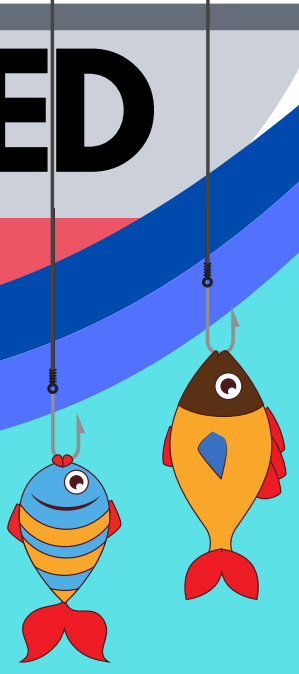
Don't get HOOKED



5 Ways to Spot a Phishing Email

Urgency and Warnings

Some scam emails convey a sense of urgency and include warnings that your accounts will be closed or your access limited if you don't reply right away.

Generic Greeting/Signature

Fradulent emails may not be personalized and are instead addressed in general terms, such as "Dear valued customer" or the email signature is not normal.

Spoofed Name

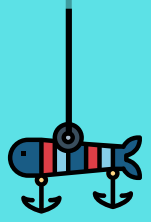
The name in the "From" field is recognizable but the reply to email address is an impostor's email address or the "From" field has the name but has a different impostor email address (i.e. main.ems@main.com)

Spelling Errors

Phishing emails can look very real with logos and website addresses that appear authentic, but there is usually some part that doesn't seem quite right: spelling mistakes, bad grammar, altered logos.

Getting Personal

Does the email ask you to disclose personal information such as your credit card number, MEFIRS password, or your mother's madien name? Maine EMS will never send you an email asking you for this information. Do not click on any links to website addresses as they may link you to fake websites that will be used to capture your personal information or that of others.



Prevent it, Report it, and Delete it! Don't take the Bait!

MAINE EMS