Ada County Emergency Management & Community Resilience

Emergency Preparedness Pointer

CYBERATTACKS - PHISHING

As cybercrimes become more common and sophisticated with the advancement of technology, we encourage everyone to learn about preventing cyberattacks and taking necessary steps to become more prepared. A common cyberattack, **Phishing**, is a cybercriminal's attempt to steal information or infect a device with malware or ransomware. They can do this by getting people to click on malicious links sent through text messages, emails, social media posts, direct messages, or even phone calls. The Cybersecurity & Infrastructure Security Agency (CISA) provides the following three steps to prepare yourself against phishing attacks.

Step 1: Recognize Phishing

Cybercriminals use many different tricks to disguise their phishing attacks, including creating fake profiles of family members, friends, and coworkers, as well as using fake branding from popular companies or organizations to make their messaging and links look legitimate. No matter the method, there tends to be some common signs within their messaging which can include:

- Language that is urgent and that wants you to take some sort of action.
- Requests for personal or financial information.
- Email addresses that mimic but do not match a legitimate web address.
- Embedded links to unsecured or untrusted websites or even links to a different destination than suggested in the text. (Unsecured or untrusted links have a URL that begins with "**http://".** Trusted and secured links will include an "s" "**https://**"). To view a links destination, hover over the link with your cursor **WITHOUT CLICKING**. The destination should pop up over the link or on the bottom left of the webpage for you to view.

Step 2: Resist and Report

Get in the habit of carefully examining each message you receive before replying or clicking on any links or attachments. If you are unsure if a message is a phishing attack or not, always err on the side of caution, report it and delete the message.

Reporting suspected phishing attacks will not only protect yourself, but will protect others who may have received the attack as well. How to report a message may vary depending on the platform you're using, but most programs will have a "**Report Spam**" feature that you can use.

Step 3: Delete the Message

After you report a suspected phishing attack, do not reply to the message or click on any links or attachments, including any link to "**Unsubscribe**" from further communications. Just simply delete it.

For more information about Phishing and more, please view the Cybersecurity & Infrastructure Security Agency's ***Secure Our World*** campaign, which provides simple ways for individuals, families, and businesses to protect themselves from cyber threats. The Secure Our World campaign can be found on their website here: https://www.cisa.gov/secure-our-world

Ada County Emergency Management & Community Resilience
Address: 7200 Barrister Drive. Boise, ID. 83704
Phone: (208) 577-4750 E-mail: gstone@adacounty.id.gov
FAX: (208) 577-4759 Website: www.adaprepare.id.gov