ADA COUNTY EMERGENCY MANAGEMENT & COMMUNITY RESILIENCE

EMERGENCY PREPAREDNESS POINTER

NOVEMBER 2022

CYBERSECURITY

PROTECT YOURSELF FROM CYBERATTACKS

The internet enables criminals to attempt malicious attacks to steal your information and damage your devices in multiple ways. There are several steps you can take to prevent your information and devices from being compromised. The following information is provided from the ***Cybersecurity & Infrastructure Security Agency (CISA) Public Toolkit***. Access the full toolkit here: https://www.cisa.gov/sites/default/files/publications/CAM22_PublicToolkit_FINAL_OCC_CSD_DIR_508c.pdf Public Toolkit

BEWARE OF COMMON THREATS

A **phishing attack** is a method that cybercriminals use to collect personal and financial information. Often, these attacks utilize **malware** or **ransomware**, which is malicious code in the form of a virus, worm, or Trojan Horse that can infect your devices. Be wary of emails, texts, and unsecure websites that encourage you to open links or attachments that may look legitimate, but are actually disguised cyberattacks (CISA, 2022).

Imposter scams happen when you receive an email or phone call seemingly from a government official, business representative, family member, or friend requesting that you wire them money to pay taxes or fees (FTC, n.d.). Often, these scammers will even request that you pay fees through purchasing gift cards from a store and providing them the pin and card number on the back of the gift card.

Identity theft scams can occur whether you're online or not. Don't give criminals the opportunity! They can gain access to your information and steal your identity through phishing attacks, by stealing your wallet, overhearing a phone call, looking through your trash, or picking up a receipt that contains your account number (CISA, 2022).

References

CISA (2022). Public Toolkit. Retrieved from: Link to site

Federal Trade Commission (FTC). (n.d.). Imposter Scams. Retrieved from: Link to site

WAYS TO PROTECT YOURSELF

Think Before You Click: If prompted to click a link, think before you click. If you are suspicious that a link is malicious, then trust your better judgement and don't click on it, report it!

Update Your Software: Software is constantly being evaluated and improved. When an update becomes available for your device, start the process and give your device the protection it needs. A best practice is to turn on automatic updates.

Use Strong Passwords: Use passwords that are at least 12 characters long with a variety of lowercase, uppercase, number, and special characters. Also, make sure you use unique passwords for different programs and devices.

Enable Multi-Factor Authentication (MFA): Many programs give the option to enable MFA, which provides an account with a second layer of protection against cyberattacks. MFA makes you significantly less likely to get hacked (CISA, 2022).