T

Tech Support Scam: Warning Signs, Remote Access, and Recovery

Tech support scams manufacture urgency to obtain money, credentials, or remote access. Recovery depends on what the scammer actually received or controlled.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

A **tech support scam** is fraud in which someone impersonates a software company, device maker, internet provider, security service, or internal IT team. The scammer invents a virus, expired subscription, refund, suspicious charge, or account problem to obtain payment, credentials, or remote access.

Legitimate companies do not make unsolicited calls because they detected an infection on a personal computer. Browser pages also cannot perform a complete device scan merely by loading.

Common approaches

- a full-screen browser warning with alarms and a phone number;
- a call claiming to be Microsoft, Apple, an ISP, a bank, or company IT;

- a fake invoice or renewal notice that tells the recipient to call;
- a search advertisement or fake support page above the legitimate result;
- a refund story that leads to remote banking, gift cards, cash, cryptocurrency, or a money transfer.

The FTC warns that scammers often request remote access and payment through methods that are difficult to reverse. See its current tech support scam guidance.

Warning signs

- unexpected urgency, threats, countdowns, sirens, or claims the computer will be blocked;
- requests to install remote-control software or paste commands into Terminal or PowerShell;
- Event Viewer, normal network connections, or harmless errors presented as proof of hackers;
- requests to hide the call from family, bank staff, or coworkers;
- payment by gift card, crypto, wire, cash shipment, or moving money to a “safe” account.

If you only saw a popup

Do not call, click, or download. Exit full-screen and close the tab. If the browser is trapped, force-quit it and reopen without restoring that page. Remove the site's notification permission and clear its site data. Run a scan if anything downloaded or redirects continue. A popup alone does not prove malware is installed.

If you called but gave no access or payment

End the call and block the number. Do not trust a follow-up “refund” or “fraud investigator.” If you disclosed a password, verification code, identity data, or card number, follow the relevant recovery steps even without remote computer access.

If a scammer had remote access

1. **Disconnect the computer from networks.** Do not continue banking or password changes on it.
2. **Record what happened.** Note the remote tool, session time, commands, files, accounts opened, phone numbers, and messages.
3. **Remove unattended access.** On a clean or safely isolated system, uninstall the remote tool and check whether it was configured to start automatically or allow access without approval.
4. **Scan or reinstall.** Run an updated full scan. A clean OS reinstall is the safest choice if the scammer had administrator access, ran commands, installed unknown software, or the scope is uncertain.
5. **Secure accounts from a clean device.** Revoke sessions and change passwords for email, password managers, banking, work accounts, and anything visible or used during the session. Review MFA, recovery methods, forwarding rules, and connected apps.

If you paid or moved money

Contact the bank, card issuer, payment app, exchange, or gift-card issuer immediately using independently verified details. Ask about a freeze, recall, chargeback, card replacement, and protection for linked accounts. Preserve receipts and transaction identifiers, then report the scam to the appropriate national fraud service or police.

For workplace incidents

Contact the internal security team immediately. Preserve identity, endpoint, remote-access, email, and network logs. Revoke enterprise sessions and investigate actions performed during access. Do not privately “clean up” a managed computer and destroy evidence.

Expect a recovery scam

Victim details are often reused. Nobody can guarantee recovery for an upfront fee, and legitimate investigators do not need gift cards, cryptocurrency, remote access, or another transfer to release money.

Tech support scam FAQ

Is remote-support software itself malware?

Usually not. The danger is unauthorized or deceptive use and any unattended access or payload added during the session.

Should I reset the router?

Only if its settings or administrator account were accessed. Focus first on the controlled device, exposed accounts, and payments.

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