CITY OF VENTURA POLICE DEPARTMENT

NEWS RELEASE

Contact: Community Outreach, (805) 339-4317
Release Prepared by: Ashley Bautista

Tech Support Scam Alert

The Ventura Police Department has received reports of residents becoming victims of a tech support scam. Residents are urged to review scam prevention measures to avoid becoming a victim of this scam.

Scammers use scare tactics to trick you into paying for unnecessary technical support services that supposedly fix your device, platform, or software problems.

Scammers may call you directly on your phone and pretend to be representatives of a software company. They might even spoof the caller ID so that it displays a legitimate support phone number from a trusted company. They then ask you to install applications that give them remote access to your device. Using remote access, these scammers can misrepresent normal system output as signs of problems.

Scammers might also initiate contact by displaying fake error messages on websites you visit, displaying support numbers and enticing you to call. They can also put your browser on full screen and display pop-up messages that won't go away, essentially locking your browser. These fake error messages aim to trick you into calling an indicated technical support hotline.

When you engage with the scammers, they can offer fake solutions for your "problems" and ask for payment in the form of a one-time fee or subscription to a purported support service.

How to protect yourself from tech support scams:

- If you receive an unsolicited email message or phone call from a software company asking you to send personal information or click links, ignore or report the email, or hang up the phone.
- Do not share personal information, click links, or install applications when requested.
- Do not trust unsolicited calls. Do not provide any personal information.
- Download software only from official vendor websites. Be wary of downloading software from third-party sites, as some of them might have been modified to bundle support scam malware and other threats.

If you are victim of this scam:

- Consult a computer professional.
- Update or download legitimate security software and scan your computer.
- Change any passwords that you shared with someone. Change the passwords on every account that uses passwords you shared.
- If you paid for fraudulent services with a credit card, call your credit card company and ask to reverse the charges.
- Report it to the Federal Trade Commission.