Scam Alert – The Tech Support Scam

Tech support fraud involves a criminal claiming to provide customer, security, or technical support in an effort to defraud unwitting individuals. This type of fraud continues to be widespread in Santa Barbara County.

Here's How the Scam Works:

Criminals pose as a security, customer, or technical support representative offering to resolve problems such as a compromised e-mail or bank account, a virus on a computer, or to assist with a software license renewal. The victim may be contacted by telephone or on line.

Telephone: A victim receives a phone call from someone claiming that the victim's computer is infected with a virus or is sending error messages.

Pop-up message: The victim receives a pop up message on their screen claiming that a virus has been found on their computer. They are given a number to call, which is associated with a fraudulent tech support company.

Phishing e-mail warning: The victim receives a phishing e-mail warning of a possible intrusion to their computer or an e-mail warning of a fraudulent charge on their bank account or credit card. The e-mail provides a phone number to call for help.

Once the fraudulent tech support representative makes verbal contact with the victim, the scammer convinces the victim to provide remote access to the victim's computer in order to "fix" the problem. The scammer then claims to find viruses or malware, which can be removed for a fee. The criminal usually requests payment through a check, wire transfer, prepaid card, or credit card. The scammer might tell the victim if they don't pay, they won't regain access to their computer, or it will be infected with a virus.

How to Protect Yourself:

- A legitimate company will not initiate unsolicited contact; hang up on these calls.
- Resist the pressure to act quickly.
- Do not give unverified persons remote access to your computer.
- If you are suspicious of a fraudulent attempt, shut down your computer immediately.