HOW TO AVOID TECH SUPPORT SCAMS

Cybercrimes are costing Americans nearly $3 billion dollars per year and are on the rise. Our community has seen a recent increase in technical support scams that target computer users by falsely claiming to represent legitimate technical support departments of major corporations such as Microsoft, Apple, and Amazon.

The scams can be very expensive and disruptive, resulting in permanent loss of data and exposing users to costly charges and even potential identity theft. Tech support scams are typically initiated in one of two ways:

Tech Support Robocalls

Robocallers will falsely identify themselves as a technical support representative of familiar tech-related companies such as Microsoft, Apple, or other security-related providers (e.g. Norton, McAfee) and tell you that they have identified an imminent threat to your computer.

They prey on victims' fears that their computers have been hacked and will ask for remote access to run phony diagnostic tests. Once they have control of your computer, they will then press you to pay hundreds of dollars for phony services and software you don't need and may in fact infect your computer with harmful malware that can be used for identity theft.

Computer Fake Virus Alerts and Adware

Similar to robocalls, scam pop-ups can invade your computer when you click on "adware" or "scareware" that can unwittingly download malicious software.

The adware hijacks your Internet browser and has a threatening alert message that urges you to call a toll-free number to speak to a technician to fix the problem. This results in a high-pressure sales pitch for payment to fix the problem.

DO'S & DON'TS TO STAY SAFE

Fortunately, you can avoid these scams by being aware of the warning signs for scammers and implementing precautions against being infected by malware and viruses.

Do's

- Hang up the phone if you get an unsolicited phone call from someone claiming to work for a major tech company. These companies typically have policies NOT to contact customers unless the customer initiates an interaction.
- If prompted by a suspicious fake virus alert message, shut down your browser. For PCs, press Ctrl-Alt-Delete; and on a Mac, press Option, Command, and Esc keys or Force Quit command from the Apple menu.
- Implement best practices for healthy computing, including running antivirus software and keeping your computer up to date. Make sure you have proper backup and recovery mechanisms in place to recover data in case of an attack.

Don'ts

- Don't give remote access to your computer or give payment information over the phone to unsolicited callers.
- Don't call the number in a pop-up virus alert.
- Don't click on any links in suspicious pop-ups. This may redirect you to a scam site or download malware and infect your computer.

Contact the author at mitchell@bridgittech.com.