President's Corner: Tech Support Scams
By Eric Moore
October 12, 2019

Tech support scams have become a serious problem in recent years as the number of people in the world connected to the Internet continues to grow. Numerous news reports, articles, podcasts, and YouTube videos demonstrate that such scams are not going away. They must be successful as the Nigerian 419, even though efforts are made to educate computer users not to fall for these scams. The risk can be considerable, whether you lose money, privacy, or control of your computer. Do be careful with whom you deal. Do not give your money or control of your computer to someone without being certain they are legitimate.

Tech support scams commonly show up in one of two ways. You may receive an unsolicited phone call claiming a risk such as a virus, hacker, or expired software subscription will compromise your computer, and possibly your personal data as well. Some calls will immediately connect you to a live agent while others may require you to call back. Once you are connected to someone (who most likely speaks with a heavy accent works for a rogue outfit in a foreign country), you will be instructed to perform a series of tasks that supposedly prove that your computer is in danger. They may falsely claim that innocuous errors in the Windows system log file or information displayed by network tools are proof of the presence of a virus or hacking activity. The "agent" may then offer to help by performing tasks to clean the problem, but most likely will install useless or malicious software on your computer. You may also be asked to pay money for the service, usually in a manner that cannot be traced such as an electronic money transfer or gift cards. If you question or argue with the agent, he will vehemently deny any deception.

Another way of tricking users into tech support scams is to generate a pop-up window in the web browser reporting some dire problem and directing the user to call an 800 number for assistance. (Some even activate Windows narration, so an ominous electronic voice reads the message to the user.) Closing the pop-up window may be nearly impossible. Forcefully shutting down the browser through Task Manager or logging off Windows may be the only way to eliminate it.

Please always be skeptical of any tech support problems reported to you through pop-ups and unsolicited phone calls. It is safe to say that no legitimate company—including Microsoft and Apple—will ever take the initiative to contact you about a security issue with your computer. You must do so if you ever suspect a problem. No one is out there monitoring your computer for suspicious or malicious activity. (One exception is your ISP, which may shut down your Internet access if they detect a virus or other malware active on your computer. The "walled garden" they put you in will present a page to the effect that you need to contact them to resolve the issue.) Even if a company such as Microsoft could detect a user's computer has a virus, the best they would know is the IP address of the computer. Tracking the IP address down to a user's address and phone number is not easily done and usually requires the cooperation of the user's ISP. (Don't believe all you see on *NCIS* and other crime dramas that make it look so easy.)

If you are confronted with such a scam, get out as quickly as you can. If you receive a phone call, simply hang up. It is pointless to argue with the scammer and trying to trick him may only anger him. If the scammer knows your phone number, then there are possibilities of getting back out of spite, such as *swatting* you. Many individuals have recorded and posted YouTube videos of themselves baiting scammers by acting dumb and wasting their time for a half hour or more. The videos can be

educational as to what the scammers do to try fooling their potential victims and entertaining as well. However, once the scammer is caught red-handed—proven to be a liar—he tends to become annoyed or angry and turns into a vile potty-mouth. I recommend against baiting scammers, as you don't know how they will react.

If you are faced with an annoying pop-up, you may need to use Task Manager to shut it down. A web search such as *shut down Chrome through Task Manager* should lead you to instructions on how to forcefully shut down the browser and save you the trouble of logging out or rebooting. If you are concerned about possible malware, be sure your anti-virus software is up-to-date and perform a thorough scan. You can also get a free second opinion with Malwarebytes and Trend Micro HouseCall.

For more information, please check out the video posted by Ask Leo!

Be safe and be skeptical...always.