How to Spot a Phish

What to do if you receive a suspicious email.

- ⊗ Do not panic.
- ⊗ Do not click or download.
- ⊗ Do not respond to the sender.
- ⊗ Do not forward to anyone else.
- ⊗ Do not share your username, password, or any personal/private information.
- ✓ Immediately mark it as SPAM or delete it.

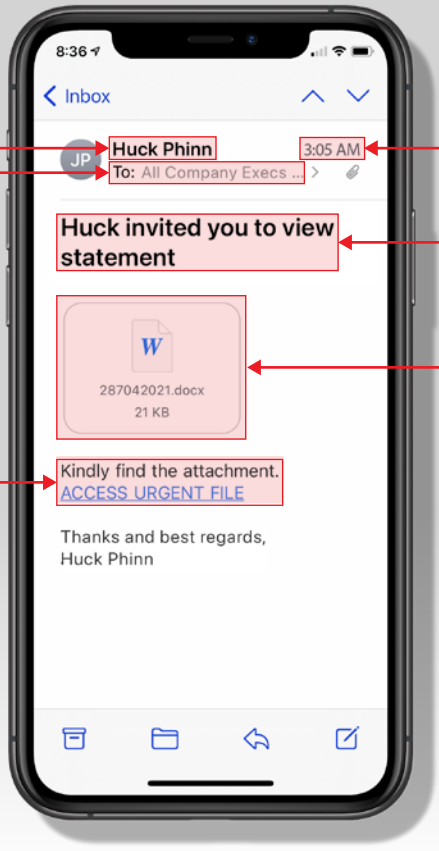
Phishing Red Flags

FROM

- The sender's email address is someone I don't regularly communicate with.
- The email was sent from someone inside the organization or from a customer, vendor, or partner and is very unusual or out of character.
- This is an unexpected or unusual email with an embedded hyperlink or attachment.

TO

- This email was sent to an unusual mix of people. For example, it may have been sent to a group of people whose last names start with the same letter, or a list of unrelated addresses.



DATE

- Was the email sent at an unusual time like 3 a.m.?

SUBJECT

- Is the subject line irrelevant or does not match the message content?
- Is the email a reply to something I never sent or requested?

ATTACHMENTS

- The sender included an email attachment that I was not expecting or that makes no sense in relation to the message.
- The attachment looks like it could be a dangerous file type.

CONTENT

- The sender asked me to click on a link or open an attachment to avoid a negative consequence or to gain something of value.
- Is the email out of the ordinary? Does it have bad grammar or spelling?
- The sender is asking me to click a link or open an attachment that seems odd or illogical.

INGALLS INFORMATION SECURITY

Cyber Innovation Center (CIC)
6300 Texas Street, Ste. 240, Bossier City, LA 71111
WWW.IINFOSEC.COM
(888) 860-0452