PHISHING

When criminals go phishing, you don't have to take the bait.

See it so you don't click it.

Phishing is when criminals use fake emails to lure you into clicking on them and handing over your personal information or installing malware on your device. It's easy to avoid a scam email, but only once you know what to look for.

The signs can be subtle, but once you recognize a phishing attempt you can avoid falling for it. Here are some quick tips on how to clearly spot a fake phishing email:

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 Security@uccs.edu as quickly as possible.

Signs of a Phish

- Contains an offer that's too good to be true
- Language that's urgent, alarming, or threatening
- Poorly crafted writing with misspellings, and bad grammar.
- Greetings that are ambiguous or very generic
- Requests to send personal information.
- Urgency to click on an unfamiliar hyperlink or attachment
- Strange or abrupt business requests
- Sending e-mail address doesn't match the company it's coming from

Phishing Stats

The most common brands/companies impersonated are; Microsoft, Netflix, Amazon, Comcast, Chase, and Paypal.

Only 72% of people say they check messages to see if they are scams or a phish. Source: National Cybersecurity Alliance

The National Cybersecurity Alliance says that only 42% of people report phishing attempts to their email provider. Lets work together to increase this stat, report Phishing attempts to security@uccs.edu

For more information on Phishing and other Security related topics please visit https://oit.uccs.edu/security

#BeCyberSmart #CybersecurityAwarenessMonth #security@uccs.edu