



COMPUTER TIES IT RESOURCE CENTER • QUICK REFERENCE GUIDE

Remote Support Safety Guide

How to tell real technical support from somebody pretending to be it, and how to let a technician onto your computer safely.

FILLABLE PDF

Type into any field, then save or print a copy.

EDITION

Version 1.1 • September 2026

QUESTIONS?

(517) 788-6393 • computer-ties.com

Remote support, where a technician connects to your computer and takes a look, is the fastest way to fix most problems. It is also one of the best tools an attacker has, because it asks you to hand over control yourself.

The difference between the two is not what the screen looks like once the session starts. It is who got in touch first, how you checked they were genuine, and what they ask you for.

The words you will hear, and what they actually mean

Remote support session

A technician temporarily viewing and controlling your screen with your permission. Handing someone your car keys so they can hear the noise for themselves. Fine when you asked them to. Not fine when a stranger asks for them at a gas station.

RMM (remote monitoring and management)

Software already installed on computers a provider looks after, so they can see health and apply updates without interrupting you. A building manager with a maintenance key, on the buildings they manage, agreed in advance.

Tech support scam

Someone contacting you, unprompted, claiming your computer has a problem, in order to be granted access. The plumber who knocks and tells you about a leak you had not noticed.

Social engineering

Attacking the person rather than the technology. It is cheaper than breaking encryption and it works more often, which is why the phone rings instead of a firewall alarm.

1 The One Question That Prevents Most of This

Who contacted whom?

You got in touch, and support connected to you. This is normal. You rang, emailed, or logged a problem, and the connection follows a conversation you started.

They contacted you out of the blue and need access now. Treat this as an attack until you have checked it independently, however convincing the caller, the pop-up, the email, or the search result looks.

Almost every remote access scam depends on flipping that order around. If you did not start the conversation, stop and check before anything else happens.

2 Signs This Is Not Really Support

- ☐ A pop-up, an alarm noise, or a full-screen warning tells you to call a number.

Real security software never asks you to phone anybody.



- ☐ Somebody calls to say your computer is infected, is sending errors, or has been flagged.
No company monitors a random computer and phones the person using it.
- ☐ You searched for a support number and got a company you have never dealt with.
- ☐ They want access before you have had a chance to check who they are.
Being hurried past the checking step is the strongest warning sign there is.
- ☐ You are asked for your password, a sign-in code, or to approve a prompt on your phone.
- ☐ You are asked to install a remote access program you have never used with your own IT people.
Ask which program your organization actually uses, and check it with somebody you already know.
- ☐ The conversation moves toward money, especially gift cards, bank transfers, cryptocurrency, or a refund that needs access to your bank.
- ☐ You are told to keep it private, not to tell a colleague, or not to hang up.

3 Before You Let Anybody Connect

- ☐ Check that you started this.
You rang, emailed, or logged a problem, or the session was arranged with you in advance.
- ☐ Check who they are, independently.
Hang up and call the number you already have. Do not use a number the caller gave you, and do not simply call back the number that showed on your phone.
- ☐ See whether they can tell you about your problem, your organization, or your last conversation without you feeding them the details first.
- ☐ Close anything that does not need to be open.
Your bank, payroll, patient records, and personal files do not need to be on screen while somebody fixes a printer.
- ☐ Know how to end the session yourself, and stay at the computer while it is going on.
- ☐ If it feels wrong at any point, end it. You do not need a reason and you do not owe anybody an explanation.

4 During the Session, and Afterwards

Stage	What should happen	What should not
Starting	You open the program and read a code to the technician, or you accept a connection you were expecting.	They connect without you doing anything, or they ask you to turn off your security software first.
While it runs	You can see everything happening on your screen, and they explain what they are doing.	Your screen goes blank, or you are asked to look away or step out of the room.
Passwords	They use their own access, or ask you to type your password yourself without saying it out loud.	You are asked to read a password out, type it into a chat box, or approve a sign-in prompt you did not trigger.
Ending	The session closes and you can see that it has ended.	Something is left installed that nobody mentioned, or the program reconnects afterwards.



Stage	What should happen	What should not
After	You know what changed and why, and it is written down against your support request.	There is no record of what happened and nobody to ask.

5 How Remote Support Works at Computer Ties

Knowing what normal looks like makes anything abnormal easy to spot.

- ☐ **One-off sessions are started by you, when we ask.** We use a program called ShowMyPC for temporary sessions. You download it from our website and start it only when one of our technicians has asked you to.
It is temporary. It does not leave a permanent connection behind on your computer.
- ☐ **Computers we already look after do not need any of that.** Our remote monitoring and management software is already installed on them, so a technician has no reason to send you an installer or a link.
Enrollment links and internal management tools are not distributed publicly. If somebody sends you one out of the blue, it did not come from us.
- ☐ **Work is attached to a support request.** A technician can tell you what was reported, who reported it, and what they intend to do about it.
Ask them. A genuine technician will not mind in the slightest.
- ☐ **We will never ask for your password or a sign-in code.** Not on the phone, not by email, not during a session.
- ☐ **We will never ask for payment during a support session,** and never by gift card, transfer, or cryptocurrency.

Check with a call to a number you already have

Computer Ties Help Desk: (517) 905-3168 • Office: (517) 788-6393 • Email: helpdesk@computer-ties.com Help Desk hours are Monday to Friday, 8:00 AM to 5:00 PM. If you are already a customer and it is an emergency out of hours, call (517) 788-6393 and choose Option 9.

6 If You Think You Let Somebody In

Move quickly, and do not wait until you are certain. Work down this list in order.

- ☐ Disconnect the computer from the internet. Unplug the network cable, or turn off the Wi-Fi. Leave it switched on.
Switching it off can destroy information that helps work out what happened.
- ☐ Call your IT provider or whoever looks after your computers, right away.
Computer Ties customers should call the Help Desk on (517) 905-3168.
- ☐ Change your passwords from a different device, starting with email.
Changing a password on the computer somebody else may still be watching does not help.
- ☐ Call your bank immediately if money, card details, or a refund came up at any point.
- ☐ Write down what happened while you remember it: times, the number that called, what was said, what got installed, what they asked for.
- ☐ Do not wipe or reinstall the computer before somebody has looked at it, unless you are told to.
- ☐ Tell someone at work, even if it looks like nothing came of it.



■ Fill this in before you hand it out

Our IT provider is

The number we call them on

Our internal contact

Report problems to

Last updated

About this guide

This is general awareness guidance for staff. It does not replace your own organization's rules about remote access, acceptable use, or reporting. If your organization has requirements about who may connect to its computers, check what those require.

Support you can easily check up on

Computer Ties provides help desk support, remote and on-site help, and managed IT services across southern Michigan. Our customers always have a number they already know and a support request to point at, which is exactly what makes somebody pretending to be us easy to catch.

NEW PROJECTS AND PLANNING
(517) 788-6393

EXISTING CUSTOMER SUPPORT
(517) 905-3168



2903 West Michigan Avenue, Jackson, MI 49202 • computer-ties.com • Serving Jackson since 1990