SCAM PROTECTION GUIDE KEEP THIS BY YOUR PHONE

The story changes. The ask doesn't.

Scammers call, text, email, and message with stories like these:

- "This is your bank."
- "This is the police."
- "It's me. I need help."
- "Your computer is hacked."
- "Unpaid toll. Pay now."
- "I love you. Let's invest."

STOP if anyone asks you to:

Send money	Share a code	Let them in
Gift cards, crypto, wire, or cash	Or a password or PIN	Install an app or share your screen

Hang up. Call back.

1. **Hang up. It's always OK.**
   AI can fake any voice, face, or caller ID, even family, your bank, or the police.
2. **Call back on a number you already have.**
   The one on your card or a bill, never theirs. **Use another phone if you can.**
3. **Talk to someone you trust.**
   Before you send anything. Real problems can wait. Scams can't.

No real bank, police, or government agency will ever ask you to:

- Pay with gift cards or crypto
- Hand cash or gold to a courier
- Move money to "protect" it
- Keep it secret from family

Someone coming to your door for money? Call 911.

Not sure? Get free help.
Identity Theft Resource Center, a national nonprofit. Open to everyone.

888-400-5530
Call or text · Mon–Fri, 9 am–8 pm ET

This guide is free. No one will ever call you about it. latchstring.org Turn over ›

SCAM PROTECTION GUIDE SET UP ONCE

Why do scammers know so much about me?
Your name, address, bank, and family's names leak in data breaches and are sold by data brokers. **Knowing your details proves nothing.**

Set these up once.

Do one a week. Ask for help if you need it.

- [ ] **Lock your phone number.**
  In your carrier's app or by phone, ask for a number lock. Free at AT&T, Verizon, and T-Mobile.
- [ ] **Choose a family safe word.**
  Agree on it in person. On a worrying call, ask for it.
- [ ] **Freeze your credit. It's free.**
  Your cards still work. At **equifax.com**, **experian.com**, and **transunion.com**.
- [ ] **Get an IRS identity PIN.**
  It stops fake tax returns in your name. Free at **IRS.gov/ippin**.
- [ ] **Turn on automatic updates.**
  In Settings on your phone and your computer.
- [ ] **Screen unknown callers.**
  iPhone: Settings › Apps › Phone › Screen Unknown Callers. Android: Phone app › ⋮ › Settings.
- [ ] **Turn on bank alerts.**
  Call the number on your card. Ask for payment alerts and lower limits.
- [ ] **Protect your email.**
  In your email's security settings, turn on two-step sign-in.
- [ ] **Claim Social Security online.**
  At **ssa.gov/myaccount**, before a scammer does.
- [ ] **Hide your details from search.**
  Free. Go to **goo.gle/resultsaboutyou** on any phone or computer.

Everyday habits

- **Don't tap links** in texts or emails. Open the app instead.
- **Get support numbers** from your bill or card, not from search ads.
- **Never send money** to someone you haven't met in person.
- **Share less online.** Hide your birthday and address.

If a scam has already happened

Act fast. It's not your fault.

1. **Call your bank** or the company you paid, on a number you already have.
2. **Let someone in?** Turn off the computer.
3. **Report it:** ReportFraud.ftc.gov and IC3.gov
4. **Free recovery plan:** call or text **888-400-5530**.
5. **Never pay to get money back.** That's a second scam.

Free to copy and share. Tap any **blue text** for step-by-step help. October 2026