Division of Technology Services

Email Phishing Guide – How to Report Phishing Attempts in Outlook

Revision History

Effective Date	Revision #	Revision Summary
February 12, 2021	1.0	Created

Purpose

The purpose of this document is to demonstrate how to safeguard FSSA data through the proper reporting of phishing attempts via Outlook and Outlook Web App.

References

FSSA Information Security Policy
FSSA Privacy & Security Compliance Policies

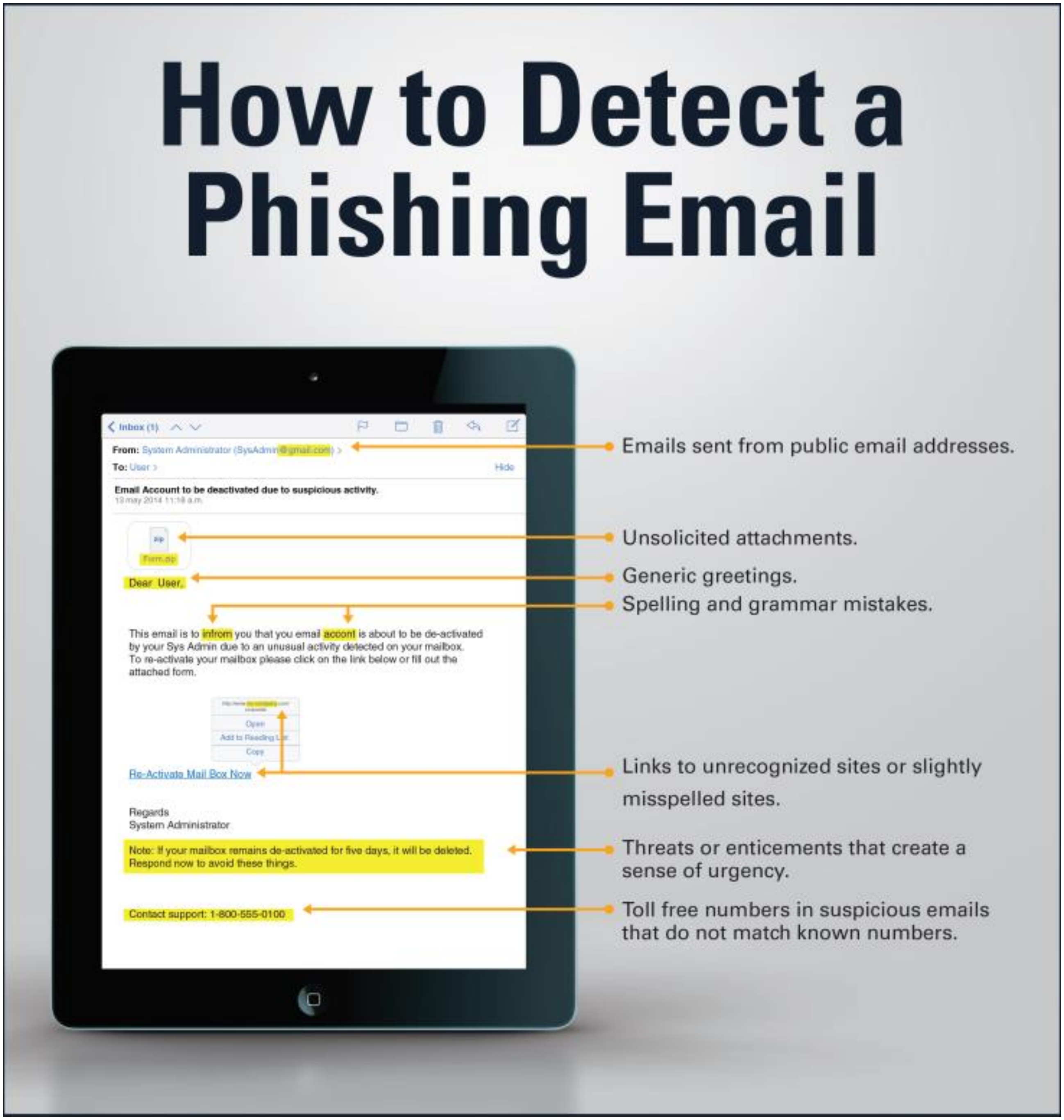
Policy Statements

Phishing is the fraudulent attempt to obtain sensitive information or data, such as usernames, passwords and personal details or other sensitive details, by impersonating oneself as a trustworthy entity in a digital communication.

The following statements should be followed when you've identified a potential phishing attempt:

1. Immediately report the email via the procedures outlined below.
2. If you believe you may have opened an attachment or clicked on a link in a phishing email, please do the following:
   - Immediately change all FSSA related passwords.
   - Do not forward the actual phishing message to any other parties unless directed to do so. Contact the FSSA Privacy & Security Office immediately by sending an email to the FSSA.PrivacyOffice@fssa.in.gov with a basic description of the incident.

Quick Guide to Identifying a Phishing E-mail



How to Detect a Phishing Email

From: System Administrator (SysAdmin@gmail.com)

To: User

Email Account to be deactivated due to suspicious activity.
13 may 2014 11:18 a.m.

Dear User,

This email is to infrom you that you email acoont is about to be de-activated by your Sys Admin due to an unusual activity detected on your mailbox. To re-activate your mailbox please click on the link below or fill out the attached form.

Re-Activate Mail Box Now

Regards
System Administrator

Note: If your mailbox remains de-activated for five days, it will be deleted. Respond now to avoid these things.

Contact support: 1-800-555-0100

Emails sent from public email addresses.

Unsolicited attachments.

Generic greetings.

Spelling and grammar mistakes.

Links to unrecognized sites or slightly misspelled sites.

Threats or enticements that create a sense of urgency.

Toll free numbers in suspicious emails that do not match known numbers.

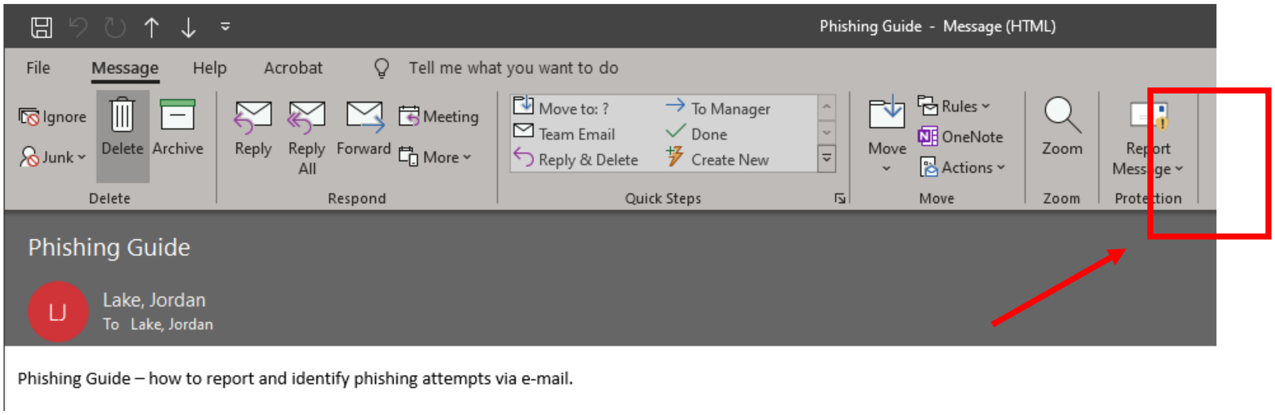
Reporting Phishing in Outlook

The Microsoft Outlook application allows users to report email phishing attempts via an add-in button that can be found in the toolbar. **Note:** If you are using the Outlook Web App (OWA), follow the steps “Reporting Phishing in OWA”.

Steps – Sharing files in OneDrive (Backup & Sync App via File Explorer)

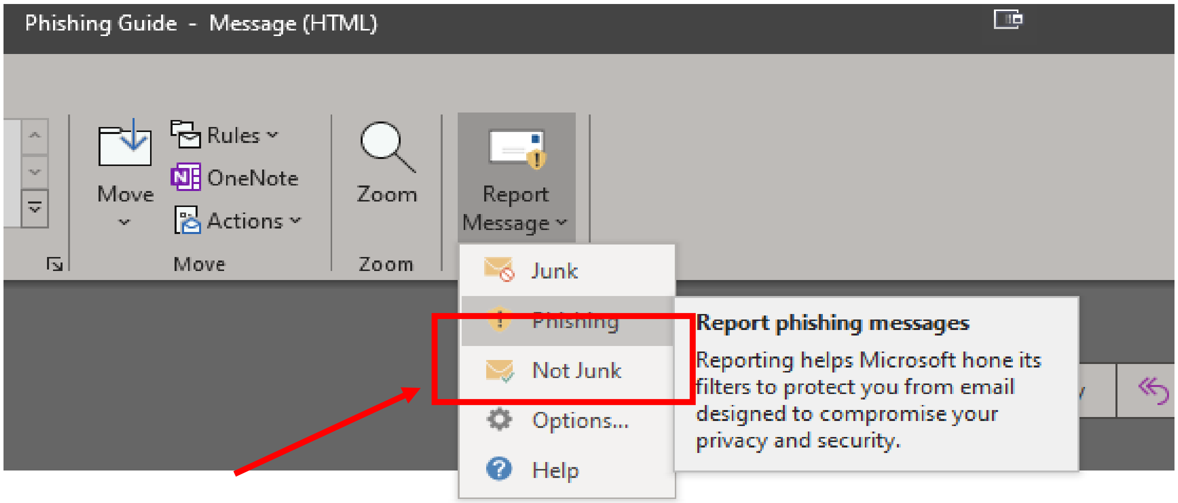
1. Once you've identified a potential email phishing attempt, select the email from your inbox.

2. Once you've selected the email in question, click on the "**Report Message**" button located in the toolbar in "**Protection**".



Phishing Guide – how to report and identify phishing attempts via e-mail.

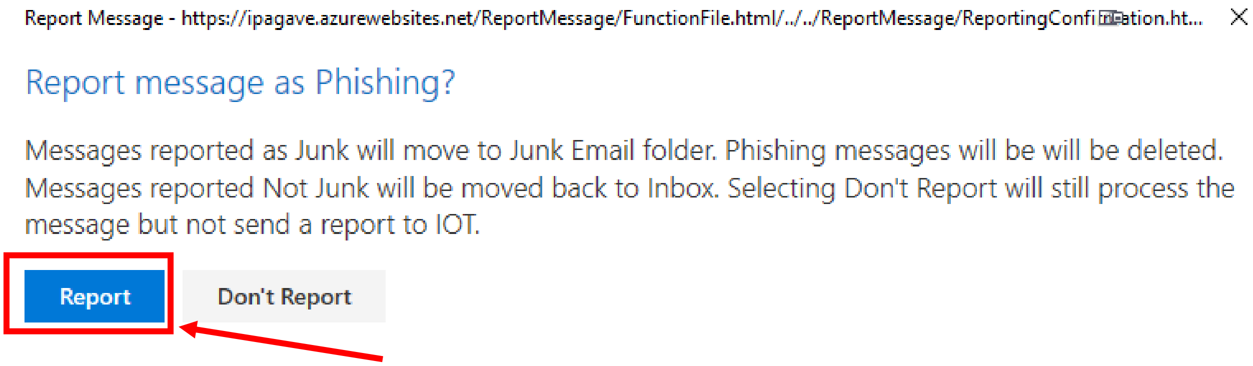
3. After selecting "**Report Message**", you will then select phishing from the prompted drop-down menu.



Report phishing messages

Reporting helps Microsoft hone its filters to protect you from email designed to protect your privacy and security.

4. A pop-up will appear where you will be prompted to confirm, click "**Report**".



Report Message - https://ipagave.azurewebsites.net/ReportMessage/FunctionFile.html/../../ReportMessage/ReportingConfirmation.ht...

Report message as Phishing?

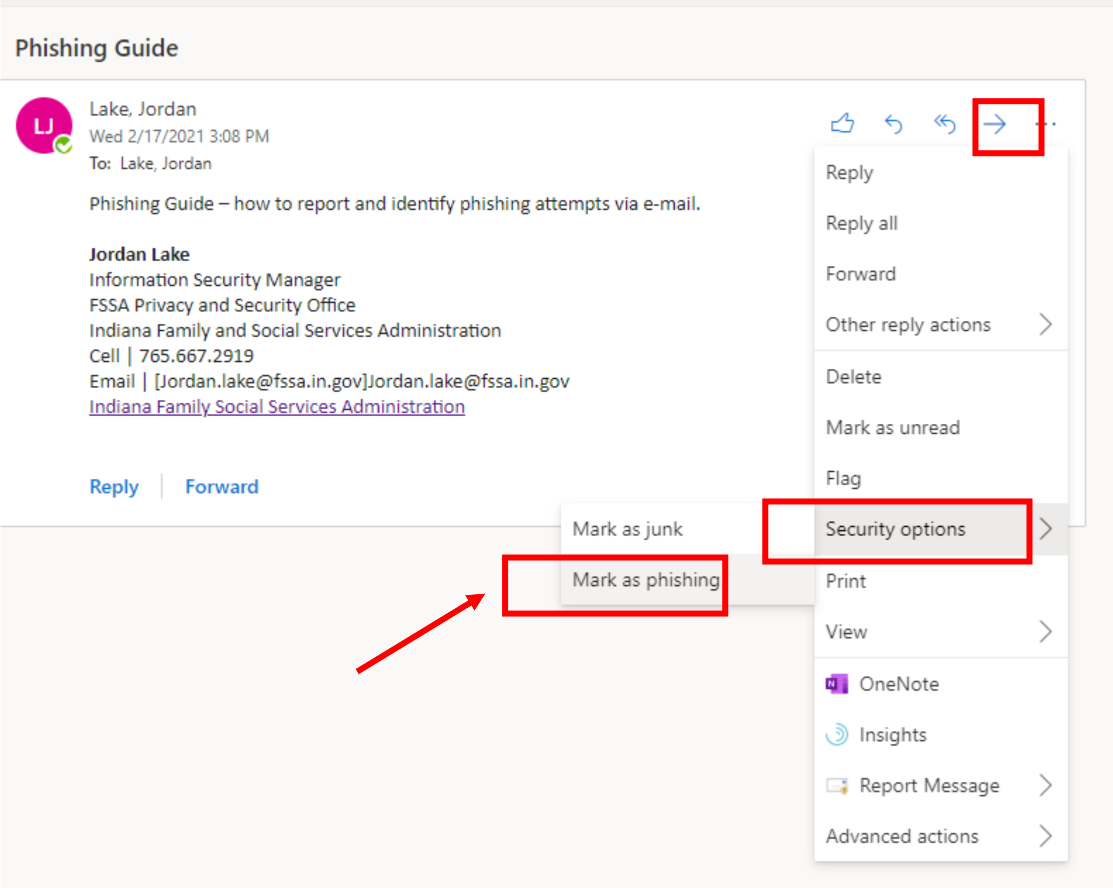
Messages reported as Junk will move to Junk Email folder. Phishing messages will be will be deleted. Messages reported Not Junk will be moved back to Inbox. Selecting Don't Report will still process the message but not send a report to IOT.

Reporting Phishing in OWA (Outlook Web App)

If you are using the Outlook Web App, you will follow these steps to report a phishing attempt email.

1. Once you've identified a potential email phishing attempt, select the email from your inbox.

2. Once you've selected the email in question, click on the 3-dot "More Actions" menu at the top right of the email, then select "**Security options**" followed by "**Mark as phishing**".



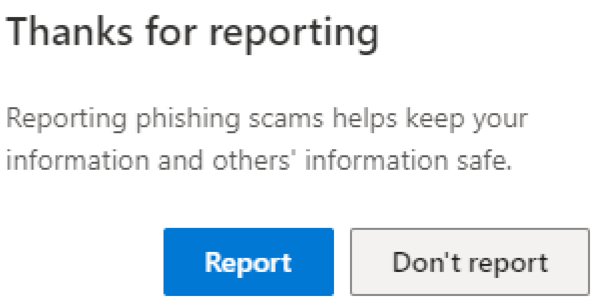
Phishing Guide

Lake, Jordan
Wed 2/17/2021 3:08 PM
To: Lake, Jordan

Phishing Guide – how to report and identify phishing attempts via e-mail.

Jordan Lake
Information Security Manager
FSSA Privacy and Security Office
Indiana Family and Social Services Administration
Cell | 765.667.2919
Email | [Jordan.lake@fssa.in.gov]Jordan.lake@fssa.in.gov
Indiana Family Social Services Administration

3. Once you click "**Mark as phishing**", you will be prompted by another window where you will select "**Report**".



Thanks for reporting

Reporting phishing scams helps keep your information and others' information safe.

Additional Support Options:

Privacy and/or Security policy questions regarding the FSSA requirements for reporting phishing attempts may be sent to the following:
H. Cliff McCullough, Director
FSSA Privacy & Security Compliance Office
(317) 232-4732
FSSA.PrivacyOffice@fssa.in.gov