12 Scams Seniors Should Know & How to Stay Safe

AmeriFirst Bank | Updated October 2026

Scams can happen to anyone. Criminals use fear, urgency, friendship, or promises of money to pressure people into acting. These are 12 important scam types to recognize, not a ranking. You have the right to stop, ask questions, and talk with someone you trust.

1. Grandparent or family emergency

The approach: Someone claims a relative is injured, arrested, or needs urgent money. A scammer may imitate a familiar voice using AI and demand secrecy.

Protect yourself: Hang up and call your relative or another trusted family member at a known number. Consider a family verification phrase. Do not hand cash to a courier or send money before checking independently.

2. Sweepstakes, lottery, or prize

The approach: You are told you won but must pay taxes, shipping, or a processing fee before receiving the prize.

Protect yourself: Do not pay to collect a prize. Verify the organization independently. Do not share banking information or send gift card numbers to claim unexpected winnings.

3. Home improvement or storm repair

The approach: A door-to-door worker offers leftover materials, a free inspection, or immediate repairs, then pressures you for a large payment.

Protect yourself: Do not allow an unverified visitor into your home. Check licenses where required, insurance, references, and written terms. Compare estimates. Avoid paying the full price upfront; tie payments to agreed work and keep records.

4. Bank or fraud-department impersonation

The approach: A caller or text reports a suspicious charge and asks for a code, remote access, or a transfer to a supposed "safe account."

Protect yourself: End the contact and call your bank at a trusted number. Never disclose sign-in codes or approve an unfamiliar login. Do not move money, buy gold or cryptocurrency, or withdraw cash for collection at an unexpected caller's direction.

More Scams to Recognize

5. Fake shopping, delivery, or refund

The approach: A bargain ad, delivery text, unexpected package QR code, or refund notice leads to a fake site or a request for a small fee.

Protect yourself: Open the retailer's or carrier's official app or type its known address. Research unfamiliar sellers. HTTPS encrypts the connection but does not prove a site is honest. Use a credit card when possible and monitor transactions.

6. Charity or disaster relief

The approach: An urgent appeal uses a familiar-sounding charity name, emotional story, or disaster to pressure you to donate.

Protect yourself: Research the charity independently and donate through its verified website or established channel. Do not rely on caller ID or a link in an unexpected message. Avoid demands for gift cards, cryptocurrency, or wire transfers.

7. Technical support

The approach: A pop-up or unexpected call claims your device is infected and asks you to call a number, install software, or give access.

Protect yourself: Do not call a pop-up's number or allow unexpected remote access. Contact a trusted technician independently. Do not sign in to banking or share your screen while a stranger controls or watches the device.

8. Romance or online friendship

The approach: A person builds trust online, then requests money for travel or emergencies, or offers to teach you investing. Photos, videos, and voices may be fabricated.

Protect yourself: Do not send money or invest at the direction of someone you know only online. Discuss the request with a trusted person. Do not receive and forward money for an online acquaintance.

9. Investment or cryptocurrency

The approach: Someone promises unusually high or guaranteed returns, shows a fake account balance, or demands extra fees or taxes to release withdrawals.

Protect yourself: Check the professional's registration and background through **Investor.gov** or your state securities regulator. Registration alone does not guarantee safety. Do not let an online friend or pressure to act quickly replace independent research.

Know the Warning Signs. Get Help Quickly.

10. Medicare, healthcare, or insurance

The approach: A caller offers a new card, free equipment, or testing and asks for your Medicare number or other personal details.

Protect yourself: Verify through the number on your card or your provider's known number. Medicare calls requesting personal information occur only in limited situations; do not assume an unexpected caller is genuine. Review claims and report services you did not receive.

11. Fake check or overpayment

The approach: Someone sends a check and asks you to return part of the money or buy supplies, gift cards, or cryptocurrency.

Protect yourself: An available balance does not mean the check is genuine. A fake check can take weeks to be discovered. Do not send money back based on a deposited check; contact your bank. You may have to repay funds from a fraudulent check.

12. Government or utility impersonation

The approach: Someone threatens arrest, loss of benefits, or service shutoff unless you pay immediately or share personal information.

Protect yourself: Hang up and use an official number from your bill, card, or existing records. Demands to resolve taxes, fees, or fines with gift card numbers are scams. Do not trust caller ID, badges, or threatening messages as proof of identity.

If you suspect a scam

Call AmeriFirst Bank immediately at 1-800-298-1763 if you sent money, shared banking access, or noticed an unfamiliar transaction. Ask whether a payment can be stopped or recovered; recovery is not guaranteed. Tell a trusted person and keep messages, receipts, and transaction records. There is no need to feel embarrassed or handle it alone.

If you paid with a gift card or payment service, contact that provider promptly too. Use a trusted device to secure exposed accounts. Beware of anyone who demands an upfront fee to recover your lost money - this may be another scam.

Type these addresses into your browser:
ReportFraud.ftc.gov - Report scams | **IC3.gov** - FBI internet-crime reporting
IdentityTheft.gov - Identity theft recovery
amerifirstbank.com - Bank website | **my.amerifirstbank.com** - Online banking

An online report does not notify the bank. If you face immediate danger, call 911.