FLORIDA CONSUMER eNEWSLETTER
www.800helpfla.com | 1-800-HELP-FLA (435-7352) | 1-800-FL-AYUDA (352-9832)

Tech Support Scams

Cybercriminals are no longer targeting victims solely through email messages and fake websites. They're diversifying their tactics and contacting individuals by telephone, claiming to represent well-known software companies and offering to solve computer problems. These individuals may claim that they have detected viruses or other malware on your computer to trick you into granting them remote access to your computer, or paying for software you don't need. The goal of these fraudulent individuals is to make money and access your personal files to steal your identity.

Once scammers have gained your trust, they may ask you to give them remote access to your computer in order to make changes to your settings that could leave your computer vulnerable; try to enroll you in worthless computer maintenance or warranty programs; 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; or direct you to websites and ask for your credit card number and other personal information. Regardless of the tactics they use, their intention is to take your money.

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.

How Can I Avoid Tech Support Scams?

- Never grant a third party access to your computer unless you can verify that it is a legitimate representative of a

computer support team with whom you are already a customer.

- Never provide credit card or financial information over the phone, especially if you did not initiate the call or it is not from a known and trusted source.
- Never provide a password over the phone. No legitimate organization will call you to verify your password.
- If you receive a call claiming there is a virus on your computer, hang up!

Steps to Take if You Become a Victim

- Update or download security software from a legitimate source and scan your computer. Delete any malware or viruses that may have been downloaded or installed through a third party.
- Change the passwords for your computer, email and online banking/credit card accounts.
- Contact your credit card provider and dispute charges for any bogus services rendered or purchases made without your consent.
- Consider placing a fraud alert on your credit report if you shared personal and banking information with the scammer. Fraud alerts can be administered by calling one of the three major credit report agencies: Experian, Equifax or TransUnion.

For additional information, contact the department at 1–800–HELP–FLA (435-7352), 1–800–FL–AYUDA (352-9832) en Español, or visit 800helpfla.com.

Repost by Napoles Consulting, Inc. 954-364-4970