MAHARASHTRA CYBER

2025

Caller ID Spoofing Threats

ADVISORY REPORT

CCCMH_CA_2025_06

Table of Contents

EXECUTIVE SUMMARY

Caller ID Spoofing is a deceptive practice where the caller intentionally falsifies the information transmitted to your caller ID display to disguise their identity.

With the growing frequency of telecommunication frauds, spoofing is now a tool used for social engineering, scams, data theft, and harassment.

This advisory aims to inform the public, businesses, and institutions about:

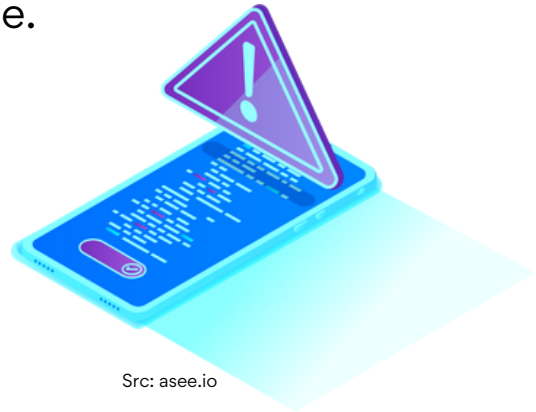
- What Caller ID Spoofing is
- How spoofing is conducted
- Legal implications
- Real-world impact
- Best practices to detect and respond
- Preventive measures
- Reporting mechanisms

INTRODUCTION

Src: freepic

What is Caller ID Spoofing?

It's a technique used to manipulate caller ID info to display a fake or misleading number. This misleads the call receiver into believing the call is from a trusted source.



Src: asee.io

Why it Matters:

- Rise in fraud cases
- Erosion of trust in communication
- Economic and psychological impact on victims

How Caller ID Spoofing Works

Spoofing is typically carried out using Voice over IP (VoIP) services, third-party applications, or private exchanges (PBX) that allow customization of caller IDs.

Key Techniques Used

- VoIP systems: Allow modification of outgoing caller ID data.
- Spoofing apps/websites: Like SpoofCard, PrankDial, and SIM spoofing tools.
- PBX configurations: Used to reroute calls with altered caller information.
- Telecom exploits: Sometimes used to bypass network protections.

Typical Spoofing Process

1. Setup: Attacker uses a spoofing platform or VoIP service.
2. ID Input: They choose the number to display.
3. Call Made: The call is placed using this spoofed ID.
4. Deception: The recipient sees a trusted number and may respond.

Types of Spoofing & Their Motives

Types of Spoofing:

- Neighbor Spoofing: Mimics local numbers to increase pick-up rate
- Government/Authority Spoofing: Pretends to be from police, IRS, etc.
- Bank/Service Provider Spoofing: Attempts to steal credentials
- Personal Spoofing: Used for harassment or manipulation

Motives:

- Identity theft
- Financial fraud
- Pranks or harassment
- Bypassing call blocking systems

Real-World Impact

Case Study 1: A senior citizen received a spoofed call claiming to be from a government department demanding immediate tax payment. The victim transferred ₹50,000 before realizing the fraud.

Case Study 2: An IT company received spoofed calls from what appeared to be a client, leading to the disclosure of internal credentials used in a later cyberattack.

Impacts:

- Financial loss through phishing
- Psychological stress and fear
- Reputational damage
- Business credibility loss
- Telecom service disruptions due to call volume

- **Example:** Victim tricked into revealing OTP to spoofed bank caller — led to ₹1.2 lakhs theft.

Legal Aspects in India

Spoofing with malicious intent is illegal under the Indian Telegraph Act and IT Act, 2000, with penalties under Section 66D for cheating by personation.

IPC Sections 419 and 420 also address fraud. TRAI mandates call tracing and caller ID regulations, while DoT focuses on identity verification and AI-driven fraud detection

Globally, laws like the U.S. Truth in Caller ID Act prohibit deceptive spoofing. Some countries are enhancing regulations by integrating advanced verification techniques. Increased collaboration between telecom providers and regulatory bodies aims to curb fraudulent activities more effectively

Identify a Spoofed Call

Watch for these signs:

- Caller ID matches your own number or an oddly formatted number.
- Caller pressures you for urgent action or payment.

You receive multiple calls from “your” number.

Caller refuses to provide a callback number or credentials.

Red Flag:

- Caller asks for OTPs or passwords
- Pressure tactics or threats
- Claims of account suspension or legal trouble
- Call appears to be from your own number

Verification Steps:

- Hang up and call the organization back using a verified number.
- Ask specific, verifiable questions.
- Don’t share OTPs, banking info, or credentials over a call.

Preventive Measures

For Individuals:

- Enable call blocking and spam detection apps.
- Use Do Not Disturb (DND) services.
- Never trust caller ID alone—verify independently.

For Organizations:

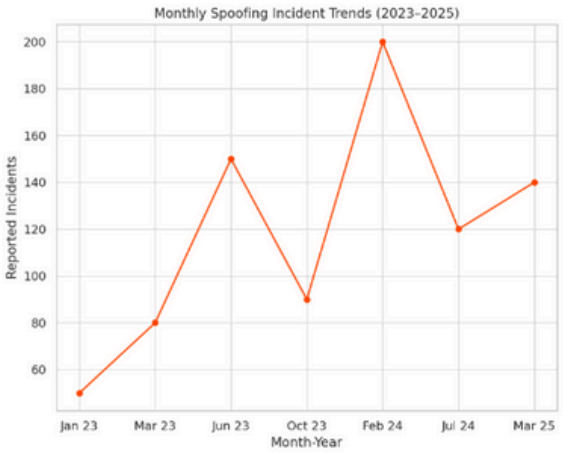
- Train employees on social engineering and spoofing awareness.
- Implement multi-layered identity verification.
- Protect your brand with STIR/SHAKEN frameworks where available.
- Report spoofing numbers to telecom regulators.

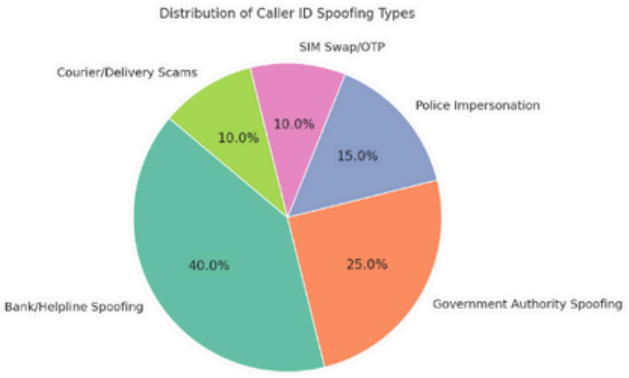
Recent Incidents

India has seen a sharp rise in spoofing incidents, particularly those targeting financial and law enforcement trust structures. Here's a visual summary of key incidents:

Date	Location	Type of Spoofing	Target	Impact
Jan 2023	Mumbai	Government (Income Tax Dept.)	General Public	Dozens misled, shared PAN/Aadhaar info
June 2023	Hyderabad, Pune	Police impersonation	Professionals	Threatened with arrest for fake cases
Feb 2024	Pan-India	Bank Helpline spoofing	ATM/Digital Wallet Users	Call centers impersonated RBI, SBI etc.
July 2024	Gujarat	Health service scam	Women, Senior Citizens	Promised free checkups, stole data
Mar 2025	Bengaluru, Lucknow	Courier service spoofing	Online Shoppers	Victims lost parcels and money

Total Incidents (2023-2025)	% Using Bank Spoofing	Top Affected City	Worst Month
3,200+	40%	Mumbai	February 2024





Government Actions:

- DoT's TAFCOP portal to check your SIM usage
- Nationwide caller ID verification drive
- Penalties on telecoms not blocking spoofed calls

Telecom Operators:

- Integration of spam detection
- Trial runs of verified caller ID logos

References

ECONOMICS TIMES

https://ciso.economictimes.indiatimes.com/news/cybercrime-fraud/dont-trust-caller-id-info-can-be-spoofed-easily-cyber-advisory-to-govt-officials/115041091

ASEE

https://cybersecurity.asee.io/blog/caller-id-spoofing-what-is-it-and-how-to-avoid-it/

FCC.GOV

https://www.fcc.gov/consumers/guides/spoofing

Don’t Be Fooled — Scammers Use Your Trust!

Call 1945

mhcyber.gov.in