CYBERSECURITY AWARENESS MONTH

Phishing Tip Sheet

CITYNET

Cybercriminals like to go phishing, but you don't have to take the bait.

Phishing is when criminals use fake emails, social media posts or direct messages with the goal of luring you to click on a bad link or download a malicious attachment. If you click on a phishing link or file, you can hand over your personal information to the cybercriminals. A phishing scheme can also install malware onto your device.

No need to fear your inbox, though. Fortunately, it's easy to avoid a scam email, but only once you know what to look for. With some knowledge, you can outsmart the phishers every day.

See it so you don't click it.

The signs can be subtle, but once you recognize a phishing attempt you can avoid falling for it. Before clicking any links or downloading attachments, take a few seconds (like literally 4 seconds) and ensure the email looks legit. Here are some quick tips on how to clearly spot a phishing email:

- Does it contain an offer that's too good to be true?
- Does it include language that's urgent, alarming, or threatening?
- Is it poorly crafted writing riddled with misspellings and bad grammar?
- Is the greeting ambiguous or very generic?
- Does it include requests to send personal information?
- Does it stress an urgency to click on an unfamiliar hyperlinks or attachment?
- Is it a strange or abrupt business request?
- Does the sender's e-mail address match the company it's coming from? Look for little misspellings like pavpal.com or anazon.com.

CYBERSECURITY AWARENESS MONTH

Phishing Tip Sheet

CITYNET

Uh oh! I see a phishing email. What do I do?

Don't worry, you've already done the hard part, which is recognizing that an email is fake and part of a criminal's phishing expedition. If you're at the office and the email came to your work email address, report it to your IT manager or security officer as quickly as possible.

If the email came to your personal email address, don't do what it says. Do not click on any links – even the unsubscribe link – or reply back to the email. Just use that delete button.

Remember, DON'T CLICK ON LINKS, JUST DELETE.

You can take your protection a step further and block the sending address from your email program. Here's how to...

- Block a sender on Outlook.
- Block a sender on Gmail.
- Block a sender on Mac Mail.
- Block a sender on Yahoo! Mail

Report phishing

Some email platforms let you report phishing attempts. If you suspect an email is phishing for your information, it's best to report it quickly. If the phishing message came to your work email, let your IT department know about the situation ASAP.

Here's how to:

- Report a phish on Outlook.
- Report a phish on Gmail.
- Report a phish on Mac Mail.

You can report a phishing attempt to the Federal Trade Commission here.