Tech Support Scams

By: Federal Trade Commission

In a recent twist, scam artists are using the phone to try to break into your computer. They call, claiming to be computer techs associates with well-known companies like Microsoft. They say that they've detected viruses other malware on your computer to trick you into giving them remote access or paying for software you don't need.

These scammers take advantage of your reasonable concerns about viruses and other threats. They know that computer users have heard time and again that it's important to install security software. But the purpose behind their elaborate scheme isn't to protect your computer; it's to make money.

How Tech Support Scams Work

Scammers have been peddling bogus security software for years. They set up fake websites, offer free "security" scans, and send alarming messages to try to convince you that your computer is infected. Then, they try to sell you software to fix the problem. At best, the software is worthless or available elsewhere for free. At worst, it could be malware — software designed to give criminals access to your computer and your personal information.

The latest version of the scam begins with a phone call. Scammers can get your name and other basic information from public directories. They might even guess what computer software you're using.

Once they have you on the phone, they often try to gain your trust by pretending to be associated with well-known companies or confusing you with a barrage of technical terms. They may ask you to go to your computer and perform a series of complex tasks. Sometimes, they target legitimate computer files and claim that they are viruses. Their tactics are designed to scare you into believing they can help fix your "problem."

Once they've gained your trust, they may:

- ask you to give them remote access to your computer and then make changes to your settings that could leave your computer vulnerable
- try to enroll you in a worthless computer maintenance or warranty program
- ask for credit card information so they can bill you for phony services — or services you could get elsewhere for free
- trick you into installing malware that could steal sensitive data, like user names and passwords
- direct you to websites and ask you to enter your credit card number and other personal information

Regardless of the tactics they use, they have one purpose: to make money.

If You Get a Call

If you get a call from someone who claims to be a tech support person, hang up and call the company yourself on a phone number you know to be genuine. A caller who creates a sense of urgency or uses high-pressure tactics is probably a scam artist.

Keep these other tips in mind:

- Don't give control of your computer to a third party who calls you out of the blue.
- Do not rely on caller ID alone to authenticate a caller. Criminals spoof caller ID numbers. They may appear to be calling from a legitimate company or a local number, when they're not even in the same country as you.
- Online search results might not be the best way to find technical support or get a company's contact information. Scammers sometimes place online ads 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.
- Never provide your credit card or financial information to someone who calls and claims to be from tech support.
- 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.
- Never give your password on the phone. No legitimate organization calls you and asks for your password.
- Put your phone number on the National Do Not Call Registry, and then report illegal sales calls.

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, don't panic. Instead:

- Get rid of 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.
- File a complaint with the FTC at ftc.gov/complaint.

How to Spot a Refund Scam

If you paid for tech support services, and you later get a call about a refund, don't give out any personal information, like your credit card or bank account number. The call is almost certainly another trick to take your money.

The refund scam works like this: Several months after the purchase, someone might call to ask if you were happy with the service. When you say you weren't, the scammer offers a refund.
Or the caller may say that the company is going out of business and providing refunds for "warranties" and other services.

In either case, the scammers eventually ask for a bank or credit card account number. Or they ask you to create a Western Union account. They might even ask for remote access to your computer to help you fill out the necessary forms. But instead of putting money in your account, the scammers withdraw money from your account.