

STOP • VERIFY • THEN ACT

A Senior's Everyday Scam Prevention Guide



Protecting Yourself from Today's Most Common Scams



IMPOSTER SCAMS

When Scammers Pretend to Be Someone You Trust



STOP



VERIFY



THEN ACT

CAPTCHA Safety Scams

HOW IT WORKS

- A box appears on a website asking you to prove you are not a robot
- On fake or hacked sites, clicking it secretly installs harmful software
- Some fake CAPTCHAs ask you to copy and paste a command into your computer
- Following the instructions gives scammers access to your device and files

RED FLAGS

- The CAPTCHA appears on a website you did not intentionally visit
- It asks you to press unusual keyboard combinations
- It asks you to copy and paste text or a command into your computer
- You are asked to download a file to 'complete verification'

WHAT TO DO

- Close the browser tab immediately if CAPTCHA instructions seem unusual
- Real CAPTCHAs only ask you to click a checkbox or identify photos
- Never copy and paste commands into your computer from a website
- Keep your computer's security software and browser updated

CAPTCHA Safety Scams



CAPTCHA SCAM (I'M NOT A ROBOT... OR AM I?)

Scammers trick you with a fake "I'm not a robot" test to gain access to your device or personal information.



You see a CAPTCHA pop-up on a website. ✓



You click "I'm not a robot" or "Allow" to continue. ✓



Hidden malicious code is downloaded to your device. ✓



Scammers can steal your information, track you, or take control of your device.



REMEMBER:

If a CAPTCHA looks strange or appears when you weren't expecting it—
DON'T CLICK! Close the window.



Celebrity Scams

HOW IT WORKS

- 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

RED FLAGS

- 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

WHAT TO DO

- 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

Celebrity Scams



IMPOSTER SCAM

(Celebrity Scam)

Scammers pretend to be a celebrity to gain your trust and ask for money or gifts.



They may contact you on social media, email, or texting apps.



They say they "like" you and want a special relationship.



They ask for gift cards, money, or help with a personal emergency.



The relationship is not real – it's all a scam.



Remember:

Celebrities don't contact fans privately asking for money or gifts. If in doubt, it's a **SCAM!**

STOP.
VERIFY.
THEN ACT.

STOP. VERIFY. THEN ACT.

Protect Yourself. Protect Your Money. Protect Your Future.



● STOP • VERIFY • THEN ACT

Fake Bank & Credit Card Fraud Calls

HOW IT WORKS

- Caller claims to be from your bank or credit card company
- Says suspicious activity has been detected on your account
- Asks you to verify your account number, SSN, or PIN
- May ask you to transfer money to a 'safe' account

RED FLAGS

- Pressure to act immediately or your money will be lost
- Caller already knows some of your info to seem legitimate
- Asks for your full card number, CVV code, or PIN
- Requests payment via wire transfer or gift card

WHAT TO DO

- Hang up immediately — do not stay on the line
- Call the number on the back of your bank card yourself
- Banks never ask you to move money to a 'safe account'
- Report the call to your bank's fraud department



STOP • VERIFY • THEN ACT

Fake Bank & Credit Card Fraud Calls

FAKE BANK & CREDIT CARD FRAUD CALLS

Scammers pretend to be from your bank or credit card company and try to steal your money or personal information.

They sound convincing. Don't be fooled!



SCAMMER MAY SAY:

- There's been suspicious activity on your account.
- We need to verify your account information.
- You could be charged if you don't act now.
- Press 1 to speak with an agent.
- We need you to install software to protect your account.

THE SCAM:

They may know a little about you.
They use fear and urgency to trick you into giving personal or financial information.
They may also ask for remote access or payment.



WARNING SIGNS

- You get an unexpected call about your account.
- They claim there's a problem or "fraud" on your account.
- They ask for personal or card information.
- They ask for online banking login or one-time codes.
- They ask you to move your money or send payments.
- They pressure you to act immediately.

SMART CHECKLIST

- Your bank will NEVER call and ask for your PIN, full card number, or one-time codes.
- Don't share personal or account information.
- Don't click links or call numbers from suspicious callers.
- Hang up and call your bank using the number on the back of your card or their official website.
- When in doubt, check it out!

WHAT TO DO:



STOP
Don't give any information.
Don't panic.



VERIFY

Hang up.
Contact your bank using the official number on your card or website.



THEN ACT

Protect your account.
Report the call.
You're in control.



REPORT SCAMS

Report scam calls to the FTC:
[ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud)

Your report helps protect others!

STOP • VERIFY • THEN ACT

Stay alert. Stay safe. Protect what matters.

STOP • VERIFY • THEN ACT

Fake Government Calls

HOW IT WORKS

- Caller claims to be from the IRS, Social Security, or law enforcement
- Says you owe back taxes or there is a warrant for your arrest
- Demands immediate payment to avoid arrest or loss of benefits
- Caller ID may show a real government number — this can be faked

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

- Hang up — government agencies do NOT demand instant phone payment
- The IRS contacts taxpayers by mail first — never by phone
- Call the agency directly from their official website
- Report the call to the FTC at [ReportFraud.ftc.gov](https://www.ftc.gov/ReportFraud)

Fake Government Calls



FAKE GOVERNMENT CALLS SCAM

Scammers pretend to be from the government to scare you and steal your money or personal information.



They call and say you owe money or have a problem with the IRS, Social Security, or Medicare.



They threaten you. They may say you'll be arrested, sued, or have your benefits suspended.



They demand payment. They tell you to pay with gift cards, wire transfers, or cryptocurrency.



They ask for personal information. They may ask for your Social Security number, bank account number, or credit card information.



REMEMBER: Government agencies will NEVER call to demand payment or ask for personal or financial information. **HANG UP. IT'S A SCAM!**



STOP. VERIFY. THEN ACT.



Scammers count on fear. You can count on **KNOWLEDGE.**

Report scams to the FTC: [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud)

● **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.

Grandparent's Scam



GRANDPARENTS SCAM

Scammers pretend to be a grandchild in trouble and ask for money.



They contact you suddenly.
You get a call, text, or message saying, "Hi Grandma, it's me."



They say it's an emergency.
They may say they lost their phone, are in trouble, or need money fast.



They ask for money.
They may ask you to send money, buy gift cards, or wire funds.



They tell you to keep it a secret.
They may say, "Don't tell Mom or Dad. It's a surprise!"



They steal your money.
Once they get the money, they disappear.



REMEMBER:
It could be a scam. Take a breath.
Don't rush. Don't send money.
Check it out!

Grandson

Hi Grandpa, it's me. I'm in a bind and need \$1,000 fast. Can you help?

10:24 AM

Oh no... My grandson needs help!

I lost my phone and my wallet. I need help right now!

Got him! Easy money!



CHECK IT OUT!

- ✓ Call another family member.
- ✓ Use a known phone number.
- ✓ Ask a question only they would know.
- ✓ Don't send money.
- ✓ Report the scam.

When in doubt, CHECK IT OUT!

Be Smart
Be Safe
Be Secure



STOP. VERIFY. THEN ACT.

Scammers count on love.
You can count on KNOWLEDGE.

Report scams to the FTC: [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud)

STOP • VERIFY • THEN ACT

Investment & Cryptocurrency Scams

HOW IT WORKS

- Someone promises guaranteed high returns on stocks or cryptocurrency
- They show you fake account screens with impressive growing profits
- They encourage you to invest more money as your 'balance' grows
- When you try to withdraw, your money is gone

RED FLAGS

- Guaranteed returns with no risk — this does NOT exist in real investing
- Pressure to invest quickly before the 'opportunity closes'
- You are asked to invest through an app or platform they control
- Promises of secret tips or insider knowledge

WHAT TO DO

- Never invest based on an unsolicited call or online relationship
- Check any investment at investor.gov (the SEC's official site)
- Talk to a trusted family member before moving any money
- Report suspected investment fraud to the FTC and the SEC

Investment & Cryptocurrency Scams

INVESTMENT & CRYPTOCURRENCY SCAM

Scammers promise high returns to steal your money.

- They promise big profits.** They say you'll get rich quick with little or no risk. If it sounds too good to be true, it probably is!
- They use fake testimonials.** They show fake reviews or celebrity endorsements to make it look real.
- They direct you to fake websites.** Their websites may look official but are designed to steal your money and personal information.
- They push cryptocurrency.** They may ask you to buy crypto and send it to them—once it's sent, it's almost impossible to get back.
- They pressure you to act fast.** They create urgency so you don't have time to think or talk to someone you trust.

REMEMBER: Real investments don't guarantee huge returns or pressure you to act. **Do your research. Check it out!**

STOP. VERIFY. THEN ACT.

Scammers want your money. Knowledge protects you.

Report scams to the FTC: [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud)

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

Lost Pet Scam

LOST PET SCAM






A scammer's trick to steal your heart and your money.

Scammers create fake ads about lost or found pets to steal your money—and your heart.

Is this really our dog?

The ad looks real, but let's not rush. Let's **VERIFY** first.

SCAMMERS MAY SAY:

-  We found your pet! Click here for details.
-  You need to pay a fee to get your pet back.
-  Send money by gift card, wire transfer, or an app.
-  Act fast—someone else wants your pet!
-  We just want to help reunite you.

THE SCAM:

- Scammers post fake ads with pets that don't belong to them.
- They use your emotions to rush you.
- They ask for money, fees, or payments before you see your pet.
- After you pay, they disappear—and so does your pet.



WHAT TO DO:



STOP
Don't send money.
Don't act out of emotions.



VERIFY
Check the story.
Research the ad and image. Ask questions.



THEN ACT
Meet in person.
Use safe payment methods. You're in control.



REPORT SCAMS

Report pet scams to the FTC:
[ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud)
Your report helps protect others!

WARNING SIGNS

-  The pet looks like yours, but the story doesn't add up.
-  They won't meet in person or let you see the pet.
-  They ask for payment before you see your pet.
-  They say they're out of town or can't meet.
-  They pressure you to act fast.
-  They won't answer video calls or provide details.

SMART CHECKLIST

- ✓ Search online for the pet image—it may be stolen.
- ✓ Ask for a video call to see your pet.
- ✓ Meet in person in a public place.
- ✓ Don't send money before you see your pet.
- ✓ Use safe payment methods (credit card with protection).
- ✓ If it feels wrong, STOP and check it out!

STOP • VERIFY • THEN ACT

Stay alert. Stay safe. Protect what matters.

STOP • VERIFY • THEN ACT

Lottery, Sweepstakes & Prize Scams

HOW IT WORKS

- You receive a call, letter, or email: you have won a large prize!
- You may be told you won a lottery you never entered
- To collect your prize, you must pay taxes, fees, or customs upfront
- Once you pay, the scammer disappears — there is no prize

RED FLAGS

- You must pay any amount of money to receive a prize
- You won a lottery or sweepstakes you don't remember entering
- Payment required by wire transfer, gift card, or money order
- Caller urges secrecy: 'Do not tell your family yet'

WHAT TO DO

- Legitimate sweepstakes NEVER require you to pay to collect a prize
- Hang up the phone or throw away the letter
- Never send money, gift cards, or personal info to claim a prize
- Report the scam to the FTC at [ReportFraud.ftc.gov](https://www.ftc.gov/ReportFraud)

Lottery, Sweepstakes & Prize Scams

LOTTERY, SWEEPSTAKES & PRIZE SCAMS

Scammers say you've won big prizes you never entered to take your money or information.

- They say you've won.** You get a call, text, email or letter saying you won a lottery or prize—but you never entered.
- They ask for fees or taxes.** They say you must pay upfront fees, taxes, or shipping costs to claim your prize.
- They want payment or gift cards.** They ask you to pay with gift cards, wire transfers, crypto, or prepaid cards.
- They ask for personal information.** They may ask for your bank details, Social Security number, or other personal information.
- They pressure you to act fast.** They create urgency, saying the offer will expire or you'll lose your prize.
- Then they disappear.** After you pay or share information, they vanish—no prize, no refund.

REMEMBER: If you didn't enter, you can't win! Be smart. Check it out!

CONGRATULATIONS!
You've won \$1,000,000! 🎁
Claim your prize now!
Call 1-800-555-PRIZE

You're a Winner!
You've been selected to receive a \$500 Gift Card or \$5,000 Cash!
Click here to claim now!

FINAL NOTICE!
Pay \$199 processing fee within 24 hours or your prize will be forfeited!

SMART CHECKLIST

- ✓ Did I enter?
- ✓ Who is the company?
- ✓ How did they get my contact?
- ✓ Do I have to pay anything upfront?
- ✓ Have I checked with an independent source?
- ✓ When in doubt, don't respond.

BIG PRIZES!

- ✓ Cash
- ✓ Cars
- ✓ Vacations
- ✓ Electronics and more!

When in doubt, CHECK IT OUT!

Stay Safe Online

YOU COULD BE NEXT!
WIN BIG!
ACT NOW!

I didn't enter anything... Is this real?

It sounds too good to be true! Let's check it out first.

STOP. VERIFY. THEN ACT.

Scammers promise prizes. Knowledge protects you.

Report scams to the FTC: [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud)

Medicare & Health Insurance Scams

HOW IT WORKS

- Caller claims to be from Medicare or your insurance company
- Offers free equipment, genetic testing kits, or a new Medicare card
- Asks for your Medicare number or Social Security number
- Uses your number to bill for services you never received

RED FLAGS

- Unsolicited call about your Medicare coverage or benefits
- Request for your Medicare ID number over the phone
- 'Free' offers that require personal or insurance information
- Threats that your Medicare coverage will be cancelled

WHAT TO DO

- Hang up immediately on all unsolicited Medicare calls
- Call Medicare directly: 1-800-MEDICARE (1-800-633-4227)
- Never give your Medicare number to an unsolicited caller
- Report Medicare fraud: 1-800-HHS-TIPS (1-800-447-8477)

Medicare & Health Insurance Scams



MEDICARE & HEALTH INSURANCE SCAM

Scammers pretend to be from Medicare or health insurance companies to steal your money or personal information.



They call you.
They say they're from Medicare or your health insurance company. Caller ID can be faked.



They create urgency.
They say your coverage will end, you owe money, or you must act today to avoid a penalty.



They offer "free" benefits.
They promise free medical supplies, tests, or services that Medicare doesn't cover.



They ask for personal information.
They may ask for your Medicare number, Social Security number, bank info, or credit card details.



They want payment.
They may ask you to pay for "covered" services, rebates, or to keep your coverage active.



They steal your identity and money.
They can use your information to commit fraud or bill Medicare for services you never received.



REMEMBER:
Medicare will NEVER call you to sell anything or ask for personal information or payment.
HANG UP. PROTECT. REPORT.



STOP. VERIFY. THEN ACT.

Protect your Medicare.
Protect your health. Protect your future.

Report scams to the FTC: [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud)

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](https://www.ftc.gov/ReportFraud)



Online Pet Scams

ONLINE PET SCAMS

The puppy you want may not be real.

Scammers create fake ads for puppies or kittens to steal your money—and your heart.

Cute photos.
Fake stories.
Real losses.

SCAMMER MAY SAY:

- I'm moving and need to rehome my pet.
- Shipping is available anywhere!
- Send a deposit to hold the pet.
- You'll get lots of photos and updates!

He's so adorable! I want him!

The seller seems nice. Let's send the deposit.

Adorable Puppy – Ready Now!



Vet checked
Up to date on shots
Health guarantee
Shipping available

Only \$500!

Send Deposit



Too good to be true?
CHECK FIRST!

Ask questions.
Verify everything.
Protect your heart
and your money.

WARNING SIGNS

- The price is much lower than usual.
- The seller won't let you see the pet in person.
- They make excuses about why you can't visit.
- They ask for payment by wire transfer, gift card, or payment app.
- They pressure you to send money quickly.
- The ad uses photos that look like stock pictures.

SMART CHECKLIST

- ✓ Search the ad and photos online—are they used elsewhere?
- ✓ Ask for a video call to see the pet live.
- ✓ Get the seller's full name, address, and contact info.
- ✓ Use secure payment methods (credit card with protection).
- ✓ If something feels off, STOP and walk away.

THE SCAM:

You pay a deposit or full amount, but the pet never arrives.
The seller disappears—or sends excuses.
You lose your money and your new pet.



WHAT TO DO:



STOP

Don't send money.
Don't act out of emotions.



VERIFY

Research the seller.
Check the ad, photos, and pet information.
Verify everything.



THEN ACT

Use safe payment methods.
Only after you've verified.



REPORT SCAMS

Report pet scams to:
[ReportFraud.ftc.gov](https://www.ftc.gov/identity-theft/identity-theft-reporting)

Your report helps protect others!

STOP • VERIFY • THEN ACT

Stay alert. Stay safe. Protect what matters.

STOP • VERIFY • THEN ACT

Password Reset & Email Security Scams

HOW IT WORKS

- You receive an email or text saying your password must be reset now
- Message warns your account will be locked or deleted if you don't act
- The link leads to a fake website that looks like the real company
- You enter your login — now the scammer has your account

RED FLAGS

- Urgent language: 'Act now or lose access permanently'
- Email sender address looks slightly off or misspelled
- The link URL does not match the company's real website
- You did not request a password reset

WHAT TO DO

- Delete the email or text — do not click any links
- Type the company's website address directly in your browser
- Enable two-step verification on all important accounts
- Call the company's official customer service if unsure

Password Reset & Email Security Scams



PASSWORD RESET & EMAIL SECURITY SCAM

Scammers pretend to be from trusted companies to steal your passwords, money, and personal information.



They send fake emails.

They pretend to be from companies you know—like your email provider, bank, or other services.



They create urgency.

They say your account will be locked or closed unless you act right away.



They trick you to click.

They include links or buttons that look real but take you to fake websites designed to steal your information.



They ask for login details.

They ask for your password, security codes, or personal information—but real companies never do.



They take over your account.

Once they have your info, they can steal your identity, your money, and lock you out.



REMEMBER:

Don't click. Don't share. Don't trust. When in doubt, go to the official website by typing it into your browser. Be smart. Be safe. Protect your accounts.

This looks urgent... Is this real?



Important: Security Alert

From: Account Support

We noticed unusual activity on your account. To keep your account secure, please reset your password now.

Reset Password

Or click here



STOP. VERIFY. THEN ACT.

Your security is in your hands.

Report scams to the FTC: [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud)

STOP • VERIFY • THEN ACT

Phantom Hacker Scams

HOW IT WORKS

- A pop-up alarm warns that your computer has been hacked
- You reach a fake 'tech support' agent who says your bank is at risk
- A second 'bank official' or 'government agent' tells you to move your money
- The 'protected account' belongs to the scammer — your money is gone

RED FLAGS

- An alarming pop-up message with a phone number to call for help
- Multiple strangers call in sequence: tech support, then bank, then government
- You are told to keep this secret from your family
- You are instructed to withdraw cash or buy gold bars to 'protect' it

WHAT TO DO

- Close the pop-up — never call a number shown in a pop-up alarm
- No real government agency or bank will ever tell you to move your money
- Tell a trusted family member or friend immediately
- Report to the FBI at ic3.gov and the FTC at ReportFraud.ftc.gov



Phantom Hacker Scams

PHANTOM HACKER SCAM

Scammers pretend to be hackers or tech experts to scare you into giving them money or access to your devices.

They show fake warnings. They display scary pop-ups or send alerts saying your computer is infected or hacked.

They contact you out of the blue. They call, email, or message you claiming to be from Microsoft, Apple, or a security company.

They ask for remote access. They want you to let them connect to your computer so they can “fix” the problem.

They demand payment. They say you must pay for fake services, software, or protection right away—often with gift cards or wire transfers.

They steal your information. They can steal your personal data, passwords, and money—or lock your device and demand more.

They disappear. Once they get your money or information, they cut off contact and you’re left with the loss.

REMEMBER: Real companies don’t call or message you about computer problems. Don’t trust. Don’t click. Don’t give access.

STOP. VERIFY. THEN ACT.

When in doubt, check it out!

Report scams to the FTC: [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud)

SYSTEM ALERT!
Your Computer Is Infected!
Call (888) 555-0199 Immediately!
Do not restart or turn off your computer.

Windows Security Support (888) 555-0199
We have detected a virus on your computer. We can help you fix it. Please allow remote access to scan and repair now.

SMART CHECKLIST

- ✓ Don't trust scary warnings.
- ✓ Don't call numbers on pop-ups.
- ✓ Don't give remote access.
- ✓ Don't share passwords.
- ✓ Don't pay with gift cards.
- ✓ Report the scam.

I just wanted to check my email... Now they're saying I'm hacked! What should I do?

Be Smart
Be Safe
Be Secure

Stay Safe Online

When in doubt, CHECK IT OUT!

● 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



QR Code Scams (Quishing)

QR CODE SCAMS

Don't scan without thinking!

Scammers use fake QR codes to steal your money, login information, or install malware on your device.

SCAMMERS MAY USE QR CODES TO:

- Take you to fake payment sites.
- Steal account login information.
- Install malware or spyware.
- Collect personal information.



I'll scan this QR code to see the menu.

STOP AND THINK!
Not every QR code is safe.



WARNING SIGNS

- A QR code in an unexpected place.
- No information about where the QR code will take you.
- The QR code is covering up something else.
- The offer seems too good to be true.
- You're pressured to scan immediately.
- You don't recognize the company or source.

THE SCAM:

- The QR code may look real, but it could take you to a fake website.
- You might be asked to enter personal or payment info.
- Malware could be downloaded to your device without you knowing.



SMART CHECKLIST

- Ask yourself if the QR code is from a trusted source.
- Look for spelling errors or poor design around the code.
- Don't scan QR codes from emails, texts, or flyers you don't trust.
- Check the link before you enter any information.
- If in doubt, don't scan. Go to the website yourself.

WHAT TO DO:

STOP
Pause before you scan.

VERIFY
Check the source. Is it trustworthy?

THEN ACT
Scan only if you're sure it's safe.

REPORT SCAMS
Report QR code scams to the FTC: [ReportFraud.ftc.gov](https://www.ftc.gov/identity-theft/identity-theft-scams-reports)
Your report helps protect others!

STOP • VERIFY • THEN ACT

Stay alert. Stay safe. Protect what matters.

STOP • VERIFY • THEN ACT

Romance Scams

HOW IT WORKS

- Scammer creates a fake profile on a dating site or social media
- Builds a warm relationship over weeks or months
- Claims to be a military member, doctor, or professional overseas
- Eventually creates an emergency and asks you to send money

RED FLAGS

- They never agree to meet in person — always have an excuse
- They declare love or deep affection very quickly
- They avoid live video calls or the video is blurry and brief
- They ask for money, gift cards, wire transfers, or cryptocurrency

WHAT TO DO

- Never send money to someone you have not met in person
- Do a reverse image search of their profile photo
- Share the profile with a trusted friend or family member
- Report romance scams to the FTC at [ReportFraud.ftc.gov](https://www.ftc.gov/identity-theft/identity-theft-fraud-report)

Romance Scams



ROMANCE SCAM

Scammers pretend to fall in love with you to steal your money or personal information.



They show lots of attention—fast.

They say you're perfect and express strong feelings quickly, even if you just met online.



They communicate off the platform.

They ask to move to email, text, or chat apps to build a "private" connection.



They use stolen photos and stories.

Their photos may be fake or stolen. Their stories might sound too perfect or hard to verify.



They make up excuses to meet.

They say they want to meet in person, but something always comes up—travel, work, or emergencies.



They ask for money.

They may ask for help with medical bills, travel costs, or emergencies. Then they ask for more.



They may steal your information.

They might ask for personal details or use your trust to access your accounts.



REMEMBER:

If you haven't met in person, it could be a scam. Be smart. Check it out!

He understands me like no one else. I think he really cares about me.



YOU ARE NOT ALONE



Romance scammers target kind and caring people.

You did nothing wrong. There is help.



STOP. VERIFY. THEN ACT.

Trust your heart—and your head.

Report scams to the FTC: [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud)



Be smart. Be safe. Be secure.

STOP • VERIFY • THEN ACT

Scareware Scam

HOW IT WORKS

- 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

RED FLAGS

- 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

WHAT TO DO

- 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

Scareware Scam

SCAREWARE SCAM

Don't let fake warnings scare you!

Scammers use pop-ups or full-screen alerts that look real to trick you into calling a fake number or installing harmful software.

It's designed to frighten you into acting — don't!

SCAMMERS MAY USE:

- ⚠️ Unexpected pop-ups or full-screen alerts
- ☎️ Fake phone numbers to call for "help"
- 🔒 Claims your computer is infected or locked
- 📄 Links or downloads that install malware
- 💳 Requests for payment or personal information

WHAT TO DO:



STOP

Don't call the number. Don't click anything. Don't panic.



VERIFY

Go to the official website or contact the company using a trusted number.



THEN ACT

Close the pop-up. Run a virus scan. Restart if needed.



REPORT SCAMS

Report tech support scams to the FTC: [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud)
Your report helps protect others!



WARNING SIGNS

- ⚠️ Unexpected pop-ups or full-screen warnings
- ⚠️ Claims your computer is infected
- ⚠️ Tells you to call a phone number
- ⚠️ Pressures you to act immediately
- ⚠️ Says not to shut down your computer
- ⚠️ Asks for remote access
- ⚠️ Asks for payment or gift cards

SMART CHECKLIST

- ✓ Real companies don't use pop-ups to alert you.
- ✓ Microsoft will NEVER call you about your computer.
- ✓ Don't call numbers from pop-ups or click suspicious links.
- ✓ Don't give remote access to anyone you don't know.
- ✓ When in doubt, verify on the official website.

STOP • VERIFY • THEN ACT

Stay alert. Stay safe. Protect what matters.

STOP • VERIFY • THEN ACT

Subscription Renewal Scams

HOW IT WORKS

- 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

RED FLAGS

- 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

WHAT TO DO

- 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



Subscription Renewal Scams

SUBSCRIPTION RENEWAL SCAM

Scammers send fake notices about subscriptions to steal your money or personal information.

They send fake renewal notices.
They pretend to be from companies you know—like streaming, antivirus, or retailers.

They create urgency.
They say your subscription is about to expire or will be canceled today.

They include links or buttons.
These links may take you to fake websites designed to steal your money or info.

They ask for payment details.
They may ask for your card number, billing info, or say a payment failed.

They pretend to be real.
They use real logos and look-alike emails, but it's all fake.

They can charge you.
They may sign you up for services you don't want or charge you over and over.

REMEMBER:
Real companies don't ask you to click links or call from an email. Check your account directly on the official website or app.
Be smart. Check it out!

SMART CHECKLIST

- ✓ Check the sender's email address
- ✓ Don't click links in emails
- ✓ Go to the official website or app directly
- ✓ Check your account there
- ✓ Monitor your statements
- ✓ Report the scam

STOP. VERIFY. THEN ACT.

Protect your money.
Protect your information.

Report scams to the FTC: [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud)

When in doubt, CHECK IT OUT!

Amount: \$89.99

RENEW NOW CLICK HERE

[No thanks, I'll lose access](#)

Your Subscription Will EXPIRE TODAY!

Renew now to avoid interruption.

**Be Smart
Be Safe
Be Secure**

● STOP • VERIFY • THEN ACT

Title Deed Scams

HOW IT WORKS

- 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

RED FLAGS

- 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


WHAT TO DO

- 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

Title Deed Scams

TITLE DEED SCAM

Scammers Steal Ownership of Your Home—On Paper



HOW IT WORKS

- 1 They Steal Your Identity**
Scammers gather personal information from public records, data breaches, social media, or phishing scams.
- 2 They Create Fake Documents**
Using stolen information, they prepare forged deeds or property transfer documents.
- 3 They File the Documents**
The fake paperwork is filed with local government offices, making it appear that ownership has changed.
- 4 They Profit**
The scammer may take out loans, sell the property, collect rent, or use it as collateral.

Many victims don't discover the fraud until months later.

RED FLAGS

- You receive notices about loans you never requested.
- Property tax bills stop arriving.
- Mail is redirected without your knowledge.
- Unknown names appear on property records.
- Collection notices arrive for unfamiliar debts.
- You receive calls about selling property you never listed.
- Mortgage or title documents arrive unexpectedly.
- Someone claims to own or manage your property.

WHAT SCAMMERS MAY SAY

- "We're calling about your property transfer."
- "We need to verify ownership information."
- "There is a problem with your title."
- "You need to pay a fee to protect your deed."
- "Sign these documents immediately."

WHAT TO DO

STOP
Don't provide personal information or sign documents immediately.

VERIFY
Check ownership records through your county recorder, assessor, or land records office.

THEN ACT
Report suspicious activity and contact your title company, attorney, or local authorities.

SMART CHECKLIST

- Review property records periodically.
- Monitor your credit reports.
- Protect personal information.
- Be cautious about signing documents.
- Consider title monitoring services if available.
- Respond immediately to unexpected property notices.

REMEMBER
Your home may be your largest asset. Scammers can't legally take ownership of your property with a phone call, email, or text—but forged documents and stolen identities can create expensive legal problems.

STOP • VERIFY • THEN ACT

Knowledge is power.
Awareness is protection.

Share what you learned with friends and family.
Together, we can stop scams!

STOP • VERIFY • THEN ACT

Tech Support Scam

HOW IT WORKS

- 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.

RED FLAGS

- 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.

WHAT TO DO

- 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.



Tech Support Scam



TECH SUPPORT SCAM

Scammers pretend to be from a trusted tech company to gain access to your device and steal your information.



They create a fake alert.

A pop-up or warning message claims your computer has a virus or other problem.



They tell you to call.

You're given a phone number to "tech support" to fix it.



They ask for remote access.

They may ask you to install a program so they can "fix" your computer.



They ask for payment.

They may demand payment for the "service" or a warranty.



They steal your information.

They can access your files, steal passwords, or lock your device until you pay.



REMEMBER:

Real tech companies don't call you or show pop-up alerts.
DON'T CALL. DON'T CLICK.



STOP. VERIFY. THEN ACT.

Scammers pretend to help.
You stay in control.

Report scams to the FTC:
[ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud)



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](https://www.ftc.gov/ReportFraud)

Utility Shutoff Scams

UTILITY SHUTDOWN SCAM! ⚠️

Scammers threaten to shut off your power, gas, water, or internet to **STEAL YOUR MONEY OR PERSONAL INFORMATION.**

This is your utility company. Your account is past due. Your service will be **DISCONNECTED TODAY!** Press 1 to make a payment and avoid shut off.

FINAL WARNING! Your account is past due. Your service will be **DISCONNECTED TODAY.** Press 1 to make a payment and avoid disconnection.

DON'T PANIC. DON'T PAY. VERIFY FIRST!

Stay Safe, Stay Smart!

SCAMMERS MAY...

- Call, text, or email saying your service will be shut off **IMMEDIATELY.**
- Demand immediate payment with a prepaid card, gift card, or app.
- Ask for personal or banking information.
- Send fake links to "resolve" the issue.
- Pressure you to act **FAST** and not think.

SMART CHECKLIST

- ✓ Hang up on suspicious calls.
- ✓ Contact the utility company using the number on your bill or their official website.
- ✓ Never click on links or call numbers from unsolicited messages.
- ✓ Protect your personal, account, and financial information.

BE SMART. BE SAFE. BE SECURE.

STOP. CHECK. PROTECT.

- STOP** Stop and don't react right away.
- CHECK** Check with your utility company.
- PROTECT** Protect your money, information, and peace of mind.

When in doubt, **VERIFY BEFORE YOU PAY!**

REPORT SCAMS: [ReportFraud.ftc.gov](https://www.reportfraud.ftc.gov)

● STOP • VERIFY • THEN ACT

Your Account Is Closed Scams (F)

HOW IT WORKS

- 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

RED FLAGS

- 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

WHAT TO DO

- 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](https://www.ftc.gov/report-fraud)

Your Account Is Closed Scam

YOUR ACCOUNT IS CLOSED SCAM

Don't lose access to your money!

Scammers pretend to be from your bank or the government. They say your account is closed or suspended and need your information to fix it.

It's fake. It's urgent. It's designed to steal your money and your information.

SCAMMERS MAY SAY:

-  Your account is closed or suspended.
-  You must call a number right away.
-  You need to verify your information.
-  We're from your bank or the government.
-  You must move your money to keep it safe.



WARNING SIGNS

-  Unexpected calls about your account.
-  You're told your account is closed or suspended.
-  They pressure you to act immediately.
-  They ask for personal or account information.
-  They ask you to move or transfer your money.
-  They say it's to avoid legal action or a penalty.
-  They use caller ID to fake your bank's number.

SMART CHECKLIST

-  Real banks will never call and ask for your full account number, PIN, or password.
-  Hang up and call your bank using the number on your card or official website.
-  Don't share personal or account information.
-  Don't transfer money or move it to a "safe" account.
-  When in doubt, STOP and VERIFY!

THE SCAM:

- Scammers create a sense of urgency and fear.
- They claim your account is closed or will be closed.
- They ask for your personal or account information.
- They may ask you to move your money.
- Their goal is to steal your money and identity.



WHAT TO DO:



STOP

Don't give any information. Don't act out of fear.



VERIFY

Call your bank using the official number on your card or website. Ask a trusted person.



THEN ACT

Protect your money and information. You're in control.



REPORT SCAMS

Report scams to the FTC:
[ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud)

Your report helps protect others!

STOP • VERIFY • THEN ACT

Stay alert. Stay safe. Protect what matters.

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](https://www.ftc.gov/report-fraud)**

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

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](https://www.ftc.gov/ReportFraud) | FBI: [ic3.gov](https://www.fbi.gov/IC3) | AARP: 1-877-908-3360

“When in doubt — don’t. You always have the right to hang up and check.”



STOP • VERIFY • THEN ACT