A citizen recently contacted our Department to report being the victim of a scam for $18,000.

Through investigation, our Officer discovered:

The caller's home computer had been attacked by ransomware. Ransomware is malicious software (or malware) that is downloaded onto your computer by opening attachments in spam emails or through unsolicited malicious advertising. Once downloaded onto your computer, the software acts as a virus and locks the computer.

When the computer is booted up, a lock screen appears, sometimes with an official looking logo that informs the user that the computer is locked. The lock screen will typically inform the user that the computer is locked due to suspicious activity, or illegal activity despite the fact that this never occurred. The user is instructed to call a number to contact "technical support" to unlock their computer.

Calling the number for "technical support" on the lock screen will contact the software maker or owner who will ask for access to your computer. Once granted, they will unlock the computer for you, typically for a fee, and then ask you to purchase additional technical support.

In this case, a few days later, the caller was contacted by another party, most likely involved with the "technical support" line, and informed the business from which she purchased technical support was going out of business and attempting to refund her money. The caller was asked for, and provided, her bank account information so they could return the money to her account. **Instead, the user removed money from her account.**

If a lock screen appears, there is not much that can be done. Steps could include disconnecting the computer from the internet and taking it to a reputable, local, computer repair specialist. Take care to notify the computer repair company so they do not connect the computer to their network and infect other devices. The fee to unlock the computer could also be paid, this is typically a nominal fee less than $100.

The important thing to remember is NEVER provide any information over the phone, online, etc.

Here is a helpful website to check out: https://www.malwarebytes.com/ransomware/