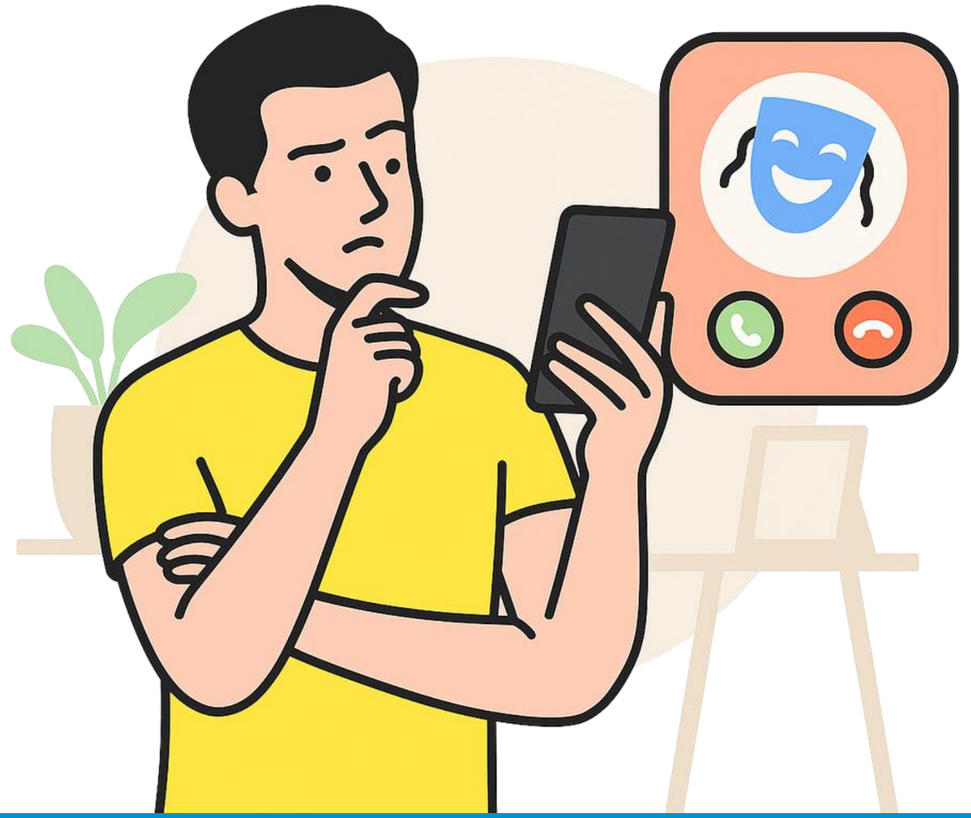
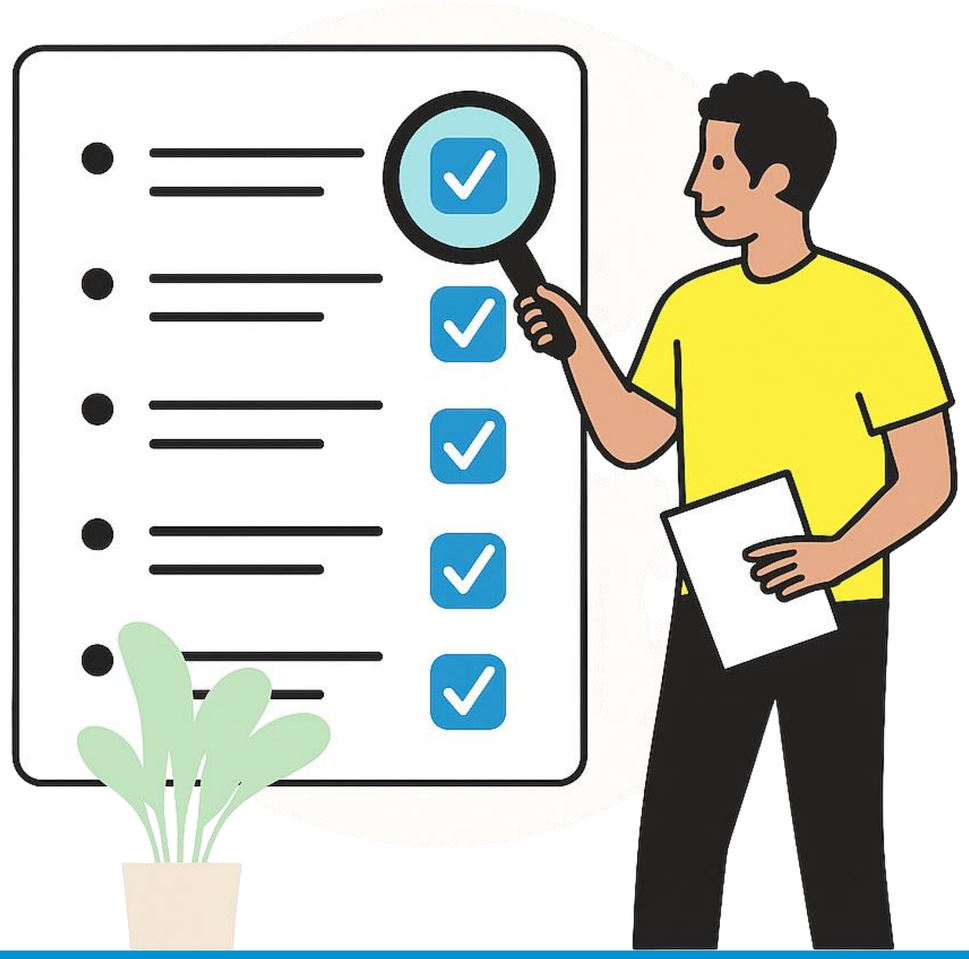
Spot the Spoof

Protecting Yourself from Phone Scams



Today's Agenda

- How Caller ID Spoofing Works
- Common Scams and Warning Signs
- Blocking and Reporting Calls
- What To Do If You're Targeted
- Q&A and Resources



The Scale of the Scam Call Problem

The average person receives **9 spam calls every month**

Americans receive **3.3 billion spam calls monthly**

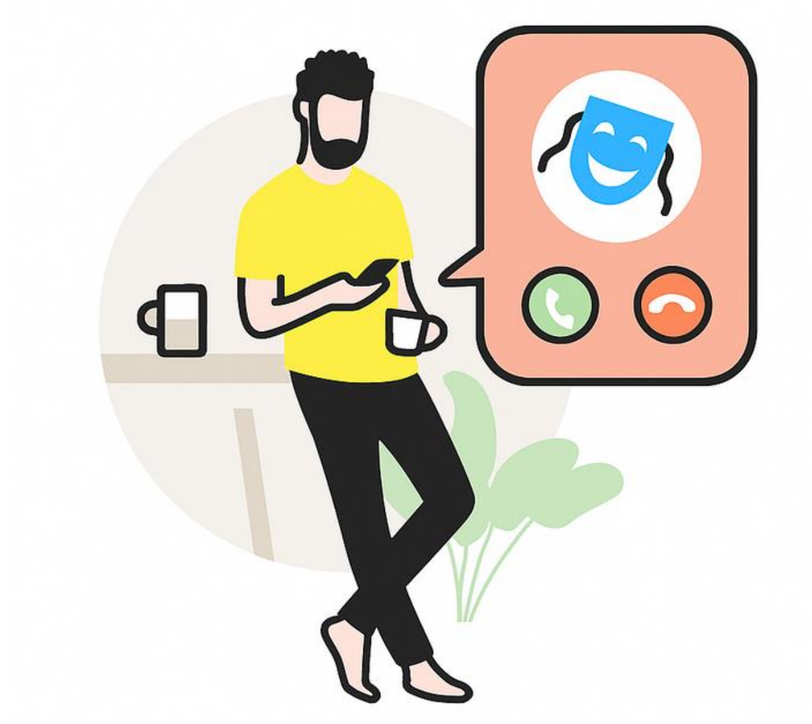
Americans wasted **260 million hours on spam calls** last year

Spoofing is the #1 tactic used by phone scammers

www.truecaller.com

UNITED STATES SENATE FEDERAL CREDIT UNION®

What is Caller ID Spoofing?



Caller ID spoofing is when someone intentionally **alters their caller ID information to hide their identity** or impersonate somebody else.

How Caller ID Spoofing Works

Spoofing Services

Online tools that let scammers choose the number displayed

VoIP Spoofing

Internet-based calling systems that allow caller ID editing

Orange Boxing

Hardware tricks to manipulate phone network signals

Common Caller ID Spoofing Tactics

- **Local Numbers:** Uses your area code to appear familiar
- **Familiar Contacts:** Mimics friends, family, or trusted companies
- **Neighbor Spoofing:** Matches your area code and prefix
- **Deepfake Voice:** Uses AI to mimic a known person’s voice

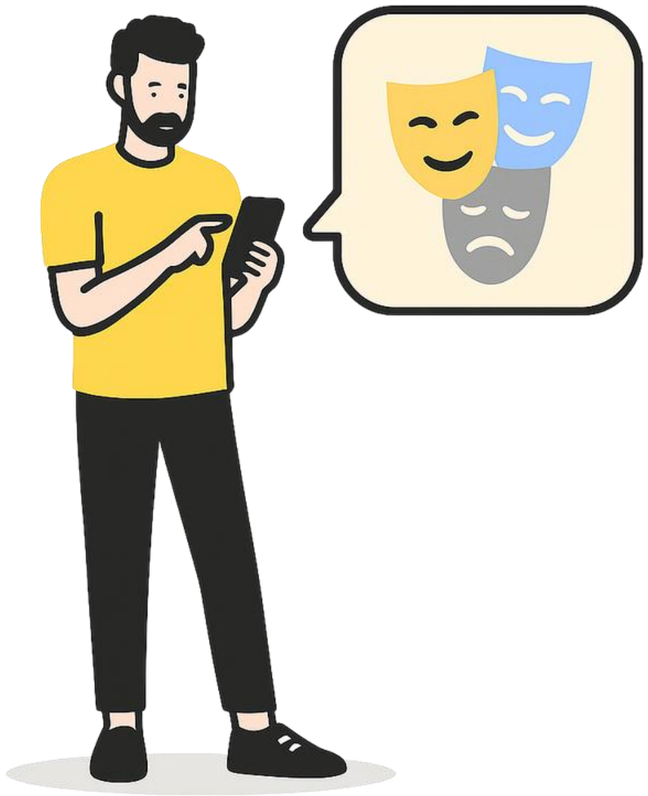
UNITED STATES SENATE FEDERAL CREDIT UNION®

What Is Vishing?

Vishing, short for voice phishing, refers to **fraudulent phone calls or voice messages** designed to trick victims into providing sensitive information.

How Scammers Get Your Number

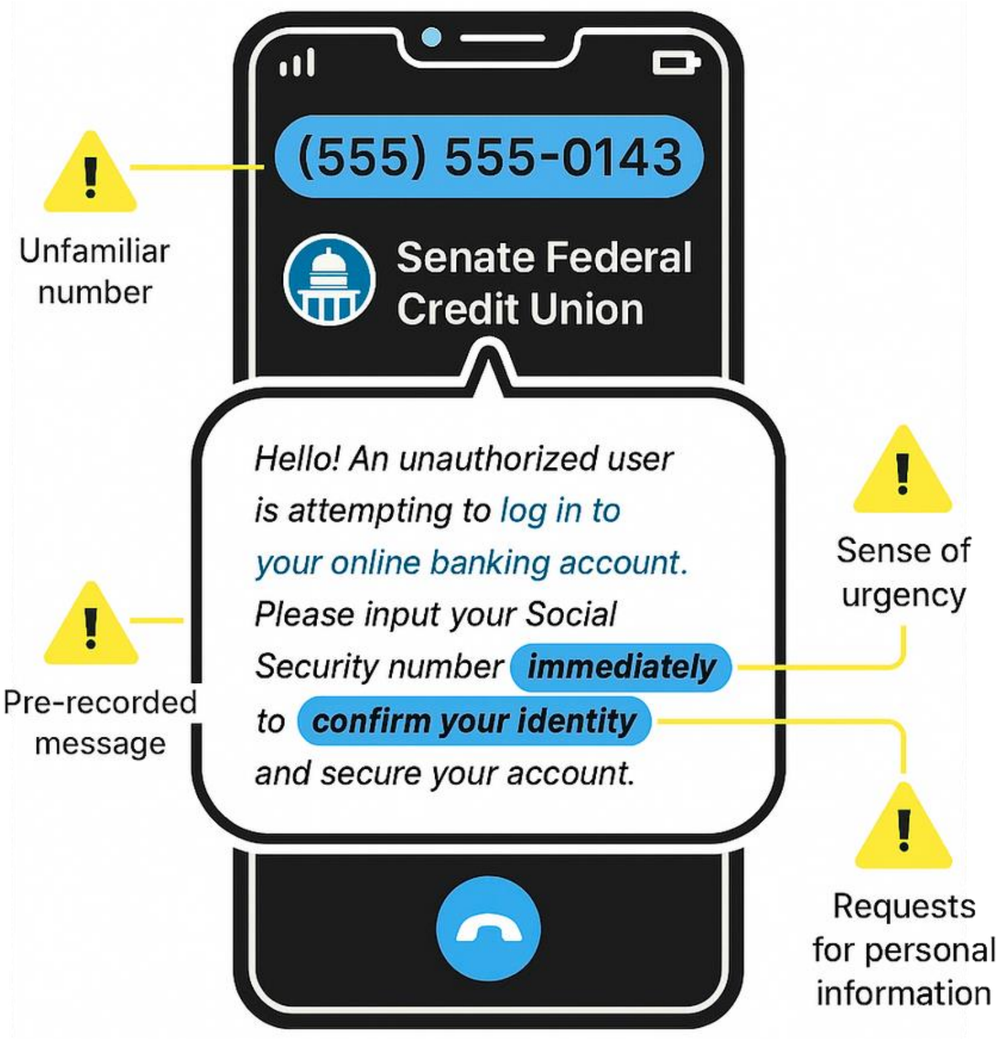
- **Data breaches** and leaks
- Purchased from **data brokers**
- Public **social media** profiles
- **Lead generators** disguised as sweepstakes or surveys
- **You answered** a scam call before



UNITED STATES SENATE FEDERAL CREDIT UNION®

How to Spot
Caller ID Spoofing

- Unfamiliar number
- Pre-recorded message
- Sense of urgency
- Requests for payment or pii
- Display differs from stored contact



Caller ID Spoofing Protection Tips

- Avoid answering unknown numbers
- Don’t hit any buttons
- Stay silent
- Keep your information private
- Enable spam-blocking features
- Secure your voicemail inbox
- Redial the number yourself
- Block suspicious callers

UNITED STATES SENATE FEDERAL CREDIT UNION®

Common Caller ID Spoofing Scams

Government Impersonators
IRS, SSA, Law Enforcement

Bank/Credit Union Impersonation
Fraud or “suspicious activity” calls

Family Emergencies
AI voices mimicking loved ones

Employer Spoofing
Fake calls from boss/HR, sometimes using Microsoft Teams

Tech Support Fraud
Fake tech reps claiming device issues

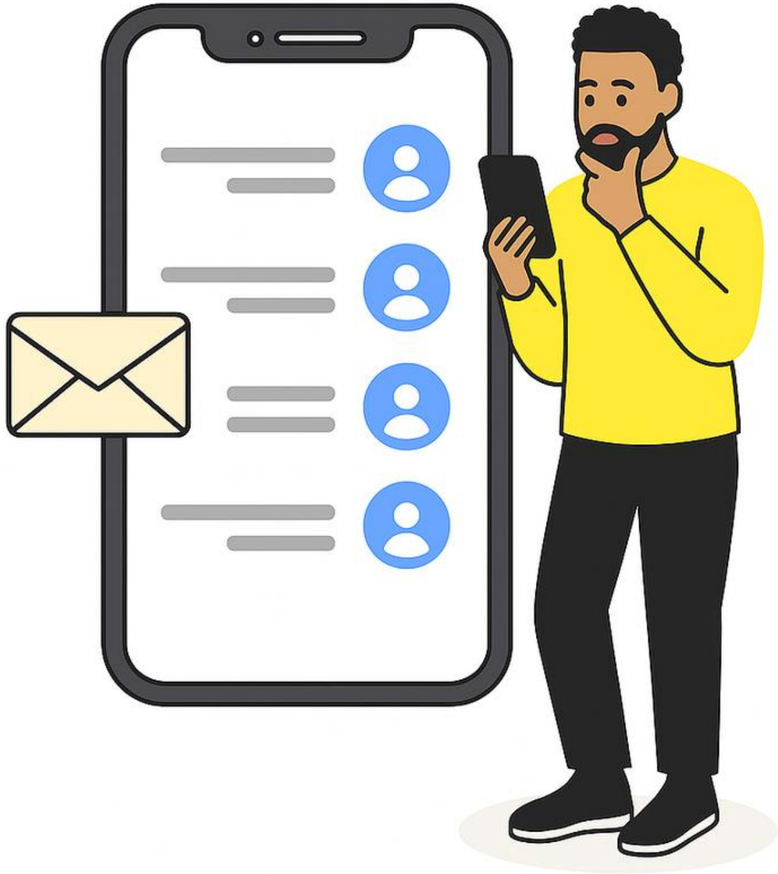
Utility Company Scams
Threats of shutoff unless paid

Delivery Scams
Fake UPS, FedEx, USPS notices

Health Insurance Scams
Impersonators claim issues with your Medicare/insurance.

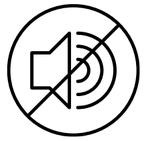
Reduce Your Digital Exposure

- **Clean up social media:** Remove your phone number and review privacy settings
- **Opt out of data broker sites:** Manually request removal from data collection websites
- **Remove from Google Search:** Submit takedown requests for personal info appearing in results
- **donotcall.gov:** Register your number and reduce marketing calls



Use Your Phone & Provider Tools

Built-In Phone Features



Silence Unknown Callers (*iPhone*): Automatically send unknown numbers to voicemail

Block Numbers: Stop repeat offenders from reaching you again

Enable Spam Protection (*Android*): Flag suspicious calls automatically

Customize Do Not Disturb: Let only known contacts ring through

Carrier Tools

AT&T ActiveArmor: Blocks fraud calls, sends spam alerts, manage block list

T-Mobile Scam Shield: Scam ID, caller ID, blocking, and even proxy numbers

Verizon Call Filter: Identifies spam, lets you report scammers

US Cellular Call Guardian: Alerts, spam blocking, premium caller ID features

Location Can Attract Spam Calls

Spoofed calls often match your current area code — travel can increase “local” spam

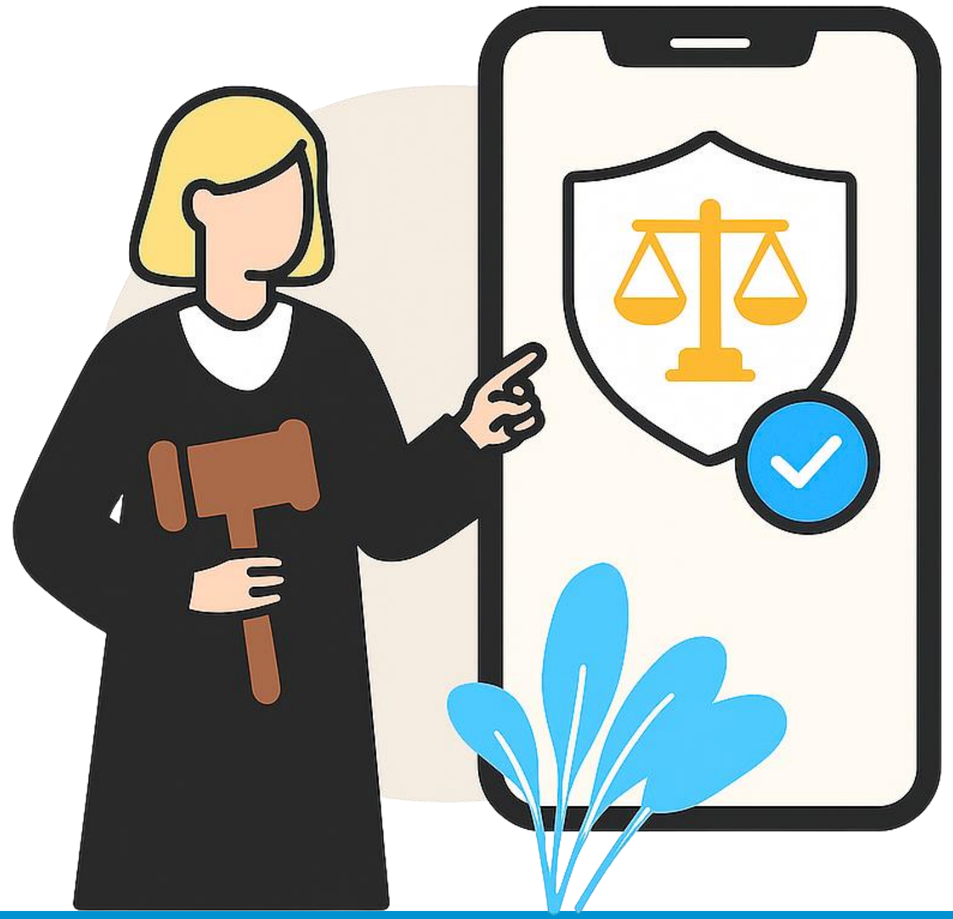
Travel apps and maps may share your location with data brokers

Roaming settings can expose you to more ad networks

Holiday travel = rise in fake booking, airline & hotel scams

Quick Tips:

- Limit app location access
- Silence unknown callers
- Don’t answer unfamiliar numbers
- Watch for travel-themed scams



Truth in Caller ID Act of 2009

Spoofing to Scam is Illegal—
Here's What the Law Says

- **Illegal to spoof** to defraud
- **FCC + states** can prosecute
- **Law enforcement use** permitted
- **Business exceptions** allowed

Report Suspicious Calls

- **Forward to 7726 (SPAM):** Report scam texts to your carrier
- **ReportFraud.ftc.gov:** Submit scams to the FTC
- **FCC.gov/complaints:** File a report with the FCC
- **Report to law enforcement** if money was lost or a crime occurred

Think It’s Us?
Trust & Verify

- USSFCU will **never** pressure for sensitive info
- Hang up and call **800.374.2758**
- Send a message securely through **myUSSFCU** Online or Mobile Banking

UNITED STATES SENATE FEDERAL CREDIT UNION®

Protect Yourself,
Stay Alert

- **Trust your gut** — if something feels off, pause
- **Block and silence** unknown or suspicious calls
- Use official channels to **verify any requests**
- **Remove your info** from public directories
- **Share what you've learned** with others

Helpful Tools & Resources

- **fcc.gov/spoofing** – Understand spoofed calls & report issues
- **consumer.ftc.gov** – Scam alerts & educational articles
- **identitytheft.gov** – Help if your info is stolen
- **optoutprescreen.com** – Stop pre-approved credit offers
- **DMAchoice.org** – Reduce junk mail and marketing outreach
- **privacyrights.org** – Remove personal info from data broker sites

THANK YOU!

Q & A