



Tech Support & Device Access Scams

Responding to Device Scams

These scams occur when criminals pretend your device is infected, unsafe, or compromised and pressure you to act quickly. The goal is to make you grant remote access, install software, pay for fake services, or hand over credentials.

These scams may involve:

- Tech support scams
- Fake virus pop-ups or browser alerts
- Remote access scams
- “Security alert” phone calls

The warnings are designed to look urgent and authoritative, but they are fake.

Tech Support Scam – Do This First

Stop and Disengage Immediately

If you encounter a pop-up, call, or message claiming your device is infected:

- Do not click anything
- Do not call the number
- Do not install software
- Do not allow remote access
- Do not provide passwords or codes

Legitimate tech companies do not contact you out of the blue about infections.

Close the Scam Safely

If it's a browser pop-up:

- Do not click “OK,” “Cancel,” or “Scan”
- Close the browser tab or force-quit the browser
- If the pop-up won't close, restart the device or seek help.

If it's a phone call:

- Hang up immediately
- Do not engage or argue

Preserve Evidence (If Needed)

Before clearing anything:





- Take photos or screenshots of:
 - The alert or pop-up
 - Phone numbers or URLs shown
 - Messages or emails received
- Note:
 - Date and time
 - What the message claimed
 - Any actions requested

This supports reporting and recovery if needed.

If You Installed Software or Allowed Remote Access

Disconnect Immediately

- Disconnect the device from Wi-Fi and networks
- Turn off Bluetooth
- Do not continue using the device for sensitive activity

Seek Professional Help

If remote access was granted or software installed:

- Do not attempt advanced removal unless confident
- Improper removal can:
 - Leave backdoors
 - Hide spyware
 - Corrupt the system
- Seek help from:
 - Trusted IT professionals
 - Organizational IT support
 - Certified repair or security services

Secure Your Accounts (From a Safe Device)

If financial accounts were accessed during the remote session, contact banks or card issuers immediately from a different device.

- Change passwords for:
 - Email
 - Banking and payment apps
 - Apple ID / Google account
 - Work or school accounts
- Watch for login or password reset alerts





Common Tech Support Scam Types & What to Do

Fake Virus Pop-Ups

Signs:

- Loud warnings
- Countdown timers
- Claims of “critical infection”

What to Do:

- Close the browser
- Restart the device
- Run a reputable security scan if needed

Remote Access Scams

Signs:

- Install screen-sharing or “support” software
- Follow step-by-step instructions

What to Do:

- Disconnect immediately
- Remove software with professional guidance
- Change passwords from a safe device

“Security Alert” Phone Calls

Signs:

- Claims that your computer sent error reports
- Claims that your IP address is compromised
- Claims that law enforcement or a tech company is calling

What to Do:

- Hang up
- Verify independently
- Report the call

Report the Scam

- National Reporting
 - Federal Trade Commission (FTC)
 - Main federal agency for consumer fraud
 - reportfraud.ftc.gov
 - Internet Crime Complaint Center (IC3) – FBI





- Tracks internet-based financial crimes and scams
 - ic3.gov
- U.S. Postal Inspection Service
 - If the scam involved mailed checks, money orders, or parcels
 - uspis.gov/report
- Secret Service Cleveland Field Office
 - Investigates certain cyber-enabled financial crimes; use FTC, IC3, or local law enforcement for routine consumer scam reporting
 - 216-750-2058
- Ohio Resources
 - Ohio Attorney General – Consumer Protection & Identity Theft
 - <https://www.ohioattorneygeneral.gov>
 - Consumer Protection Hotline: 800-282-0515
- Geauga County
 - Geauga County Sheriff's Office
 - <https://www.geaugasheriff.org>
 - Local police non-emergency line for documentation
 - Call 911 if threats, coercion, or immediate danger are involved

Recovery – After a Tech Support Scam

- Monitor accounts and statements closely
- Watch for follow-up scams offering to “fix” the problem
- Keep all reports, case numbers, and evidence together
- Consider a full system reset if advised by professionals
- Tech support scams often lead to repeat targeting.

How to Reduce Tech Support Scam Risk

- Remember: Pop-ups don't diagnose infections
- Tech companies don't make unsolicited support calls
- Never grant remote access to unknown parties
- Slow down, urgency is a scam tactic
- Ask for help before acting under pressure
- Add a trusted contact where your financial institution offers it

