📞 Phone Scams (Vishing)

Scammers spoof caller ID to pose as banks, agencies, or companies.

They create urgency, ask for codes, payments, or remote access.

🔗 Trusted Resources

FCC — Caller ID Spoofing — How spoofing works and what you can do. 🌐 https://www.fcc.gov/spoofing ↗

FTC — How to Recognize Imposter Scams — Government, business, and family emergency impostors.

🌐 https://consumer.ftc.gov/articles/how-avoid-scam ↗

Social Security (SSA) — Scam Alerts — Official contact rules and reporting. 🌐 https://www.ssa.gov/scam/ ↗

IRS — Tax Scams / Consumer Alerts — How IRS really contacts you (and how they don’t).

🌐 https://www.irs.gov/newsroom/tax-scams-consumer-alerts ↗

📞 Phone Scams (Vishing)

🧭 Recognizing & Responding Safely

Hang up. Call back using the number on your statement or official website.

Never relay verification codes. Banks and agencies won't ask for one-time codes.

Ignore caller ID. Spoofed names/numbers are common; rely on independent verification.

Report robocalls/spoofing to the FCC and add your number to the Do Not Call Registry.

📌 Sam's Tips

The more urgent the call, the more likely it's a scam.

Codes and passwords are never spoken over the phone.

Ending the call is your superpower. You can always verify later.