Nicolet NATIONAL BANK Real People. Real Conversations.

SCAM AWARENESS BULLETIN

Tech Support Scam

Introduction

Perpetrators of tech support scams try to trick victims into believing their computers are infected and they need help. Some scammers pretend to be connected with Microsoft, Apple or a familiar security software company such as Norton or McAfee, and claim to have detected malware that poses an imminent threat to the person's computer. Other scams feature planted website ads or pop-ups that display warning messages, some even feature a clock ticking down the minutes before the victim's hard drive will be destroyed by a virus - unless he or she calls a toll-free number for assistance deactivating the menace. Such scammers will often ask for remote access to your computer to run phony diagnostic tests and pretend to discover defects in need of fixing. They'll pressure you to pay unnecessary repairs or add new software and ask for payment via gift cards, wire transfer or through a money transfer app.

Technical Support Scam Motivation

The common motives behind these tech support scams are to extort the victim to gain money as well as installing malware such as keyloggers or backdoor Trojans in order to gain access to personal information.

Main Ways this Scam is Executed:

Cold Calls and Fake Phone Calls: Technical support scammer cold calls are when an individual calls the victim, claiming to be from tech support at a reputable company and stating they have found malware of the victim's computer.

The scammer will then try to get the user to install some type of remote access desktop software under the pretext of helping to remove the infestation. This would allow the attacker access to the victim's computer in order to install real malware. It can be difficult to stop scammers with security software once you grant remote access.

In addition to attempting to install malware on the victim's machine, these scammers will often ask for a fee via cryptocurrency, credit card to fix the issue. That's one way they can steal financial information.

Pop-up Warnings: Tech support pop-up warnings occur when a user is browsing the internet.

Usually, the victim is viewing a website that contains links to related content and when the user clicks on one of those links, it will redirect them to a website hosting the pop-ups. These pop-ups can be terribly intrusive, making it difficult for the user to close the window.

The pop-ups will display a message stating that the computer is infected with malware and offer a phone number for help with removing the malware. Often, these pop-ups will look like they come from a legitimate source. .

The Microsoft Tech Support Scam: Scammers like to take advantage of name recognition, pretending to represent well-known software companies such as Microsoft or Apple.

With the Microsoft tech support scam, a fake representative will call you, even spoofing the caller ID so it looks like the phone call really came from the software giant. The scammer will walk you through the process of installing applications that allow remote access to your computer. Or, the scammer may initiate contact by displaying fake pop-up messages on your screen that trick you into calling a fraudulent 'support' hotline.

With both scams, the goal is to get you to pay, in the form of a one-time fee or subscription, to fix the problem.

If someone claiming to be a representative calls you, hang up! Software companies don't initiate contact via phone or email messages to fix your computer issues. These companies never include phone numbers on its error and warning messages.

In fact, communication always has to be initiated by you. Visit the company's official website and follow prompts to get help if you're having device problems and to report scams.

When you download software, make sure it's only from official vendor websites or the Microsoft store. Software from third party sites may have to be modified to support scam malware and other threats.

Tech Support Refund Scam: If someone calls a few days, weeks, or months after you've made a tech support purchase and asks if you're satisfied or to offer a refund for tech support services you paid for, it's likely a fake refund scam. If you say 'No' they'll offer you a refund. In another variation, the caller says the company is giving refunds because it's going out of business. No matter the story, they're not giving refunds. They are trying to steal your money. Do not give them your bank account, credit card or other payment information.

Other Red Flags

Y**our computer is "sending out errors":** Scammers might also say your PC is "sending spam," "infected with a new virus undetectable by current scanners," or something similar. Even if all of these problems were true, corporate tech support wouldn't reach out to you about it.

The "Event Log Viewer" Trick: The scammers want you to think they're knowledgeable and that there's a problem with your PC. They do this by asking you to open the Windows Event Log Viewer so they can attempt to prove their case. Some kind of minor error or warning will almost always appear there. The presence of these routine glitches doesn't mean your system is having any real problems or is infected.

Tool installation: This is the part where the scam gets dangerous. The scammers want to take control of your computer, but not for the purpose of fixing it. The scammers want to infect your computer with malware, rootkits, keyloggers, etc.

How to Identify and avoid Pop-ups and Cold-calling Tech Support Scams

Pop-ups: Examine the message closely – look for obvious signs which might indicate fraud or deception, such as poor spelling and bad grammar, unprofessional imagery, and language that creates a sense of urgency.

You can also do an internet search for the phone number or business name that is listed in the pop-up to verify legitimacy.

There are many websites where people report scammers. If it is a scam, there will likely be an abundance of search results, often on the first page of the search, that clearly point out the scammer.

Cold-call telephone scams: Legitimate tech companies will not contact you by phone, email or text message to tell you there's a problem with your computer.

Scammers can have extremely thick foreign accents but claim their name is something decidedly Western, such as "Mike." Many of these scams are run from giant call centers in places like India and Pakistan. Or parts of China or South-Central Asia.

Spoofed Caller IDs: It is a trivial matter to "spoof" the caller ID system to display any name or number the scammer wants. Just because your phone says "Microsoft" or "Dell" it doesn't mean these companies are at the other end.

If you get a phone call from someone you suspect is a scammer, simply hang up. If you are on your cell phone, you can block them and send a spam report to Apple or Google. If you're still concerned the call was legitimate, you can always contact your computer's manufacturer directly for tech support

Do's and Don'ts

Do hang up if you get an unsolicited call from someone who claims to be a tech support provider for your computer or software.

Do get rid of a fake virus alert message by shutting down your browser. You can do this on a Windows PC by pressing Control-Alt-Delete and bringing up the Task Manager. On a Mac, press the Option, Command and Esc (Escape) keys, or use the Force Quit command from the Apple menu.

Do use antivirus software to regularly scan your computer for malware, and run a scan immediately after getting a scam pop-up.

Do keep your security software, browser and operating system up to date, and consider using your browser's pop-up blocker.

Do contact a computer technician you trust if you think there might be a genuine problem with your machine.

Do contact your credit card company and request a reversal of the payment if you've been victimized. You'll also want to look for other unauthorized charges and ask for those to be reversed as well.

Do Change your passwords

Do Alert the financial institutions you do business with.

Do Consider filing a police report, especially if money was stolen from you. Save all information or messages about the offer, technical issue that was reported to you, and/or the individual(s) who contacted you. You may need to provide this information when you file a report

Don't give remote access to your computer or payment information to someone who calls you out of the blue.

Don't rely on caller ID to determine if a caller is on the level. Scammers use "spoofing" techniques to make it look like they're calling from a legitimate number.

Don't call the number in pop-up virus alert. Real warnings from your operating system or antivirus program will not ask you to call anyone for support.

Don't click any links in the pop-up, even to close the window. This could redirect you to a scam site or launch a "dialogue loop," continually serving pop-up messages.

Don't buy security software from a company you don't know. If the name is unfamiliar, do an internet search to see if it has been linked to adware or scams.

Don't open previously closed sites if prompted to do so when you restart the browser after getting a scam pop-up.

Works Cited:

Tech Support Scams as found at https://www.aarp.org/money/scams-fraud/info-2019/tech-support.html on Oct 30, 2019

How to Spot, Avoid and Report Tech Support Scams as found at https://www.consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams on Oct 30, 2019

Protect Yourself from Tech Support Scams as found at https://support.microsoft.com/en-us/help/4013405/windows-protect-from-tech-support-scams on Oct 30, 2019

Ho to recognize and Avoid Tech Support Scams as found at https://us.norton.com/internetsecurity-online-scams-how-to-recognize-and-avoid-tech-support-scams.html on Oct 30, 2019