50+
DECODED

# Scam Shield: 12 red flags + what to say

The scams hitting phones and inboxes most in 2026, and the exact words that end the call. Tape this next to your phone.

**1. Rush + secret + odd payment**
When all three show up together, it's almost always a scam.

**2. Hang up, call back**
Use a number you look up yourself: the back of your card, a bill, the official website.

**3. Nobody real wants these**
Gift cards, crypto, wire transfers, or cash handed to a courier.

### 1 "Grandma, it's me. I'm in trouble."

A grandchild (or a "lawyer" or "officer") needs bail or hospital money now, and begs you not to tell anyone. The voice can sound exactly right: scammers clone voices from short social media clips.

**Say:** "I'll call you right back on your usual number." Then call them, or their parent. Agree on a family code word today.

### 2 Unpaid toll text

"You owe $4.95 in tolls. Pay today to avoid a late fee" with a link. These texts are usually fake and hit people who don't even drive toll roads.

**Do:** Don't tap the link. Check your toll account by typing the official site yourself. Forward the text to **7726** (SPAM), then delete.

### 3 "Your package is on hold" (USPS)

A text or email asks you to "update your address" or pay a small redelivery fee. USPS says it won't text or email you a link unless you signed up for tracking.

**Do:** Type usps.com yourself and use the tracking number from your order. Forward the text to 7726.

### 4 Pop-up: "Your computer is infected"

Loud alarm, frozen screen, "Call Microsoft/Apple support" with a phone number. Real error messages don't include a number to call.

**Do:** Don't call. Close the browser or restart the computer. **Never** let a caller "remote in" to your computer.

### 5 "Pay with gift cards"

A caller tells you to buy Apple, Google Play, Target or other gift cards and read the numbers off the back. Only scammers ask for payment this way.

**Say:** "I don't pay anyone with gift cards." Hang up. If someone is coaching you on the phone at a store, tell the cashier.

### 6 IRS / Social Security / Medicare threat

"Your Social Security number is suspended." "A warrant is out for your arrest." Agencies don't threaten arrest by phone or demand instant payment.

**Say:** "I'll contact the agency myself." Social Security: 1-800-772-1213. The IRS usually contacts you first by mail.

### 7 The online sweetheart

A kind, attentive new friend online who can never video chat or meet, and soon has an emergency, a travel problem, or a "sure" investment.

**Say:** "I don't send money to anyone I haven't met in person." Tell a friend or family member about the relationship.

### 8 A package you didn't order, with a QR code

A note says "scan to see who sent your gift." The code often leads to a fake site that asks for your details or installs something harmful.

**Do:** Don't scan it. You don't have to pay for or return things you never ordered.

### 9 "This is your bank's fraud department"

They say your account is under attack and ask you to read back a code sent by text, or to move money to a "safe account."

**Say:** "I'll call the number on the back of my card." Never share one-time codes. Your bank won't ask you to move money to protect it.

### 10 "A courier will pick up your cash or gold"

A "government agent" or "bank investigator" says your savings are at risk and sends someone to your door to "hold" cash, gold or silver.

**Say:** "No." No real agency or bank sends a courier for your money. If someone shows up, don't open the door; call 911.

### 11 Crypto ATM or "guaranteed" investment

Someone tells you to deposit cash into a Bitcoin ATM, or shows you an app where your "profits" keep growing but you can't withdraw them.

**Say:** "I don't invest through people I met online." Anyone telling you to pay at a crypto ATM is a scammer.

### 12 "You won! Just pay the fees."

A lottery, sweepstakes, or car prize, but first you pay taxes, shipping, or a "processing fee." Often with pressure to act before the deadline.

**Say:** "Real prizes don't cost money to collect." Hang up. Never pay to receive a prize.

50+ DECODED

# If you already paid: act today

Scammers target smart, careful people every day. Speed matters more than embarrassment: the sooner you call, the better the chance to stop the money.

## Step 1 — Call the company you paid through

| How you paid | What to do right now |
| --- | --- |
| **Gift card** | Call the company that issued the card (number on the back or its official website). Tell them it was used in a scam and ask for a refund. Keep the card and the receipt. |
| **Bank transfer, wire, Zelle** | Call your bank using the number on your card or statement. Say "this was fraud" and ask them to stop or reverse the payment. |
| **Credit or debit card** | Call the card issuer, report fraud, and ask to dispute the charge. Ask for a new card number. |
| **Crypto or crypto ATM** | Contact the exchange or ATM company (use the number on the machine or its official website). Ask them to freeze the transaction. Report it fast. |
| **Cash sent by mail** | Call the U.S. Postal Inspection Service: **1-877-876-2455**. If you used FedEx or UPS, call them to try to stop the package. |
| **Gave your SSN or ID** | Go to **IdentityTheft.gov** for a recovery plan. Place a free credit freeze with Equifax, Experian and TransUnion. |
| **Let someone into your computer** | Disconnect from the internet. Have the computer checked by someone you trust. Change your passwords from a different device. |

## Step 2 — Report it (free, official)

**FTC — ReportFraud**
**ReportFraud.ftc.gov**
Federal Trade Commission. Helps track scams and warn others.

**FBI — Internet Crime Complaint Center**
**ic3.gov**
For online, email, crypto and romance scams.

**AARP Fraud Watch Network Helpline**
**877-908-3360**
Free, for members and non-members. Mon–Fri, 8 a.m.–8 p.m. ET.

**National Elder Fraud Hotline (U.S. DOJ)**
**833-FRAUD-11 (833-372-8311)**
Case managers help people 60+ report and recover.

**National Do Not Call Registry**
**DoNotCall.gov · 1-888-382-1222**
Cuts sales calls. Scammers ignore it, so any caller who "must" keep you on the line is a red flag.

**Local police**
**non-emergency number**
A police report helps with banks and disputes. If someone is at your door: 911.

### My trusted numbers (fill in and keep by the phone)

My bank's fraud line: ____________________

Family member to call first: ____________________

Our family code word: ____________________ (never post it online)

**Watch out for "recovery" scams.** After a scam, people often get calls offering to recover the lost money for a fee, sometimes claiming to be from the FTC, the FBI, or one of the hotlines above. Government agencies never charge to help you. Look up the number yourself and call back.

Sources: Federal Trade Commission consumer alerts (consumer.ftc.gov); FBI IC3 (ic3.gov); U.S. Postal Inspection Service (uspis.gov); Social Security Administration (ssa.gov/scam); U.S. Department of Justice, Office for Victims of Crime (ovc.ojp.gov); AARP Fraud Watch Network (aarp.org/fraud). Not legal or financial advice. 