TECH SUPPORT SCAMS

HOW THE SCAMS WORK:

Scammers often pose as representatives from legitimate companies, such as financial institutions, utility companies, or cryptocurrency exchanges. They tell you there is some sort of issue with your computer, device, or account. They try to reach you in a number of ways, including:

- Internet "pop-up" windows telling you that your computer has a virus and to call a tech support phone number which is then provided to you.

- Unsolicited phone calls or text messages claiming to be from tech support.

Scammers will often try to get you to download software from multiple websites so they can gain access to your computer. Their excuse for accessing your computer is often to get the "hacking software" off your computer.

However the scammer gets your attention, they will inform you that they can fix the issue for you - for a fee (of course) - and that you must ACT FAST. Scammers may ask you to send gift cards, wire transfer money, purchase cryptocurrency, or give cash, gold, or other precious metal to a courier. Once you grant the scammer remote access to your computer or your account, they will steal your personal information and/or money.

WHAT CAN BE DONE TO AVOID BEING VICTIMIZED?

- SLOW DOWN AND THINK!!! Scammers deliberately create a sense of URGENCY and PANIC within victims to convince them to act immediately.

- Never let someone claiming to be tech support have remote access to your computer or other devices.

- Know that legitimate companies will NEVER call you and offer tech support out of the blue. If you get a call like this, hang up! (How would a legitimate company know you need tech support anyway?!?!?!)

- Keep your virus scan software up to date on your computer to help eliminate pop-ups and malicious software from being installed on your computer.

Most scammer phone calls need YOU to GIVE them information.

- Whether it is your personal information (DOB, Address, SSN, etc…) to "verify" your identity.

- Or they will need you to give them access to your computer by downloading something.

DO NOT GIVE ANYONE ANY INFORMATION OR DOWNLOAD ANYTHING FROM ANY WEBSITE FROM SOMEONE ON THE PHONE WITH YOU!!!