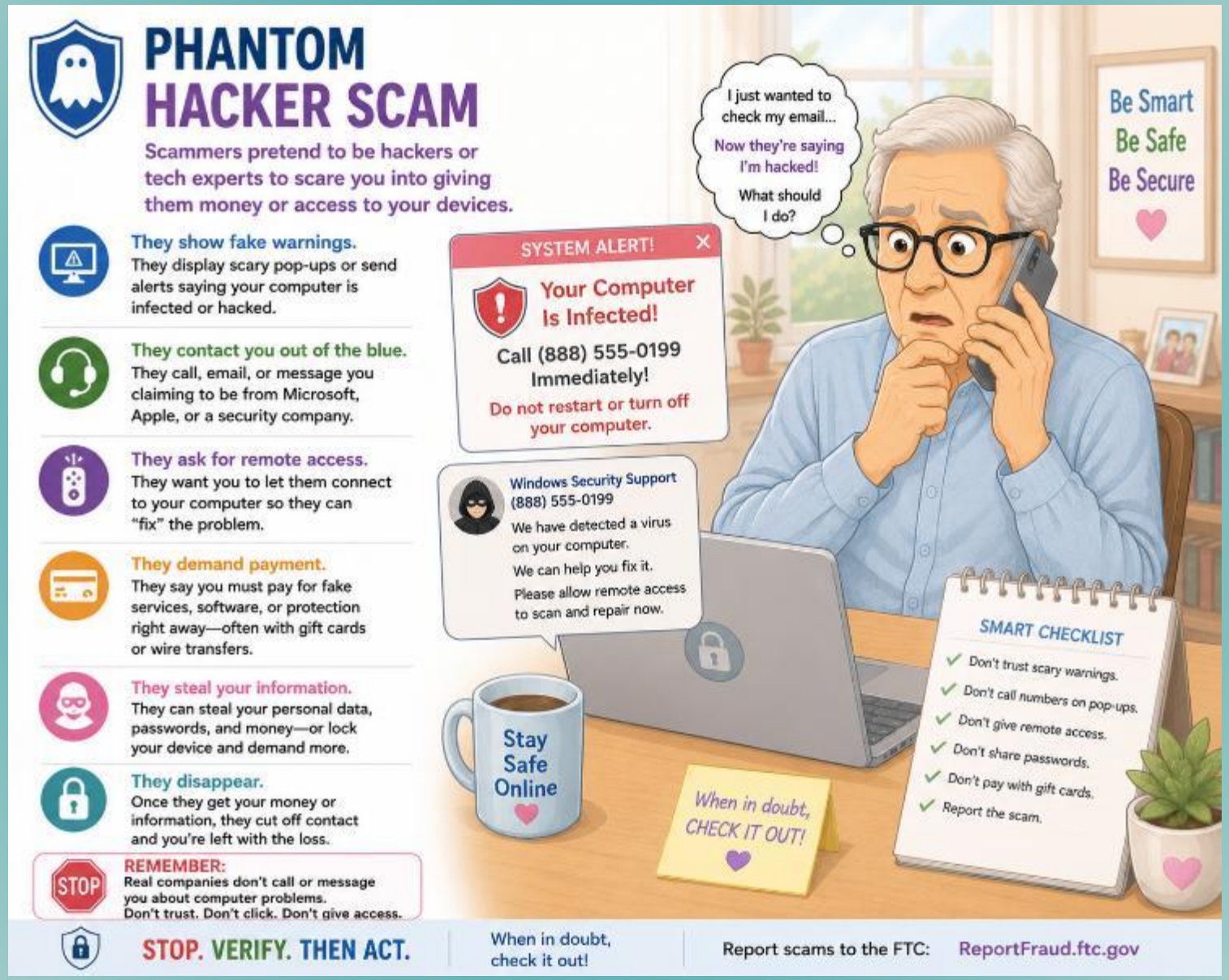
STOP • VERIFY • THEN ACT

Phantom Hacker Scams

HOW IT WORKS	RED FLAGS	WHAT TO DO
• A pop-up alarm warns that your computer has been hacked	• An alarming pop-up message with a phone number to call for help	• Close the pop-up — never call a number shown in a pop-up alarm
• You reach a fake 'tech support' agent who says your bank is at risk	• Multiple strangers call in sequence: tech support, then bank, then government	• No real government agency or bank will ever tell you to move your money
• A second 'bank official' or 'government agent' tells you to move your money	• You are told to keep this secret from your family	• Tell a trusted family member or friend immediately
• The 'protected account' belongs to the scammer — your money is gone	• You are instructed to withdraw cash or buy gold bars to 'protect' it	• Report to the FBI at ic3.gov and the FTC at ReportFraud.ftc.gov

STOP • VERIFY • THEN ACT

Phantom Hacker Scams



STOP • VERIFY • THEN ACT

QR Code Scams (Quishing)

HOW IT WORKS

- Scammers place fake QR stickers over real ones on meters or menus
- They also send fake QR codes by email or text message
- Scanning takes you to a fake website designed to steal your info
- The fake site may ask for your credit card, login, or personal details

RED FLAGS

- A QR sticker looks placed on top of another — look for raised edges
- Scanning leads to an unexpected or unfamiliar website address
- Code was sent by an unknown contact via text or email
- You are told to scan urgently to claim a prize or pay a bill

WHAT TO DO

- Inspect QR stickers before scanning — if tampered with, do not scan
- Type website addresses directly into your browser instead of scanning
- If you scanned a suspicious code, do not enter any personal info
- Call your bank immediately if you entered financial information

STOP • VERIFY • THEN ACT

QR Code Scams (Quishing)

STOP • VERIFY • THEN ACT

Romance Scams

HOW IT WORKS	RED FLAGS	WHAT TO DO
• Scammer creates a fake profile on a dating site or social media	• They never agree to meet in person — always have an excuse	• Never send money to someone you have not met in person
• Builds a warm relationship over weeks or months	• They declare love or deep affection very quickly	• Do a reverse image search of their profile photo
• Claims to be a military member, doctor, or professional overseas	• They avoid live video calls or the video is blurry and brief	• Share the profile with a trusted friend or family member
• Eventually creates an emergency and asks you to send money	• They ask for money, gift cards, wire transfers, or cryptocurrency	• Report romance scams to the FTC at ReportFraud.ftc.gov

STOP • VERIFY • THEN ACT

Romance Scams

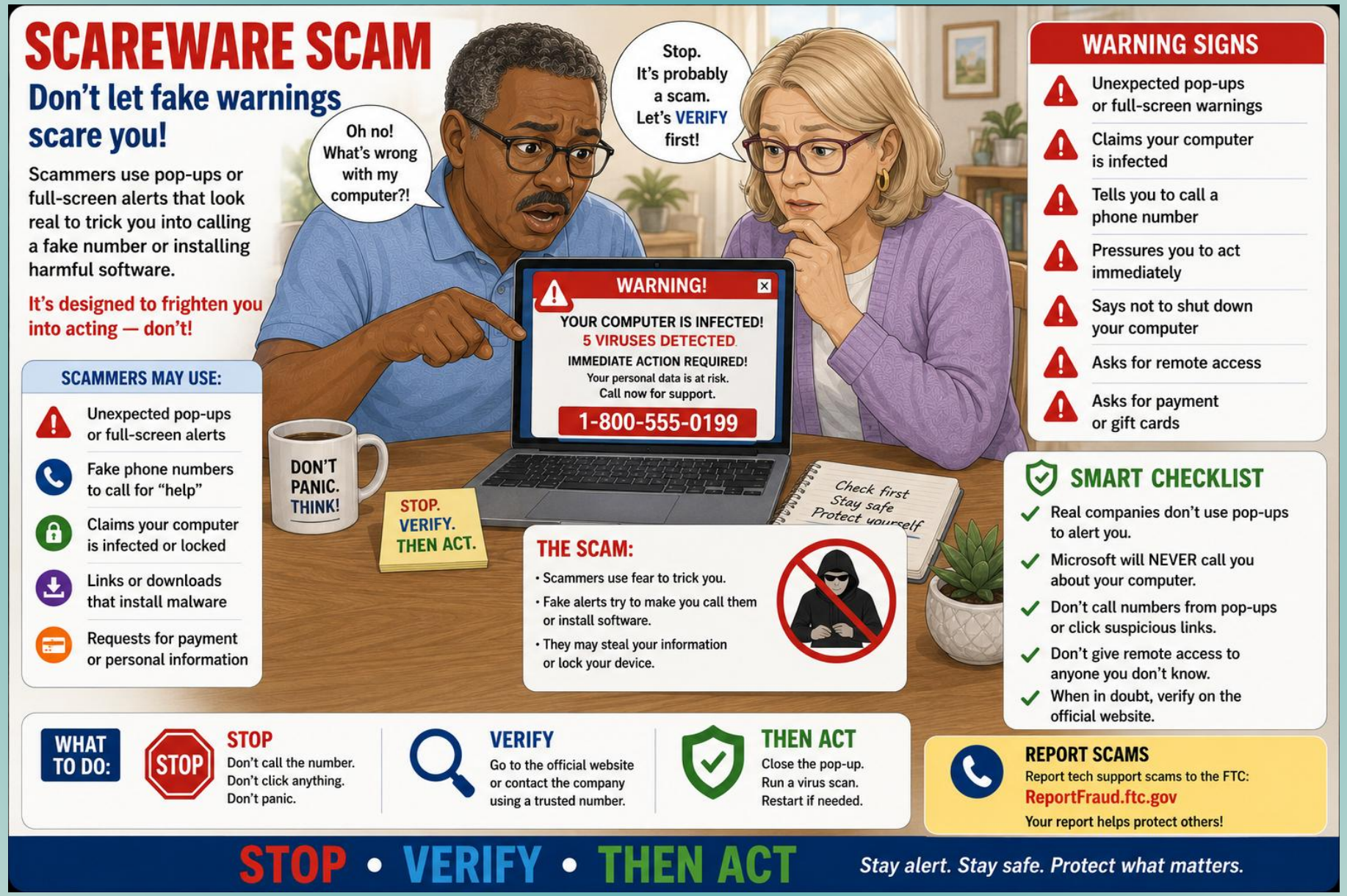
STOP • VERIFY • THEN ACT

Scareware Scam

HOW IT WORKS	RED FLAGS	WHAT TO DO
• Urgent pop-ups and flashing warnings that demand immediate action • Pop-ups that lock the screen • Clicking X doesn't do anything • The goal is to panic you into calling a fake support number	• Claims to be a tech company • Claims your computer is infected • Fake virus scans that run • Claims your data will be deleted • Requests remote access • Asks for gift card payment • Provides a phone number to call	• Do Not Click on the Alert • Close the Browser or Program • Can't do that? • Pull the plug • DO NOT restore the browser • Clear Your Browser Cache • Run a Full Antivirus Scan • Monitor Bank Statements

STOP • VERIFY • THEN ACT

Scareware Scam



STOP • VERIFY • THEN ACT

Subscription Renewal Scams

HOW IT WORKS	RED FLAGS	WHAT TO DO
• An email or pop-up says a subscription is auto-renewing for a large fee • It tells you to call a number immediately to cancel • When you call, scammer asks to access your computer to 'process a refund' • They steal your banking info or install harmful software	• The renewal charge seems unusually high — often $299 to $499 • Urgent message: 'Call within 24 hours to avoid being charged' • You are asked to buy gift cards to receive your refund • Caller asks to take remote control of your computer	• Do not call the number listed in the email or pop-up • Check your real account by typing the company's website yourself • Never give remote access unless you called the company first • If you shared bank info, call your bank immediately

STOP • VERIFY • THEN ACT

Subscription Renewal Scams

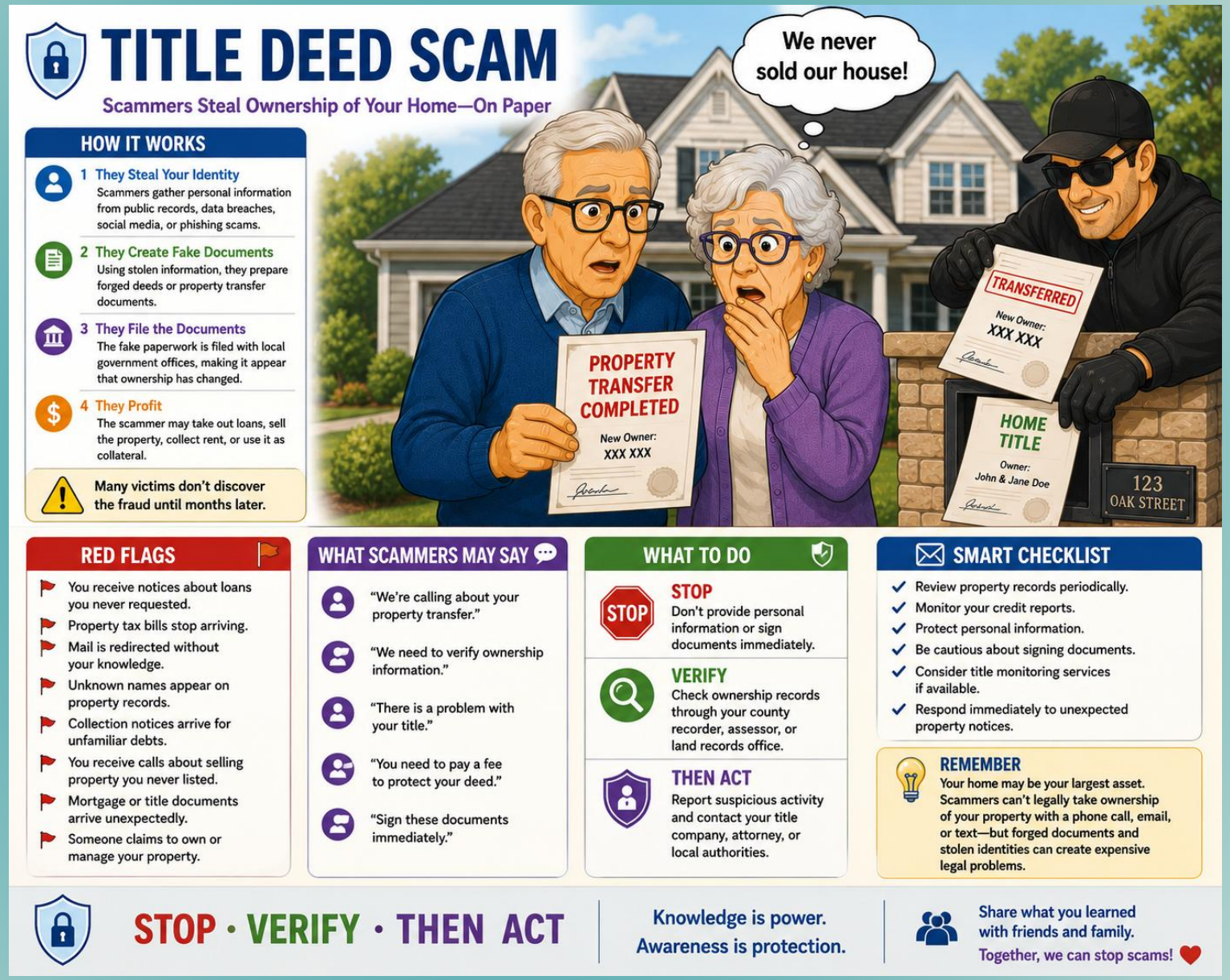
STOP • VERIFY • THEN ACT

Title Deed Scams

HOW IT WORKS	RED FLAGS	WHAT TO DO
• An email or pop-up says a subscription is auto-renewing for a large fee	• The renewal charge seems unusually high — often $299 to $499	• Do not call the number listed in the email or pop-up
• It tells you to call a number immediately to cancel	• Urgent message: ‘Call within 24 hours to avoid being charged’	• Check your real account by typing the company’s website yourself
• When you call, scammer asks to access your computer to ‘process a refund’	• You are asked to buy gift cards to receive your refund	• Never give remote access unless you called the company first
• They steal your banking info or install harmful software	• Caller asks to take remote control of your computer	• If you shared bank info, call your bank immediately

STOP • VERIFY • THEN ACT

Title Deed Scams



STOP • VERIFY • THEN ACT

Tech Support Scam

HOW IT WORKS	RED FLAGS	WHAT TO DO
• A pop-up, text, email, or phone call claims your computer is infected. • Scammers pretend to be from Microsoft, Apple, Google, or a security company. • They ask you to call a number or allow remote access to your computer. • They claim to find problems and demand payment to "fix" them.	• Unsolicited calls or alarming pop-up warnings. • Requests for remote access to your device. • Demands for payment by gift card, wire transfer, or cryptocurrency. • Pressure to act immediately or risk losing your computer or data.	• Close the pop-up or hang up the phone. • Never allow remote access to someone who contacted you first. • Contact the company directly using its official website. • Run your own security scan and seek help from a trusted source.

STOP • VERIFY • THEN ACT

Tech Support Scam

STOP • VERIFY • THEN ACT

Utility Shutoff Scams

HOW IT WORKS

- Caller claims to be from your electric, gas, or water company
- Says your account is overdue and service will be shut off within the hour
- Demands immediate payment to prevent disconnection
- Insists on payment by gift card, wire transfer, or prepaid debit card

RED FLAGS

- Extreme urgency — 'Pay in 30 minutes or your power will be cut'
- Caller ID appears to show your utility company — it can be faked
- They demand payment by gift card — utilities NEVER do this
- Call comes during a holiday, weekend, or after business hours

WHAT TO DO

- Hang up immediately
- Call your utility company using the number on your bill
- Log into your account online to check your actual balance
- Report the scam to the FTC at ReportFraud.ftc.gov

STOP • VERIFY • THEN ACT

Utility Shutoff Scams

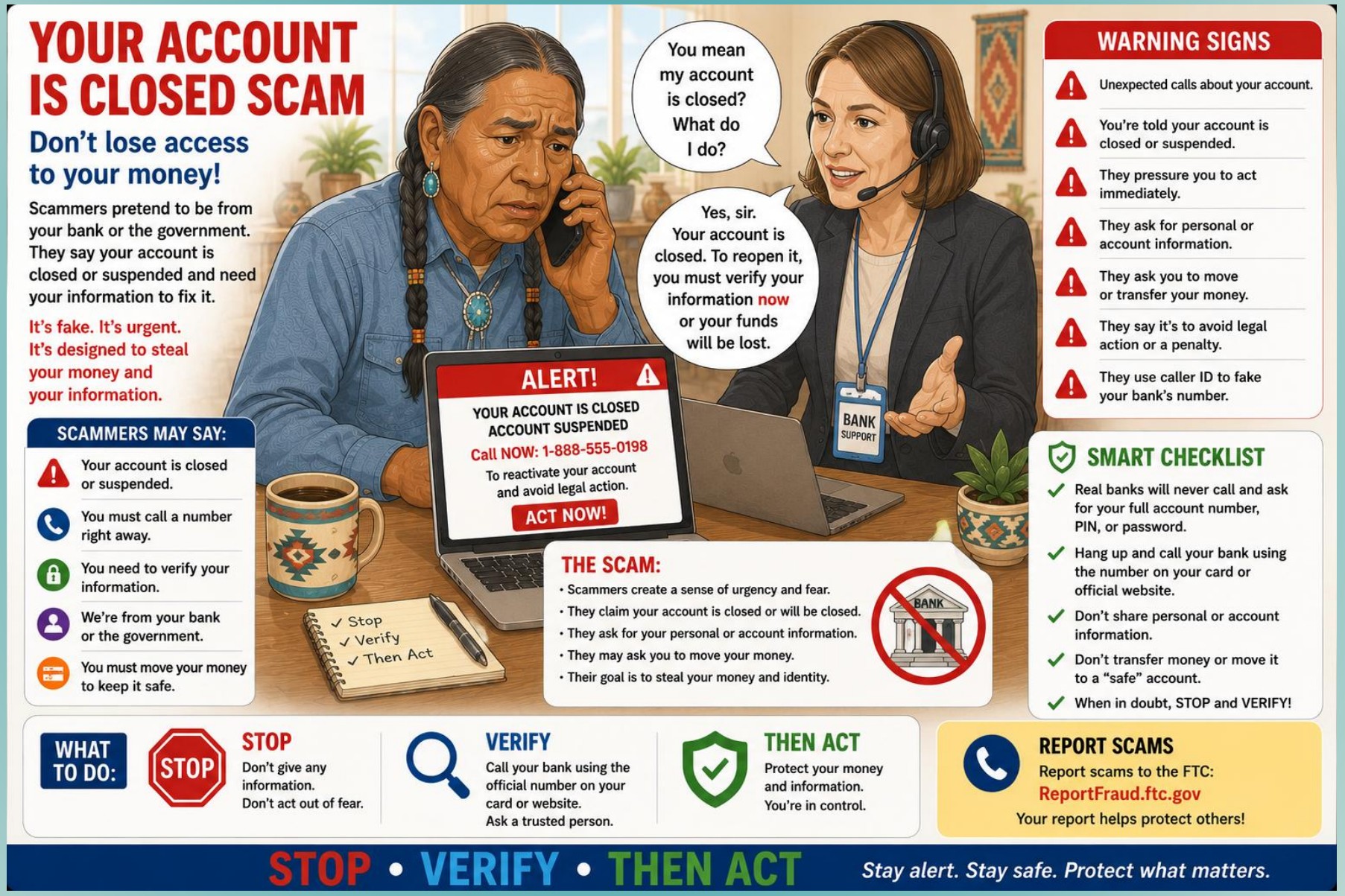
STOP • VERIFY • THEN ACT

Your Account Is Closed Scams (F)

HOW IT WORKS	RED FLAGS	WHAT TO DO
• You receive a text, email, or robocall: your account has been suspended • A link or phone number is provided to reactivate your account immediately • Clicking the link opens a fake website that looks exactly like the real company • You enter your login and personal info — now the scammer has it	• You did not request any changes to your account • Extreme urgency: 'Act within 24 hours or your account will be deleted' • The email sender address looks slightly wrong or unofficial • The link does not match the real company's web address	• Do NOT click any link in the text, email, or pop-up message • Open a new browser window and type the company's real website yourself • Call the customer service number on the back of your card • Report phishing to the FTC at ReportFraud.ftc.gov

STOP • VERIFY • THEN ACT

Your Account Is Closed Scam



STOP • VERIFY • THEN ACT

QUICK SCAM TIPS

Scammers are clever. You can be smarter.

1. STOP AND THINK

Scammers create urgency to pressure you.

Take a moment. Don't rush.

2. VERIFY FIRST

Contact the company or person using a phone number or website you know is real.

Don't use links or numbers from unexpected messages.

3. PROTECT YOUR INFO

Never share personal, financial, or account information unless you initiated the contact.

Real organizations won't ask for it that way.

4. DON'T CLICK OR DOWNLOAD

Avoid clicking on links or downloading attachments in unexpected messages.

They may steal your info or install malware.

5. PAY SAFELY

Use secure payment methods. Avoid paying with gift cards, wire transfers, or cryptocurrency.

These are red flags.

6. REPORT SUSPICIOUS CONTACTS

If something feels wrong, trust your instincts.

Report scams to help protect others.

BE ALERT. BE AWARE.
STAY SAFE.

REPORT SCAMS:
ReportFraud.ftc.gov

SCAMMERS USE THREE POWERFUL TOOLS:

FEAR

Your computer is infected!

Act now or lose your data!

They scare you to get you to act without thinking.

URGENCY

Act NOW!

Time is running out!

Do it today or else!

They pressure you to make quick decisions.

TRUST

I'm from Microsoft.

I'm your grandchild.

I work for the bank.

They pretend to be someone you know and trust.

STOP
Stop and take a breath.

VERIFY
Verify the story before you act.

THEN ACT
Then make a safe and smart decision.

Remember: If they contacted you unexpectedly and want money or information, it's probably a scam.

Quick Tips & Important Resources

YOUR FIVE GOLDEN RULES

SLOW DOWN
Scammers create panic on purpose. Take a breath.

HANG UP
Always okay to hang up and call back on a number you look up.

NO GIFT CARDS
No legitimate agency, bank, or company ever asks for gift cards.

TALK TO SOMEONE
Call a trusted friend or family member before you act.

WHEN IN DOUBT — DON'T
You always have the right to say no and hang up.

KEY CONTACTS TO REPORT FRAUD

FTC — Federal Trade Commission
ReportFraud.ftc.gov | 1-877-382-4357

FBI — Internet Crime Complaint
ic3.gov (file a report online)

AARP Fraud Watch Network
1-877-908-3360 (free helpline)

Medicare Fraud Hotline
1-800-HHS-TIPS (1-800-447-8477)

Social Security Fraud
1-800-269-0271 or oig.ssa.gov

STOP • VERIFY • THEN ACT

Your Safety Rules — Always Remember

• **SLOW DOWN**	Scammers create panic and urgency on purpose. Take a breath first.
• **HANG UP**	You can always call back on a number you look up yourself.
• **NEVER PAY WITH GIFT CARDS**	No real government agency, utility, or bank ever asks for gift cards.
• **TALK TO SOMEONE YOU TRUST**	Before sending money or giving info, call a family member or friend.
• **REPORT IT**	FTC: ReportFraud.ftc.gov | FBI: ic3.gov | AARP: 1-877-908-3360

"When in doubt — don't. You always have the right to hang up and check."

STOP • VERIFY • THEN ACT