HOW COMPUTER SUPPORT SCAMS WORK

Scammers have been peddling bogus 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 are 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 alot 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 have 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.

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 on a phone number that you know to be genuine. A caller who creates a sense of urgency or used high-pressure tactics is probably a scam artist.

Keep these other tips in mind:

- Do not 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 are 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 are concerned about your computer, call your security software company directly and ask for help.

Mississippi Attorney General’s Office Consumer Protection Division 2013