Call Spoofing: What It Is and How to Protect Yourself

What Is Call Spoofing?

Call spoofing occurs when a caller deliberately falsifies the information transmitted to your caller ID to disguise their identity. Scammers often use tactics such as:

- **Neighbor spoofing**, making the call appear as if it’s coming from a local number. [fcc.gov]
- **Impersonating trusted organizations**, such as government agencies or banks, to trick recipients into sharing sensitive information. [fcc.gov]

Spoofing is frequently used to facilitate fraud, theft of personal information, or other harmful activities.

Why Scammers Use Spoofing

Scammers spoof caller IDs to:

- Make you more likely to answer the call.
- Create a false sense of trust or urgency.
- Trick you into providing sensitive data, money, or account access.
  (Intent to defraud using spoofed caller ID is illegal under the Truth in Caller ID Act.) [legalclarity.org]

How to Protect Yourself From Spoofed Calls

The FCC and other federal agencies recommend the following steps:

1. Don’t Answer Unknown Numbers

If you don’t recognize the number, let it go to voicemail. Many spoofed calls rely on catching you off guard. [fcc.gov]

2. Hang Up Immediately If Something Seems Suspicious

If a caller pressures you or asks for personal information, hang up — even if the caller ID looks legitimate. [fcc.gov]

3. Never Share Sensitive Information

Do *not* respond to unexpected requests for:

- Social Security numbers
- Account numbers
- Passwords or PINs
- Other identifying details [fcc.gov]

4. Don’t Press Buttons or Respond to Prompts

Scammers sometimes use prompts (“Press 1 to stop receiving calls”) to identify active numbers. Hang up instead. [fcc.gov]

5. Verify Caller Identity

If the caller claims to be from your bank, doctor’s office, or a government agency:

- Hang up, then
- Call the official number from their website, statement, or the back of your card [fcc.gov]

6. Use Call-Blocking Tools

Mobile apps and carrier tools can help filter and reduce unwanted calls. Your phone provider may also offer enhanced blocking features. [fcc.gov]

7. Set a Voicemail Password

Some scammers spoof your own number to access your voicemail if it has no password. Setting a PIN stops this. [fcc.gov]

How to Report Call Spoofing

Report to the FCC (Federal Communications Commission)

The FCC handles complaints involving:

- Caller ID spoofing
- Robocalls
- Spam texts [reporttele…rketer.com]

File an official FCC complaint here: https://www.fcc.gov/complaints [reporttele…rketer.com]

You should report:

- The spoofed number
- Time and date of the call
- Description of the scam attempt

Additional Reporting for Scams

If the spoofed call involved fraud or a scam attempt, also report it to the **FTC (Federal Trade Commission)**:

> **https://reportfraud.ftc.gov** [reporttele…rketer.com]

When Spoofing Is Not Illegal

Not all spoofing is malicious. Sometimes it’s used legitimately, such as when:

- A doctor calls from a personal phone but displays the office number.
- Businesses use one main outbound number for consistency. [legalclarity.org]

The key legal factor is **intent** — spoofing becomes illegal when used to defraud, cause harm, or obtain something of value. [legalclarity.org]

Summary

Call spoofing is a growing and sophisticated tactic used by scammers. Understanding how it works and being cautious with unexpected calls can help protect your personal information. When in doubt, **hang up and verify**. And if you believe you received an illegal spoofed call, **report it immediately** using the links above.