City of Parma, Ohio

LAW DEPARTMENT

7335 RIDGE ROAD | PARMA, OHIO 44129-5593 | 440-885-8132

Timothy G. Dobeck
Law Director
Prosecutor

June 6, 2023

Law Director Advisory

Tech Support Scams – What You Need to Know

Recently, scam calls and emails claiming to be affiliated with Microsoft and other large tech companies have been on the rise. The caller will claim that your device has been compromised and you need to act quickly to save it. They will then leverage this concern into getting personal information, making you pay for unneeded services, or gaining control over your computer and making you pay to release it.

According to research done by the FBI, almost 24,000 people reported losing nearly $348 million due to tech support scams in 2021, which is a 137% increase in losses from the previous year. A similar study from Microsoft showed that 60% of global consumers encountered a tech support scam in 2021 and 15% of them were tricked into continuing with the scam. The severity of these scams has prompted the FBI and FTC to issue multiple warnings and advisories to protect the public.

How the scam works and how to prevent it:

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 on 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.

The easiest way to prevent becoming a victim to this scam is by treating unsolicited phone calls, emails, and other messages from purported tech vendors with great skepticism. Legitimate 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.

Sources to Contact if You are Hacked or Need Assistance:

- **FTC (Federal Trade Commission)**
  Report Fraud Website: https://reportfraud.ftc.gov/#/
  What to Do if You Were Scammed Website: https://consumer.ftc.gov/
- **FBI (Federal Bureau of Investigation)**
  Internet Crime Complaint Center (IC3) Website: https://www.ic3.gov/
  Elder Fraud Information: https://www.ic3.gov/Home/EF
- **DOJ (Department of Justice)**
  DOJ Elder Fraud Hotline Phone Number: 1-833-372-8311
- **Ohio Attorney General**
  Elder Justice Unit Phone Number: 1-800-282-0515
  File a Complaint Online:
  https://www.ohioattorneygeneral.gov/Individuals-and-Families/Consumers/File-A-Complaint
- **Parma Police Department**
  Non-emergency number 440-885-1234