Scam Alert – Tech Support

By Putnam County State Bank – To Keep it From Happening to You

Tech support scams can work in different ways. It can be over the telephone, through email or through malicious software. Scammers are trying to find a way to get to your computer. Although it comes in different forms, it is after the same thing: your money and your information.

How this scam works

These scammers will call you or email you and claim to be from: **Windows, Windows Helpdesk, Windows Service Center, Windows Tech Support, Microsoft Tech Support, Microsoft Support, Windows Technical Department Support Group, Microsoft Research and Development Team (Microsoft R & D Team), your internet service provider or cable provider.** They might often try to confuse you with a lot of technical terms. They will say your computer is infected with viruses or malware or your computer is sending error messages. They will say anything to convince you to allow them access to your computer.

The popups ads from malicious software will have messages like “SECURITY ALERT” or “Urgent Notice: your data may be at risk”. A phone number or link will be included to receive assistance. Once you click on the provided link or place the phone call, you will be prompted to pay for the “Antivirus” product to clean your “infected” computer. This antivirus product will turn out to be completely useless or a product you could have received for free somewhere reputable.

Once access is granted, the scammers can do a variety of things. They can make changes to your system to make it vulnerable to future attacks. They can trick you into installing malware that can steal sensitive data. They may try to enroll you in computer warranty or maintenance programs that are worthless. They may also ask for credit card information to bill you for phony services or direct you to a website to enter your card information.

What you need to be aware of

Never rely on caller ID alone to authenticate a caller. Scammers can spoof caller ID numbers for companies like Microsoft and even your internet service provider. It may appear that the caller is from where they say they are when actually they are in a different country.

These cybercriminals often use public phone directories. This gives them your name and other information to have when they call. Do not be impressed or even scared if they have this information. It is in the phone book and can be found easily online. They may even guess the operating system on your computer to aid in the scam.

Windows, Windows Helpdesk, Windows Service Center, or Windows Tech Support are not legitimate companies. Furthermore, Microsoft or their partners or any other legitimate company will never make unsolicited phone calls to fix security problems on your computer or to install software fixes.

NEVER provide credit card information or financial information to someone who calls you and claims to be from a tech support company. NEVER give any passwords on the phone. NEVER give control of your computer to anyone that calls unexpectedly. NEVER respond to emails from tech support

companies without having an established relationship with them, and then call the company to verify the email. NEVER click on popup ads.

If a call sounds legitimate, hang up and call back at a number you know to be correct. A scammer will try to dissuade you. Any caller that says “You have to act now” or other phrases that creates a sense of urgency or any caller who uses high pressure methods to get you to buy a security product or service is a scammer. Resist the pressure to act quickly.

Get as much information as possible from the scammer.

- The caller’s name
- The company name
- Location of the caller and the company
- Telephone number and email address
- Any websites used by the company

If you responded to a scam

Update legitimate antivirus software and the operating system on your computer on a regular basis.

Terminate all communication with the scammer. If the scammer has access to your computer, immediately shut down the computer and remove the Ethernet cable (connection to the internet). This will disconnect the pathway to the scammer.

Purchase and install legitimate antivirus/antimalware software. There are also free alternatives. The top 5 free antivirus programs (as rated by PCmag.com) are: Avast, AVG, Panda, Bitdefender, and ZoneAlarm. After installation, run the program and delete anything malicious that was found.

Don’t have a password to get on to your computer? Set one up. It is also wise to set up both administrator and user accounts on your computer, each with their own password. The administrator account should be the account that has the ability to install, modify or delete software. The user account should be the general account that is logged on to. This is just one more hurdle that a scammer will have to overcome in order to get to your information.

Change any passwords that you gave out to the scammers. Change your passwords to all financial institutions including credit card companies. If the same password is used in multiple places (bad idea) change those also.

If charges were made with a credit card, call your provider and ask for the charges to be reversed. Check statements often for any fraudulent charges.

If you think someone has gained access to your personal or financial information, you can minimize the damage and repair any problems cause by visiting the Federal Trade Commission’s identity theft website at: https://www.consumer.ftc.gov/features/feature-0014-identity-theft.

If the scammer represented themselves as a representative from Microsoft or Windows, Microsoft wants to know. Please report the scam at: https://support.microsoft.com/en-us/getsupport?oaspworkflow=start_1.0.0.0&wfname=scamsurvey&ccsid=636041082796784386.

Please file a complaint at: https://www.ic3.gov. This is the FBI’s site for Internet Crime.

The Federal Trade Commission wants to know too. File a complaint with them at:
https://www.ftccomplaintassistant.gov