

The 60-Second Call Defense

- **Pause** (do not answer questions)
- **Identify red flags** (below).
- **End politely** with a script.
- **Verify on a known number** (card/statement/site you type).
- **Log it** (who/when/what they asked).

Top Red Flags (Banks / Government / Medicare)

Caller ID is meaningless (this is easily manipulated).

Don't become a victim from the following scam tactics:

- **Stay on the line**
- **Don't tell anyone**
- **Act now."**
- **Requests for verification codes, passwords, remote access, gift cards, wire/Zelle to a "safe account."**
- **Threats: account locked, audit/arrest, benefits suspended.**
- **Golden Rule: No codes. Known numbers only.**

Exact Scripts:

Bank/Government/Medicare claim: "I don't handle account issues on incoming calls. I'll call back using the number on my card/official site. Goodbye."

Code request: "I never share verification codes. This call is over."

They insist you stay on the line: "I don't keep money matters secret. I'm ending the call and verifying."

Pressure or threats: "I don't act under time pressure. I'll verify through official channels."

Spoofed-Call Reality Check

- **Real institutions won't:** Ask for your code, Rush a same-call transfer, Tell you to move money to a "safe account," or forbid you from calling back.
- **Real institutions will:** Let you call back on a published number, Send secure messages inside your account, and advise you not to share codes.

Mini Scenarios (circle the move)

1. “Fraud alert: a \$9,800 wire. Read me the code we just texted to stop it.”

YOU: End call → **Call the number on your card. Never share codes.**

1. “This is the IRS. Pay today or a sheriff will arrest you.”

YOU: End call → **Contact IRS via irs.gov only. Threat = scam.**

1. “Medicare needs to re-issue your card; confirm your SSN and bank.”

YOU: End call → **Call 1-800-MEDICARE from your phone favorites.**

Do's / Don'ts

Do

- Save **Bank Fraud, Card Fraud, 1-800-MEDICARE, Safety Buddy** to Favorites.
- Keep one **hang-up script** taped by the phone.
- Log scam calls (time/claimed org/ask).

Don't

- Don't stay on the line under pressure.
- Don't call back numbers provided by the caller.
- Don't share codes, passwords, or install remote software.
- One Printable (this lesson)

“Phone Scam Hang-Up Scripts + Verification Steps”

- Box 1: 3 scripts above
- Box 2: “Verify on a Known Number” (card/statement/site you type)
- Box 3: Favorites checklist (Bank Fraud, Card Fraud, 1-800-MEDICARE, Buddy)

Quick Check (3 questions)

1. The caller says they're your bank and needs the **texted code**. Best response?

Answer: Hang up; call the number on your card. Never share codes.

1. Caller ID shows **Medicare** and they want your SSN to “keep benefits active.” Red flag?

Answer: Yes. End call; dial **1-800-MEDICARE** yourself.

1. The “IRS” threatens arrest unless you pay **today**. Next step?

Answer: End call; go to **irs.gov** for official contact. Arrest threats = scam.

This Week's 5-Minute Action

- Practice the **hang-up script** aloud twice.
- Add/confirm Favorites: **Bank Fraud, Card Fraud, 1-800-MEDICARE, Safety Buddy**.
- Place the printable near your phone.