The School District of Osceola County, Florida
Network and Information Security Department
Every Child, Every Chance, Every Day

Document Title:	**Report Phishing and External E-Mail Banner**
Responsible Team:	Network and Information Security Department
Intended Audience:	All SDOC Employees
Written By:	Angel Fonseca
Written Date:	2020-08-04
Approved By:	Angel Fonseca
Approval Date:	2024-11-05
Revision Date:	2024-11-05

Summary:

Phishing emails are a prevalent method used by malicious actors to gain unauthorized access to online accounts, install malware on devices, or solicit unusual purchases. These threats often masquerade as legitimate or trusted senders, aiming to deceive recipients into clicking harmful links, downloading attachments, or responding to their messages.

If you encounter a suspicious email or text message requesting that you click a link or open an attachment, it is crucial to refrain from doing so. Please consider the following questions:

- **Do I have an account with the company or am I familiar with the individual who contacted me?**
- **Am I anticipating an email from this person or organization?**

To assist in identifying external communications, the School District of Osceola County has implemented a system that flags emails originating outside the district. Such emails will display a distinctive external banner at the top of the message. Below is an example of this external banner:

[EXTERNAL] - This email originates outside of The School District of Osceola County. Do not click links or open attachments unless you recognize the sender.

The School District of Osceola County encourages all users to report any suspected phishing emails to the district's email security team. This allows our staff to analyze the threat and enhance our spam filters, thereby strengthening the overall security of our community. Please follow the steps outlined below to report any suspicious emails and assist in combating fraudulent activities.

*** It is essential that you report the ORIGINAL email you received. DO NOT forward phishing emails to other individuals within the district. ***

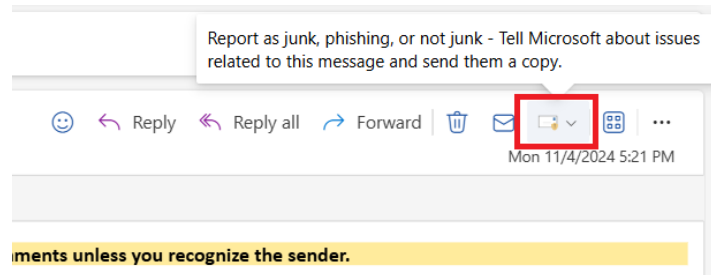Your cooperation helps protect the safety and integrity of our digital environment.
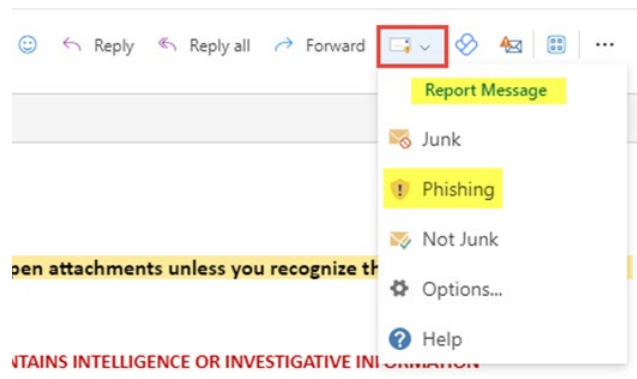
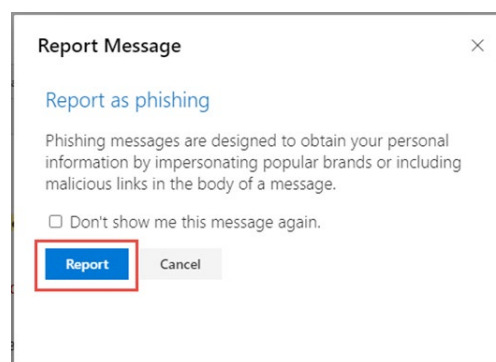## Report Phishing Emails in the Microsoft Office 365 Web Browser:

1. Click on the "**Report Message**" add-in icon located at the top-right of the suspicious email.

2. A drop-down menu will appear. Select the "**Phishing**" option to report the email as suspicious phishing.

3. Click on "**Report**" to confirm the email you are reporting.

4. You have successfully reported the message to the Network Security Team for investigation. The original email will automatically be moved to your deleted folder.

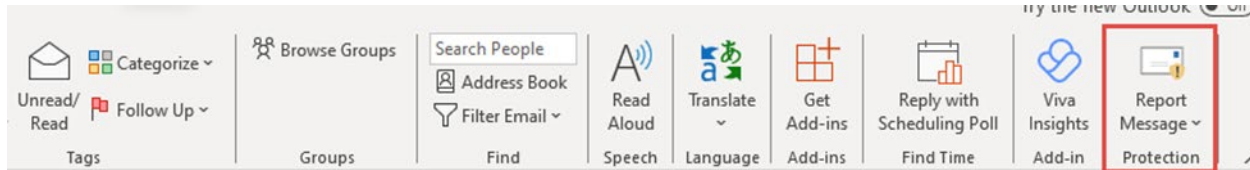Thank you for helping us maintain a secure environment!

The School District of Osceola County, Florida
Network and Information Security Department
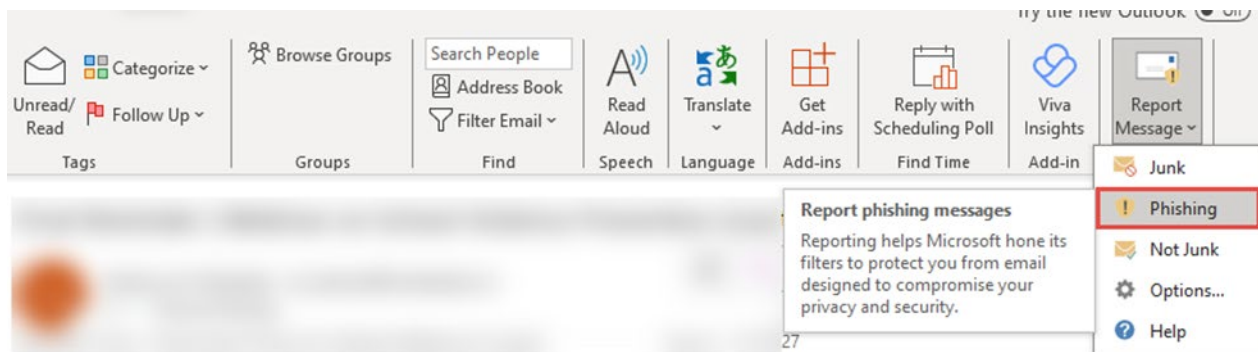*Every Child, Every Chance, Every Day*

Network
Information Security

Report Phishing Emails in the Outlook Client App:

1. Click on the "**Report Message**" add-in button located at the top-right of the suspicious email.

2. A drop-down menu will appear. Please select the "**Phishing**" option to report the email as suspicious phishing.

3. Click on "**Report**" to confirm the email you are reporting.

4. You have successfully reported the message to the Network Security Team for investigation. The original email will automatically be moved to your deleted folder.

   Thank you for helping us maintain a secure environment!