# Tech Support Scam Checklist

**Quick Reference: Is This Contact Legitimate?**

Phone Call Red Flags - Check if ANY of these apply:

- ▢ Caller claims to be from Microsoft, Apple, Google, or another tech company about a problem you didn't report
- ▢ They say your computer is "severely infected" or "under attack right now"
- ▢ They create urgency by saying you must act "immediately" or "within 24 hours"
- ▢ They ask for remote access to your computer to "show you the problem"
- ▢ They request payment via gift cards, wire transfer, or immediate credit card payment
- ▢ They can't provide a specific ticket number or case reference when asked
- ▢ The caller ID shows a generic number or doesn't match the company's official number
- ▢ They become pushy or aggressive when you ask questions

Email Warning Signs - Check if ANY of these apply:

- ▢ Subject line uses urgent language like "IMMEDIATE ACTION REQUIRED" or "ACCOUNT SUSPENDED"
- ▢ Sender's email address doesn't exactly match the official company domain (@microsoft.com, @apple.com)
- ▢ Email addresses you as "Dear Customer" instead of your actual name
- ▢ Contains spelling errors or awkward grammar
- ▢ Asks you to click a link to "verify your account" or "update security settings"
- ▢ Threatens account suspension or data loss if you don't act quickly
- ▢ Requests personal information like passwords, Social Security numbers, or credit card details

Pop-Up Message Red Flags - Check if ANY of these apply:

- ▢ Takes over your entire computer screen

Cyber Smart Seniors
Digital Guidance for Today's Seniors

### Pop-Up Message Red Flags - Check if ANY of these apply (cont.):

- □ Makes loud beeping sounds or speaks the warning aloud
- □ Claims to be a "Microsoft Security Alert" or "Apple Warning"
- □ Shows a phone number to call for "immediate help"
- □ Prevents you from closing it easily or keeps reappearing
- □ Claims to have detected specific viruses or threats
- □ Asks you to download software to "fix" the problem

## Your Action Plan

### If You Receive a Suspicious Contact:

- □ Do NOT provide any personal information
- □ Do NOT allow remote access to your computer
- □ Do NOT download any recommended software
- □ Do NOT make any payments
- □ Hang up immediately or close the message
- □ Write down the phone number, email address, or website if possible

### Verify Legitimacy (The Safe Way):

- □ Use the official company website to find their real customer service number
- □ Call the official number directly (not the number provided by the suspicious contact)
- □ Log into your account through the official website to check for real alerts
- □ Ask a tech-savvy family member or friend for advice if unsure

### If You Think You've Been Scammed:

- □ Contact your bank or credit card company immediately if you provided financial information
- □ Change passwords for important accounts (email, banking, social media)
- □ Run a virus scan on your computer using your regular antivirus software
- □ Consider having a computer professional check your device
- □ Report the scam to the Federal Trade Commission at reportfraud.ftc.gov
- □ File a report with your local police if you lost money

### Remember the Golden Rules

Real Tech Companies Will NEVER:

- □ Call you out of the blue about computer problems
- □ Ask for remote access during an unsolicited call
- □ Demand immediate payment via gift cards or wire transfers
- □ Threaten to suspend your account within hours
- □ Ask for passwords or Social Security numbers over the phone

Real Tech Companies WILL:

- □ Let you call them back using their official support number
- □ Provide specific case or ticket numbers
- □ Give you time to think about any recommended actions
- □ Direct you to log into your official account to see alerts
- □ Offer multiple ways to resolve any legitimate issues

### Quick Contact Numbers (Save These!)

- □ Official Customer Service Numbers:
- □ Microsoft Support: 1-800-642-7676
- □ Apple Support: 1-800-275-2273
- □ Google Support: 1-650-253-0000
- □ Report Fraud: Federal Trade Commission - reportfraud.ftc.gov

### Prevention Tips

Protect Yourself Going Forward:

- □ Keep this checklist handy near your computer or phone
- □ Share this information with family and friends
- □ Trust your instincts - if something feels wrong, it probably is
- □ When in doubt, always hang up and call the official number
- □ Consider setting up caller ID to screen unknown numbers
- □ Keep your computer's built-in antivirus software updated

Cyber Smart Seniors
Digital Guidance for Today's Seniors

### Monthly Safety Check:

- ▢ Review recent bank and credit card statements for unauthorized charges
- ▢ Check that your computer's antivirus software is current
- ▢ Verify that important account passwords haven't been compromised
- ▢ Update family members on any new scams you've heard about

**Remember: Being cautious about unexpected tech support contacts doesn't mean you're not tech-savvy—it means you're smart! Real technology help is always available when YOU need it, not when scammers claim you do.**