

How to Shut Down a Scammer

These are professional criminals. They do this all day, every day, and they are good at it. It is their job. Getting the call is not your fault, and knowing what to do next is what stops them.

Four rules. That is the whole thing.

1 HANG UP. IT IS NOT RUDE.

You never have to stay on a telephone call. There is no such thing as a call you are required to finish. You do not owe a stranger an explanation, a goodbye, or a reason. Hang up in the middle of your *own* sentence — it works even better.

2 CALL BACK ON A NUMBER YOU LOOKED UP.

If it is really your bank, your grandson, or Medicare, they will still be there in ten minutes. Hang up first. Then find the number yourself — on your bank card, on a statement, in your own address book. **Never the number they gave you.**

3 NOBODY REAL WANTS GIFT CARDS.

No bank, no police officer, no government office, and no utility company has ever asked to be paid in gift cards, wire transfers, cryptocurrency, or cash in an envelope. Not once, not ever. If that is the ask, it is a scam — **every single time, no exceptions.**

4 TELL SOMEBODY BEFORE YOU PAY, NOT AFTER.

Say it out loud to one person you trust — a neighbor, your daughter, a friend. Scammers work hard to keep you alone on the phone, because alone is the only way this works. Saying it out loud to another human being is the single thing that breaks the spell.

**If you remember nothing else:
Hang up. Look up the number. Call back.**

What They Actually Say

These are the real opening lines. If you hear one of them, you already know what it is — and you already know what to do.

“Grandma? I'm in trouble. Please don't tell Mom.”

They can now copy a real voice from a few seconds of video. It can sound exactly like your grandchild. **Hang up and call your grandchild on the number you already have.**

“This is Microsoft. Your computer is infected — let me connect to it.”

Microsoft and Apple do not telephone people about their computers. **Never let anyone connect to your computer because they called you.**

“This is Social Security. Your number has been suspended.”

Social Security numbers are never suspended. That sentence does not exist in real life. It is only ever spoken by a criminal.

“This is your bank's fraud department. We need to move your money to a safe account.”

There is no such thing as a “safe account.” Your bank will never move your money for you, and will never ask you to move it yourself.

Caller ID lies

A scammer can make any name and any number appear on your screen — a local 520 number, your own bank's real number, even the word POLICE. **What you see on the screen proves nothing at all.** This is exactly why Rule 2 says call back on a number *you* looked up, not the one that called you.

A caller who knows your name, your address, or part of your account number has proven nothing either. That information is stolen in data breaches and sold by the thousands.

What They Actually Say, Continued

“This is TEP. Your power will be shut off in thirty minutes unless you pay now.”

Tucson Electric Power says plainly that it never demands immediate payment and never asks anyone to pay with a pre-paid money card. Real delinquent accounts get several written notices, well in advance — never one warning an hour before. **TEP's real number is 520-623-7711, the one printed on your bill.**

“I'm with the Sheriff's Department. There's a warrant — you missed jury duty.”

No law enforcement agency takes payment over the telephone to clear a warrant, and none will ever threaten you with arrest to collect money. That call is always a fake.

“You've won! Just pay the taxes and fees to release your prize.”

You never pay money to receive money. A prize that costs you something is not a prize.

“I can get back the money you lost — for a small fee.”

This one is aimed at people who were already taken once. It is usually the same criminals, coming back for the rest. If you were taken before, **expect this second call** — and hang up on it too.

“We've been talking for months. I just need help with one emergency.”

If someone you know only from the telephone, the computer, or a dating site ever asks for money, **that is the scam** — no matter how long you have been talking, and no matter how kind they have been. Kindness over months is the investment they make.

Five sentences that mean STOP

- X** “Don't tell anyone about this.”
- X** “Stay on the line while you go to the store.”
- X** “You have to act right now.”
- X** “Pay with a gift card.” (or wire, or cryptocurrency, or cash to a courier)
- X** “Let me connect to your computer.”

Any one of these, by itself, is your answer. A real bank, a real officer, and a real family member will never say a single one of them.

What to Say to Get Off the Phone

You do not owe them a conversation. Pick one of these, say it, and hang up without waiting for the answer.

“I don't do business over the phone. Goodbye.”

“I'm going to hang up and call back on the number on my statement.”

“I never make decisions on a call I didn't make. Goodbye.”

— or say nothing at all, and hang up.

Never do these on a call you did not place

- X** Give your Social Security number, Medicare number, or any bank or card number.
- X** **Read back a code that was just texted to you.** That code is the key to your account. Nobody legitimate will ever ask you for it.
- X** Let anyone connect to or “fix” your computer.
- X** Buy a gift card, send a wire, or feed cash into a cryptocurrency machine.

At your door

- > You never have to open the door. Talk through it, or don't answer at all.
- > Real utility and city workers carry identification and **will wait** while you telephone their office to check. A real one never minds. A fake one gets angry.
- > Never let a stranger inside to “inspect” a roof, a pipe, or a meter, and never pay a contractor in cash up front.
- > If someone will not leave, call the police non-emergency line — or 911 if you feel unsafe.

On Your Computer and Your Phone

- > Never click a link in an email or a text — **and do not type in the address it shows you either**. A fake address can be one letter off from the real one. Go to the company the way you always do: your own bookmark, or the telephone number on your statement or the back of your card.
- > A pop-up that fills the screen with sirens and a telephone number is **always** fake. Do not call it. Close the browser, or shut the machine off and back on.
- > Do not scan a QR code from a flyer, a letter, a parking sign, or an unexpected package.
- > A text about a package you were not expecting is bait. Delete it.
- > If your phone asks you to **approve a sign-in you did not start**, tap Deny. Then change that password, because someone else has it.
- > A text saying you owe a court, a toll or a fine is bait. **Courts do not take payment by text, QR code, Zelle or Venmo**, and a real ticket comes in the mail.

Coming in October: the Medicare flood

Medicare Open Enrollment runs **October 15 through December 7**. Every year the calls, texts and mailers multiply, and the criminals hide in the crowd.

- X** Real Medicare **does not telephone you out of the blue** to ask for your Medicare number or a payment.
- X** There is no “new gold Medicare card,” and no new card you have to pay for.
- X** Free braces, free knee supports, and free DNA or genetic test kits offered by telephone are fraud — billed to your Medicare number.
- X** Nobody needs your Medicare number for you to **compare** plans. You only give it when you enroll.

Questions about a plan? Call **1-800-MEDICARE** yourself, or Arizona's Senior Medicare Patrol at **1-800-432-4040**.

Set These Up This Week

Ten minutes now, before anyone calls. Each one stops a scam that the four rules alone might not.

1. A family code word. One word only your people know — not a pet, not a birthday, nothing that is on Facebook. Anyone who telephones claiming to be family in trouble has to say it. It costs nothing and it defeats every voice recording on earth. *There is a card for this on the last page.*

2. A trusted contact at your bank. Ask your bank, credit union, or broker to add a “trusted contact” to your account — someone they are allowed to telephone if they think something is wrong. Brokerages are required to ask you for one, and many banks will add one too. That person **cannot touch or move your money**; they are only somebody to call.

3. Two-step sign-in on your email and your bank. After your password, the site sends a code to your phone. Turn it on in the account's security settings, or ask a family member to help. A stolen password alone will not get them in. That code is for you to type in, never to read to anyone who calls.

4. Think about freezing your credit now. You do not have to wait for a breach. It is free, it does not hurt your score, and you lift it when you apply for credit. The numbers are on the next page.

If Your Information Was in a Data Breach

A company or an agency says it lost your information. Do this the same week.

Freeze your credit. It is free.

A freeze stops anyone from opening a new loan or credit card in your name. It costs nothing, it does not hurt your credit score, and you can lift it any time you apply for credit yourself. **Call all three.** Have your Social Security number, birth date and address ready.

Equifax

or [equifax.com](https://www.equifax.com)

1-888-298-0045

Experian

or [experian.com](https://www.experian.com)

1-888-397-3742

TransUnion

or [transunion.com](https://www.transunion.com)

1-888-909-8872

- > **Read the notice, but do not tap the link in it.** Type the company's address in yourself, or call the number on your statement. Scammers send fake breach notices too.
- > **Expect calls that use your real details.** A caller who knows your account number or case number is still a stranger. Hang up and call back on a number you looked up.
- > Someone opened an account or filed taxes in your name? Report it at **IdentityTheft.gov** for a step-by-step recovery plan.

The Arizona courts breach, September 2026

Arizona's court system says criminals copied records on about **1.3 million people** whose court debt went to collections, including names, case numbers and Social Security numbers. If you ever had court debt go to collections, freeze your credit.

Check whether you are on the list at **azcourts.gov/cybersecurityalert**. Type it in yourself. The court's help desk is **602-452-3519** or **800-720-7743**, weekdays 7 a.m. to 6 p.m. The court does send real texts, from the number **83958**, but go to the website yourself instead of tapping a link.

If It Already Happened

Tell someone today. Not tomorrow. Speed is the one thing that gets money back, and it works more often than people think. You will not be in trouble, and nobody is going to think less of you. These are professional criminals who rehearse this for a living — being fooled by them is not a character flaw. Staying quiet is the only thing that helps them.

Do these things, in this order

- 1** Call your bank or credit card company and **ask for the fraud department.** Say the word “fraud” and they will move quickly. If you paid by card, ask them to reverse the charge.
- 2** Tell one family member or a friend you trust.
- 3** **If you bought gift cards, keep the cards and the receipts** and telephone the company printed on the card right away. Money is sometimes still on them, and sometimes it can be frozen. Do not throw them away, even if you already read the numbers out loud.
- 4** **If you put money into a Bitcoin or crypto machine,** keep the receipt and contact both the machine's company and the Arizona Attorney General **within 30 days.** Arizona law can require a full refund if you were new to that machine's company.
- 5** If you gave out your Social Security number, freeze your credit. The numbers are on page 7.
- 6** Report it, using the numbers on page 9, so they can go after the people who did it.

Expect a second call

Once you have been taken, your name goes on a list that gets sold. Within weeks somebody will telephone offering to *recover* the money — for a fee, or for your bank details. That call is the same crime wearing a different hat. **Nobody legitimate ever charges a fee to give you back your own money.**

Who to Call

Tear this page out.

Emergency — you are in danger right now

911

Tucson Police — non-emergency

To report a scam or a suspicious visitor

520-791-4444

Pima County Sheriff

If you live outside Tucson city limits

520-351-4900

Adult Protective Services — Arizona

Weekdays 7 a.m.–7 p.m., weekends 10–6; online any time at des.az.gov/aps

1-877-767-2385

Arizona Attorney General — Consumer Protection

Tucson office; complaints online at azag.gov/complaints/consumer

520-628-6504

Pima Council on Aging — Helpline

Weekdays, 8:30 a.m. to 5 p.m.

520-790-7262

Medicare

1-800-MEDICARE — plans, billing, impostors

1-800-633-4227

Arizona Senior Medicare Patrol

Free help with Medicare fraud

1-800-432-4040

Tucson Electric Power

The real TEP number, also on your bill

520-623-7711

Federal Trade Commission

Online at ReportFraud.ftc.gov; identity theft at IdentityTheft.gov

1-877-382-4357

Social Security fraud hotline

Weekdays 10 a.m.–4 p.m. Eastern: 7 a.m.–1 p.m. Arizona time, 8–2 from November 1

1-800-269-0271

Cut These Out and Keep Them

Tape the first one next to the telephone, where you can see it while you are standing there. Fill in the second one this week.

----- CUT ALONG THIS LINE -----

BEFORE I GIVE ANYONE MONEY OR NUMBERS

- 1** Hang up. It is not rude.
- 2** Look the number up myself — never theirs.
- 3** Tell one person I trust, out loud, first.

Nobody real ever wants gift cards.

“Don't tell anyone” means it is a scam.

Tucson Police, non-emergency: 520-791-4444

Pima County Sheriff: 520-351-4900

----- CUT ALONG THIS LINE -----

OUR FAMILY CODE WORD

It is:

Anyone who telephones saying they are family in trouble **must be able to say this word.** If they cannot say it, it is not them — no matter how much the voice sounds right.

Choose a word that is not a pet, a birthday, a street, or anything a stranger could read online. Then telephone your family today and tell them what it is.

I told:
