

Watch Out For Tech Support Scams

When you communicate with tech support, you want them to help you solve computer problems, not create them! Yet, that's exactly what scammers pretending to be tech support personnel are doing.

Here's how it works: Pop-up ads claiming to sell fixes for your computer lead you to a website to download the software. The website includes a phone number for you to call to "register" the software. When you call, the person on the other end of the line requests information, such as passwords or remote access to your computer. Using remote access, they "examine" your computer and tell you that it has problems that need additional "solutions." They then ask for your credit card number to purchase these so-called solutions that don't actually do anything. While they're at it, they may infect your computer with malware or use your financial information to commit credit card fraud.

In a variation of this scam, tricksters call you and claim that they're on the tech support team at Microsoft or another well-known company. They go through the same process of accessing your computer, getting credit card or other information, and then causing trouble.



To protect yourself, follow these tips:

- Never give access to your computer to someone who calls you out of the blue.
- To contact tech support, call the number you already have for your hardware or software.
- Never provide credit card information, passwords, or other sensitive data to someone claiming to be a tech support representative.
- Protect your computer from viruses.
- Learn how to avoid identity theft.

If you fear you may already have been a victim, check your computer for malware, change passwords you may have given out, and reverse any associated credit card charges.