R

Robocalls: Scam Warning Signs, Blocking, Reporting, and Recovery

A robocall uses an automated dialer or prerecorded or generated voice. Some are legitimate; unexpected demands for money, codes, remote access, or secrecy are dangerous.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

A **robocall** uses an automated dialing system, prerecorded message, or generated voice to reach many phone numbers. Appointment reminders, school closures, public warnings, political messages, debt notices, and calls a person consented to receive can be legitimate. Scammers use the same technology for impersonation, payment fraud, credential theft, and malicious links.

Rules differ by country and by call type. A call being automated, unwanted, or absent from a do-not-call registry does not alone establish a crime, but it should never override independent verification.

Robocall scam warning signs

- an unexpected claim that a bank, tax agency, police department, delivery company, employer, or relative needs immediate action;
- threats of arrest, account closure, deportation, service cutoff, or public embarrassment;
- payment requested through gift cards, cryptocurrency, wire transfer, cash pickup, or payment to a new account;
- a request for a password, PIN, full card number, one-time code, recovery code, or screen sharing;
- instructions to install remote-support software, move money “for safety,” lie to bank staff, or keep the call secret;
- a recorded message asking you to press a key or call a number you have not verified.

Caller ID can be spoofed to display a local number or a real organization's name. Voice cloning can imitate a known person. Treat the displayed identity and familiar voice as claims, not proof.

Safe response

1. Do not provide information, press keys, follow links, install software, or make payment.
2. Hang up. If the caller claims to represent an organization, find its number on the official website, card, statement, or app and call independently.
3. For a family emergency claim, contact the person or another trusted relative through a known number and use a prearranged verification question where possible.
4. Preserve the displayed number, actual voicemail, date, time, claimed organization, callback number, and payment instructions without continuing the conversation.

Reduce unwanted calls

- enable carrier and phone call-labeling or blocking features;
- silence unknown callers when missing legitimate first-time calls is acceptable;

- block repeated numbers, recognizing that spoofers can change them;
- register with the applicable national do-not-call service to reduce covered marketing calls;
- limit public exposure of the number and avoid giving broad marketing consent.

Blocking cannot stop every call and may occasionally label a legitimate caller. Maintain another contact route for healthcare, school, delivery, and account recovery where needed.

Reporting

In the United States, the FTC accepts fraud and unwanted-call reports and the FCC accepts complaints about unwanted calls, texts, spoofing, and related service issues. The FTC's current robocall guidance also recommends call-blocking and call-labeling services. Elsewhere, use the telecom, privacy, consumer-protection, or police channel appropriate to the country.

Report the facts you observed. The displayed caller ID may belong to an uninvolved person whose number was spoofed.

If you paid or shared access

- contact the bank, card issuer, payment app, wire service, gift-card issuer, or cryptocurrency platform immediately and ask about reversal or fraud procedures;
- change exposed credentials from a clean device, revoke sessions, and review MFA and recovery methods;
- if remote access was installed, disconnect the device, preserve details, remove the tool, run trusted security scans, and consider professional or organizational incident response;
- monitor affected accounts and report identity theft or financial fraud promptly.

Robocall FAQ

Does answering one call compromise the phone?

Normally no. Risk increases when you disclose data, follow a link, install software, grant permissions, or make a payment.

Does caller ID authentication prove the caller's story?

No. Network attestation can help trace or validate use of a number but does not prove that the message or request is honest.

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