

# MALICIOUS EMAIL:

## WHAT YOU SHOULD KNOW

HACKERS ARE PHISHING FOR YOUR:



\* \* \* \*

Passwords



Money



Financial Info



Personal Info

## DON'T TAKE THE BAIT!

### CHECK FOR:



#### GENERIC GREETING

Phishing emails contain a generic greeting and do not contain contact information for the recipient to ask questions.



#### REQUESTS FOR PERSONAL INFO

Does the email ask you to log in and provide information such as your password or financial information? Legitimate organizations will never ask for this information through email.



#### CHECK THE EMAIL ADDRESS

Does the sender's name and organization match the email address? Emails where the sender name and organization do not match the email address are likely malicious



#### REQUESTS IMMEDIATE ACTION

Does the email make a urgent request? Such as "Click here to change your password or your account will be locked in 12 hours." Emails containing urgent requests are likely malicious.



#### WEB LINKS OR ATTACHMENTS

Does the email contain unexpected web links or attachments? These are likely to be malicious.