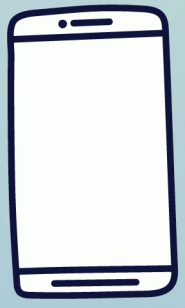
Cyber Safety and Phishing Scams



Robo calls and text messages are a common way to establish if a number is active. This is the first step in data collection to be used as potential leverage against you. They will often look like they are from an official source like a bank or social media company. If you don't recognize a phone number, don't answer it. If it is a text, don't respond to it.

If you have used social media for any length of time, you have probably received a message or an alert that looks like it takes you to your account. It then asks you to log in because you have been logged out. These are ALWAYS scams to steal your credentials. NEVER log in through a link in an email or a text. Once they have access to your account, they have access to EVERYTHING associated with your account (friends list, linked payment info and photos). Only log in though the offical app or home page.

Email scams are as old as email itself. They have evolved quite a bit over the years, but the purpose is the same. If you get an email from someone you don't know, never click a link or download a file from it. Most anti-virus software programs have built in email scanners. There are also more robust email scanners available for purchase.

For more information on phishing, go to the Federal Trade Commision's website:

https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

EMERGENCY: 911
Dispatch (non-emergency) 310-675-4444
Email: hpdweb@hawthorneca.gov