

What are Tech Support Scams?

Tech support scams are fraudulent schemes where scammers impersonate legitimate technical support services to trick individuals into giving them access to their computers, personal information, or money. These scams typically begin with unsolicited phone calls, emails, or pop-up warnings on a computer, falsely claiming that the victim's computer is infected with malware, experiencing performance issues, or at risk of a security breach.

Once the victim is convinced there is a problem, the scammer offers to fix it. They ask the victim to grant remote access to their computer, often using legitimate software like TeamViewer, AnyDesk, or UltraViewer. These applications are designed for secure remote access and are widely used for legitimate purposes. However, in the hands of scammers, they can be misused to perform fake diagnostics, install malware, or simply demand payment for unnecessary services. In some cases, the scammer might also steal personal information, passwords, or financial details.



Tactics Used by Tech Support Scammers

- **Cold Calls:** Scammers often initiate contact through unsolicited phone calls, pretending to be from well-known companies like Microsoft, Apple, or other reputable tech support providers. They claim that they have detected issues on the victim's computer and offer to help resolve them.
- **Pop-Up Warnings:** Scammers use pop-up alerts on websites or via malware that appear legitimate. These pop-ups typically warn the victim that their computer is infected or compromised and include a phone number to call for immediate assistance.
- **Phishing Emails:** Scammers send emails that appear to be from trusted companies, warning the recipient of security issues or expired software licenses. The email will often include a link to a fake tech support site or a phone number to call.
- **Fake Websites:** Scammers create fake websites that look like legitimate tech support sites. Victims who search for help online may end up on these sites, where they are prompted to call a number for assistance.

- **Remote Access:** The scammer typically requests that the victim install remote desktop software, which allows the scammer to take control of the victim's computer. This access lets them manipulate the system, install malware, or steal personal data.
- **Payment Demands:** After "fixing" the nonexistent issue, the scammer will demand payment for the service, often using high-pressure tactics to coerce the victim into paying quickly.

How To Avoid Tech Support Scams

Understanding how tech support scams operate is the first step in protecting yourself. Here are some keyways to avoid falling victim to these scams:

- **Ask Scamio Pro:** Use [Bitdefender Scamio Pro](#) to check if a message is genuine. Our AI-powered scam detector analyzes potential frauds and lets you know if someone tries to scam you. Simply describe the situation or upload any images/links/text received, and Bitdefender will guide you further.
- **Be Skeptical of Unsolicited Contact:** Legitimate companies will not contact you out of the blue to inform you of issues with your computer. Be wary of any unexpected phone calls, emails, or pop-ups claiming your system is at risk.
- **Avoid Clicking on Pop-Up Warnings:** Never trust pop-up alerts on websites that claim your computer is infected. These are often scare tactics used by scammers to trick you into calling for fake support.
- **Verify Before You Act:** If you receive a warning or message claiming to be from a reputable company, don't engage immediately. Instead, contact the company directly using verified contact information from their official website.
- **Don't Grant Remote Access:** Never allow remote access to your computer unless you are certain you are dealing with a legitimate support agent. Even then, only grant access to companies you have contacted and trust.
- **Be Cautious with Payments:** Legitimate companies will never demand immediate payment for tech support services, especially via unconventional methods like gift cards or wire transfers. Always verify the legitimacy of any payment requests.

What To Do If You've Been Scammed

If you think you have provided your account details to a scammer or if you have already paid for fake support, contact your bank immediately and open a chargeback.

You may wish to file a complaint with the appropriate authorities or your regional fraud reporting center:

- in the **US**: file a report with the [FBI](#) | [FTC](#)
- in **Canada**: contact [Canadian Anti-Fraud Centre](#)
- in the **UK**: file a report with the [National Fraud & Cyber Crime Reporting Centre](#) | [Report a cold call](#)
- in **Australia**: contact the [ACCC](#)
- **other countries**: report international scams at [ECONSUMER.GOV](#)