SCAM NOT ME

Tech Support Scam Prevention Guide

What Are Tech Support Scams?

Tech support scams occur when fraudsters impersonate technical support staff from well-known companies like Microsoft, Apple, or your internet provider. They claim your device has problems and offer to "fix" it—for a fee or by gaining remote access to your computer.

Common Warning Signs

Unexpected Contact

- **They call you** out of the blue claiming your computer has problems
- Pop-up warnings appear saying your device is infected
- You receive unsolicited emails about computer problems

Pressure Tactics

- They create urgency: "Your computer is at risk right now!"
- They use technical jargon to confuse you
- They won't give you time to think or consult others

Red Flag Requests

- They request remote access to your computer
- They ask for payment via gift cards or wire transfers
- They want your passwords or personal information

How These Scams Work

1. **Unsolicited Contact**: They reach you through phone calls, pop-ups, or emails
2. **Create Fear**: They claim your device has viruses, hackers, or critical errors
3. **Fake Diagnosis**: They have you check harmless system logs or run commands that show normal messages (but claim they're problems)
4. **"Fix" the Problem**: They ask for payment and/or remote access to your device
5. **Install Software**: They often install monitoring programs or malware

How to Protect Yourself

If You Get a Call:

- Hang up immediately

- Never provide personal information
- Don't allow remote access to your computer
- Don't provide any payment information

If You See a Pop-up:

- Don't click on it or call the number shown
- Close your browser using Task Manager (Windows) or Force Quit (Mac)
- If it won't close, restart your computer
- Update your antivirus software and run a scan

Always Remember:

- Legitimate tech companies **never** make unsolicited calls
- Microsoft, Apple, and Google **do not** call to report errors on your device
- Real support professionals **won't** ask for payment to fix security issues
- Tech problems **don't** typically generate urgent alerts with phone numbers

If You've Been Scammed

1. **Disconnect from the internet** immediately
2. **Change your passwords** from a different device
3. **Update and run antivirus software**
4. **Contact your bank** if you shared financial information
5. **Restore your computer** to an earlier point or reset if necessary
6. **Report the scam** to:
    - Federal Trade Commission (FTC): ReportFraud.ftc.gov
    - FBI's Internet Crime Complaint Center: IC3.gov
    - Your local police department

Remember:

Legitimate tech support will never:

- Contact you without you reaching out first
- Create urgency or pressure you to act immediately
- Ask for payment in gift cards or wire transfers
- Request access to your computer without your explicit request for help
- Claim to find problems you didn't report

Stay alert and protect your digital security!

SCAM NOT ME