CITY OF PARMA OHIO

LAW DEPARTMENT

6611 RIDGE ROAD | PARMA, OHIO 44129-5593 | 440-885-8132

Timothy G. Dobeck
Law Director
Prosecutor

October 16, 2019

LAW DIRECTOR ADVISORY

Tech Support Scams – What you Need to Know

There has been a recent surge in scams which involve scare tactics to trick you into paying for unnecessary technical support services. Scammers, who pretend to work for Microsoft or similar vendors, may contact you and attempt to convince you that there is a problem with your PC.

These scams are often initiated by a scammer who may call you directly on your personal phone number which can be found on publicly available directories. They may even spoof the caller ID to display a legitimate phone number from a trusted company. Scammers might also use email or chat to contact you. Their messages will likely include phone numbers or website links directing you to a fake tech support representative.

Another way a scammer may contact you is by exploiting malicious ads in dubious websites to redirect you to a fake tech support hotline. These ads when clicked will generate fake error messages or continuous pop-up messages that will effectively lock your browser. The fake messages will display support numbers and urge you to call them.

Once the scammer gains your trust, they will offer to fix the fake problem by running diagnostic tests on your device. The "fix" will likely involve the scammer asking for the login credentials to your device, or else they may direct you to a website to install software that gives them remote access to your device. Their software, like malware-laden online advertisements, will only misrepresent normal system outputs designed to convince you that your device is malfunctioning. The scammer will rely on your fear of these error messages to sell you fake solutions for your "problems" and ask for payment either as a one-time fee or subscription to a purported support service. Demands for payment often come in the form of a credit card charge, bitcoin, or gift card.

Treat unsolicited phone calls, emails and other messages from purported tech vendors with great skepticism. Tech vendors will never contact you first to offer support or security services. These communications are almost always a scam. Do not give them any information, do not give them access to your PC, do not give them any money, and do not go to any website they suggest. Hang up and definitely do not call any number that appears in pop-up notifications.

If you have installed potentially malicious software at a suspected scammer's behest, uninstall any such application immediately. If you have given control of your device to a scammer, seriously consider resetting your device. At a minimum, use verified security software to detect, quarantine, and remove malware and other threats from your system. Apply all available security updates and activate a firewall to block traffic to online services. Also, change your passwords to a unique string of letters, numbers, and characters.

If you have already paid for fake support services using a credit card, contact your provider to contest the charges. If you have paid using gift cards, contact the issuing merchant to cancel the cards. Unfortunately, confirmed bitcoin payments are irreversible and cannot be cancelled. Report the scam to the vendor (for Microsoft, www.microsoft.com/reportascam), the Ohio Attorney General (www.ohioattorneygeneral.gov/About-AG/Contact/Report-A-Scam), and the Federal Trade Commission (www.ftccomplaintassistant.gov). Last, but not least, file a report with your local police department.