



Tech Support Scams

Tech support scams are a wide ranging issue where scammers use scare tactics to trick you into unnecessary technical support services to supposedly fix device or software problems that don't exist. These scams are also known as Remote Access or RAT (Remote Access Tools) scams.

At best, the scammers are trying to get you to pay them to "fix" a nonexistent problem with your device or software. At worst, they're trying to steal your personal or financial information; and if you allow them remote access to your computer to perform this "fix," they will often install malware, ransomware, or other unwanted programs that can steal your information or damage your data or device.

Tools used by Tech support scammers to access your device remotely include TeamViewer, GoToMyPC, VNC Connect, LogMeIn, RemotePC. All of these programs have legitimate uses but should only be installed in cooperation with a known and trusted source.

Protecting yourself from Tech Support Scams is simple:

Remember that no tech company (Microsoft, BT, Apple, Amazon etc) will ever call to advise that they have found an issue with some element of your tech
Indeed, any claim to have identified one or other technical issues with your equipment is bogus
Never allow a random caller to persuade you to install remote access software
Hang up!

For more Police advice on Tech Support Scams, tap [here](#).

