Avoiding Tech Support SCAMS

You’re working on your computer when, suddenly, a message pops up on the screen: “Virus detected! Call now for a free security scan and to repair your device.” That’s a tech support scam. Don’t call, text, or email. Legit tech support companies don’t operate that way.

Scammers pose as big-name companies and use pop-up messages, fake websites, and phone calls to trick you into thinking your computer has an urgent problem. Their plan is to get your money by selling you worthless software, enrolling you in fake programs, or getting you to pay for useless tech support. The scammers urge you to call a toll-free number immediately, threatening that you may lose personal data if you don’t. They say they’ve detected viruses or other malware on your computer. They claim to be “tech support” and will ask you to give them remote access to your computer. Eventually, they’ll diagnose a non-existent problem and ask you to pay for unnecessary — or even harmful — services.

They try to sell you a security subscription or other “services” that range from worthless (for instance, they’re available for free elsewhere) to malicious (they install dangerous software that can help them steal your personal information.)

What can you do to defeat these Tech Support Scams?

- If you get an unexpected or urgent call from someone who claims to be tech support, hang up. It’s not a real call. And don’t rely on caller ID to prove who a caller is. Criminals can make caller ID seem like they’re calling from a legitimate company or a local number.
- If you get a pop-up message that tells you to call tech support, ignore it. There are legitimate pop-ups from your security software to do things like update your operating system. But do not call a number that pops up on your screen in a warning about a computer problem.
- If you’re concerned about your computer, call your security software company directly — but don’t use the phone number in the pop-up or on caller ID. Instead, look for the company’s contact information online, or on a software package or your receipt.
- Never share passwords or give control of your computer to anyone who contacts you.

And if someone asks you to pay for anything — including tech support services — with a gift card, cash reload card, or a wire transfer, it’s a scam. No legitimate company will tell you to pay that way.

Report these scam on the FTC website at www.ftccomplaintassistant.gov

Carol Kando-Pineda, an Attorney with the FTC’s Division of Consumer and Business Education, alerts us to an even more insidious form of tech support scam — the Refund Scam. If you paid for tech support services, and you later get a call about a refund, that call is probably also a scam. Don’t give the person any personal or financial information.

The refund scam works like this: Several months after a purchase, someone calls to ask if you were happy with the service. If you say “No”, the scammer offers a refund. Or, the caller says the company is going out of business and giving refunds. The scammer eventually asks for your bank or credit card account number, or asks for access to your bank account to make a direct deposit. But instead of putting money in your account, the scammer takes money from your account.

If you get a call like this, or any of the many technical support scam variations, hang up, and report it to www.ftccomplaintassistant.gov

Volunteers at all four offices are ready, willing and able to assist you. To keep up with the latest scams, LIKE “Seniors vs. Crime Region 4” on Face Book. Hablamos Español. Por favor pregunte por Yolanda. Martes a Viernes: 10:00 A.M. a 2:00 P.M., (352) 689 4606.