A Call from Tech Support – Your Computer is Infected!

Summary

A tech support scam is where a criminal claims to be a legitimate technical support service (like Microsoft or "Windows Technical Support") and warns you about a virus or some other bad thing coming from your computer.

This scam begins when you get a cold call, or it could begin when you contact a commercial technical support organization that you found on Google or Bing.

The attacker will use bogus computer "technical-speak" or even show you real error messages to make you believe that the computer has serious issues that need to be fixed or that they've detected viruses on your computer. The scam artist tricks you into giving them remote access to your computer or for paying for software you don't need.

If you give the criminal access to your computer using remote access software or some web-based conferencing solution, it allows the attacker to take complete control of your computer where he can do very serious damage.

But the purpose behind their elaborate scheme isn't to protect your computer; it's to make money or steal your passwords or other personal data.

If You Get a Call – What to Do

If you get a call from someone who claims to be a tech support person, hang up. No company is monitoring your computer.

If you are concerned about a computer issue, it's best to take the computer to a known expert (where there is a building or office) or call someone known to be trustworthy to get help. Random people who call you or who you find by doing a Google search cannot really be trusted.

Warning Signs

- The biggest tip-off that this is a scam is the call itself – no company monitors your computer.
- A caller who creates a sense of urgency or uses high-pressure tactics is probably a scam artist.
- Do not rely on caller ID alone to authenticate a caller. Criminals fake caller ID numbers. They may appear to be calling from a legitimate company or a local number, when they may not even be in the same country as you.
- The caller has a heavy foreign accent and has an American sounding name.

How to Protect Yourself

- Never give your password to a stranger on the phone. No legitimate organization calls you and asks for your password.
- Never provide your credit card or financial information to someone who calls and claims to be from tech support.
- Don't give control of your computer to a third-party who calls you out of the blue.
- Online search results are not a good way to find technical support or get a company's contact information. Scammers place online ads in Google or Bing to convince *you* to call *them.* They pay to boost their ranking in search results so their websites and phone numbers appear above those of legitimate companies. If you want tech support, look for a company's contact information on their software package or on your receipt.
- If a caller pressures you to buy a computer security product or says there is a subscription fee associated with the call, hang up. If you're concerned about your computer, call your security software company directly and ask for help.

If You've Responded to a Scam

If you think you might have downloaded malware from a scam site or allowed a cybercriminal to access your computer, do the following:

- Remove malware. Update or download legitimate security software and scan your computer. Delete anything it identifies as a problem.
- Change any passwords that you gave out. If you use these passwords for other accounts, change those accounts, too.
- If you paid for bogus services with a credit card, call your credit card provider and ask to reverse the charges. Check your statements for any other charges you didn't make, and ask to reverse those, too.
- If you believe that someone may have accessed your personal or financial information, visit the FTC's identity theft website. You can minimize your risk of further damage and repair any problems already in place.