S

Spoofing Attacks: Email, Caller ID, Website, DNS, IP, and ARP

Understand email, caller ID, website, DNS, IP, and ARP spoofing, what technical protections can and cannot prove, and how to verify and respond safely.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 What does spoofing mean?
02 Common types of spoofing
03 Email spoofing protections
04 Caller ID and text spoofing
05 Website and domain spoofing
06 DNS, IP, and ARP spoofing
07 Warning signs
08 What to do after suspected spoofing
09 Prevention

Spoofing means falsifying an identity or technical attribute so a message, call, website, or network packet appears to come from a trusted source. Attackers use spoofing for phishing, fraud, malware delivery, traffic interception, or hiding their origin. Some underlying techniques also have legitimate testing or routing uses; intent, authorization, and context matter.

01 What does spoofing mean?

To spoof something is to make its displayed or transmitted identity differ from its true origin. A **spoofer** may forge caller ID, an email sender, a look-alike domain, a DNS answer, an IP source address, or a local-network mapping. Spoofing creates the impersonation; phishing or fraud is often the social-engineering action that uses it.

02 Common types of spoofing

Type	What is falsified	Typical risk
Email spoofing	Visible sender or envelope/domain information	Phishing, invoice fraud, impersonation, and malicious attachments.
Caller ID spoofing	Name or number displayed for a call or text	Bank, government, employer, or local-number impersonation.
Website/domain spoofing	Look-alike domain, subdomain, page design, or displayed link	Credential and payment theft.
DNS spoofing	DNS answer or resolver path	Redirecting users to an unintended address.
IP spoofing	Source IP address in a packet	Reflection/amplification, trust abuse, or hiding packet origin.
ARP spoofing	IP-to-MAC mapping on a local network	Traffic interception, redirection, or denial of service.

03 Email spoofing protections

- **SPF** lets a domain publish which systems may send mail for it.
- **DKIM** adds a domain-associated cryptographic signature to selected message headers and body content.
- **DMARC** aligns authenticated domains with the visible From domain and defines reporting and handling policy.

Passing SPF, DKIM, or DMARC does not prove that a message is honest. An attacker can use a look-alike domain, a compromised legitimate account, or an authorized marketing platform. Verify unusual requests through a separate trusted channel.

04 Caller ID and text spoofing

A familiar caller ID is not identity proof. A scammer can display a bank, government office, local number, or even the recipient's own number. Call authentication systems such as STIR/SHAKEN can provide useful carrier-level attestation, but availability and displayed labels vary and they do not validate the caller's story.

If a call requests money, credentials, a one-time code, remote access, or urgent action, hang up and contact the organization using a number from its official site, statement, or card—not the number supplied by the caller or message.

05 Website and domain spoofing

- Read the registrable domain immediately before the top-level domain, not only a familiar word in the URL.
- Watch for substituted characters, extra words, misleading subdomains, and unusual endings.
- A padlock means the connection is encrypted; it does not prove that the site belongs to the expected organization.

- Use a saved bookmark or type the known official address for sensitive sign-ins and payments.
- Let a password manager fill credentials only on the domain for which they were saved.

06 DNS, IP, and ARP spoofing

DNSSEC validation can help detect forged signed DNS data, while encrypted DNS can protect queries between a client and trusted resolver. Neither guarantees that the destination itself is safe. Network teams can reduce ARP and IP spoofing risk with segmentation, switch protections, source validation, authenticated protocols, monitoring, and correctly configured routing and firewall controls.

End users should avoid ignoring certificate warnings, especially on public or unfamiliar networks. A VPN can protect traffic to its trusted endpoint but does not make a fraudulent website legitimate.

07 Warning signs

- An unexpected request creates urgency, secrecy, fear, or a payment deadline.
- The sender discourages verification or asks to use a new phone number or bank account.
- A reply address, link destination, or domain differs from the visible brand.
- A familiar caller asks for information the real organization should not need.
- Certificate warnings, changed DNS answers, duplicate IP warnings, or unexplained gateway changes appear.

08 What to do after suspected spoofing

1. Stop the interaction and preserve the message, headers, URL, caller details, and time.
2. Verify the person or organization through independently obtained contact information.

3. If credentials were entered, use a clean device to change the password, revoke sessions, and enable strong MFA.
4. If payment information or money was sent, contact the financial institution immediately through its official channel.
5. Scan the device if a file was opened or remote-access software was installed.
6. Report the incident to the service provider, employer, carrier, or relevant authority.

09 Prevention

- Use unique passwords, a password manager, and phishing-resistant MFA where available.
- Deploy SPF, DKIM, and DMARC for organizational email domains and monitor reports.
- Protect domain registrar and DNS accounts with MFA and change controls.
- Train staff to verify payment and account changes out of band.
- Keep browsers, phones, routers, and operating systems updated.
- Design procedures so caller ID, display names, and email branding are never accepted as sole proof of identity.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com