PHISHING

Protect yourself and your team

Anyone can be the target of a phishing scam. This information will help you know what to look out for. If you do think an email is suspicious, use **Forward as Attachment** to send it to your IT team. **Forward as Attachment** can be found by clicking "More" next to "Forward" in a fully open Outlook email window. It is important that you forward as attachment rather than simply forwarding the email, it reduces the risk of spreading an infection.

What is phishing?

The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

What do phishing emails ask me to do?

- ! Open an attachment
- ! Click on a link
- ! Send personal information
- ! Provide confidential agency information

How can I spot phishing emails?

Looks similar to a professional email but may have grammar, spelling, or formatting errors.

Message conveys a high sense of urgency.
Example: "Your account will be closed and your funds will be inaccessible unless you change your password at this link."

Emphasizes personal, confidential or potentially embarrassing information.

Attempts to get you to interact via threat or reward.

Mentions recent transaction or says you won a contest you have no knowledge of.

WHAT ARE YOU REALLY CLICKING?

Phishing emails frequently include hyperlinks that can giveaway their malicious intent. Hover your mouse over the hyperlink to see a small pop up window, this shows where the link will actually take you.

Look for suspicious addresses in the pop up that:

- ! Have multiple top level domains in the link (.gov, .com, .org, .net, etc.)
- ! Use URL encoding (http:%4B%2T%Fi)
- ! Subtle misspellings (apple.suport.com)
- ! Odd naming (microsoft.helpunlocking.com)