



# 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

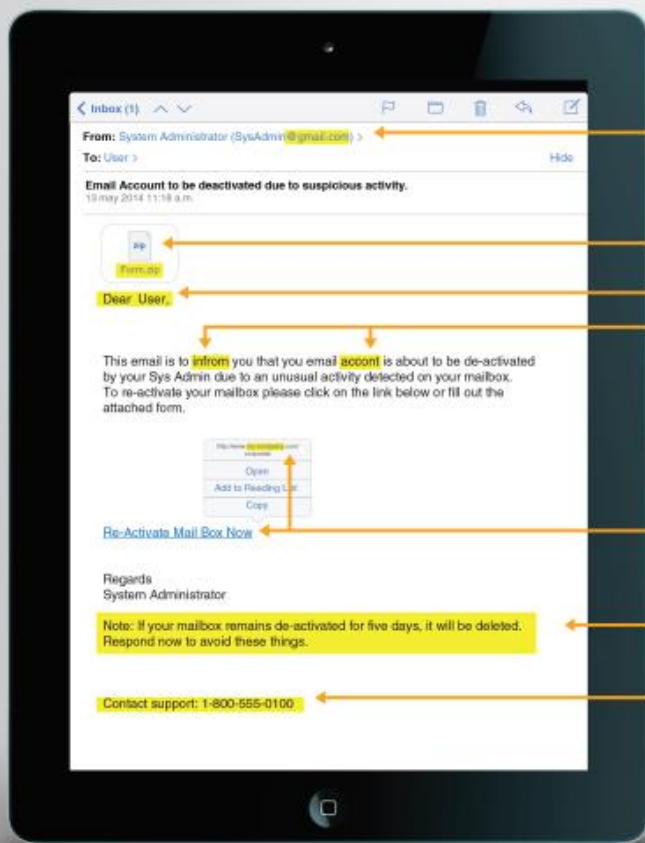
### Policy Statements

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](mailto:FSSA.PrivacyOffice@fssa.in.gov) with a basic description of the incident.

# How to Detect a Phishing Email



• Emails sent from public email addresses.

• Unsolicited attachments.

• Generic greetings.

• Spelling and grammar mistakes.

• Links to unrecognized sites or slightly misspelled sites.

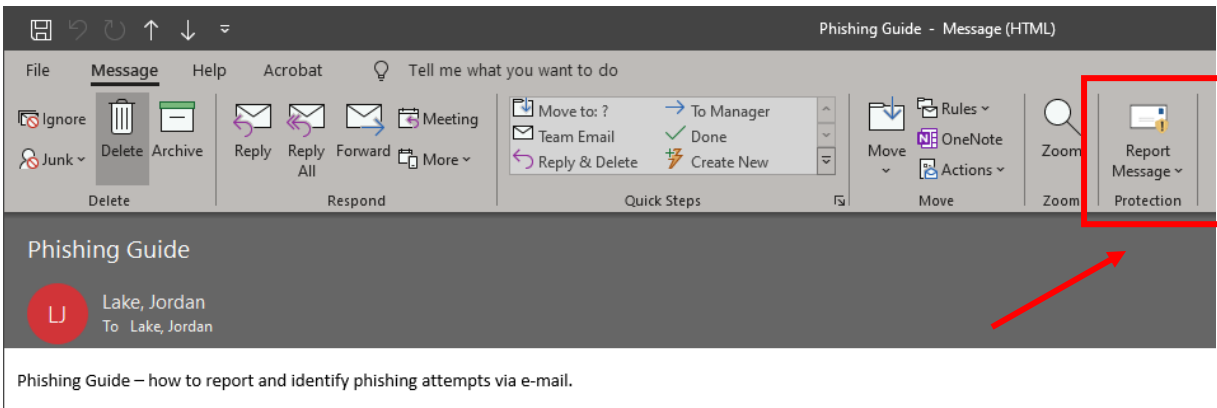
• Threats or enticements that create a sense of urgency.

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

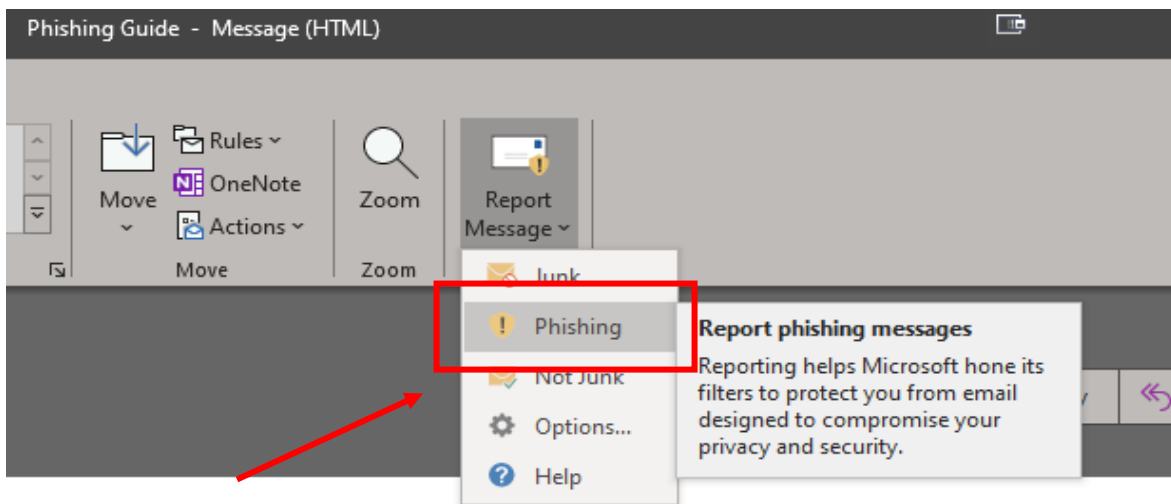
## Reporting Phishing in Outlook

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](#)".

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"**.



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



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.htm...>

### Report message as Phishing?

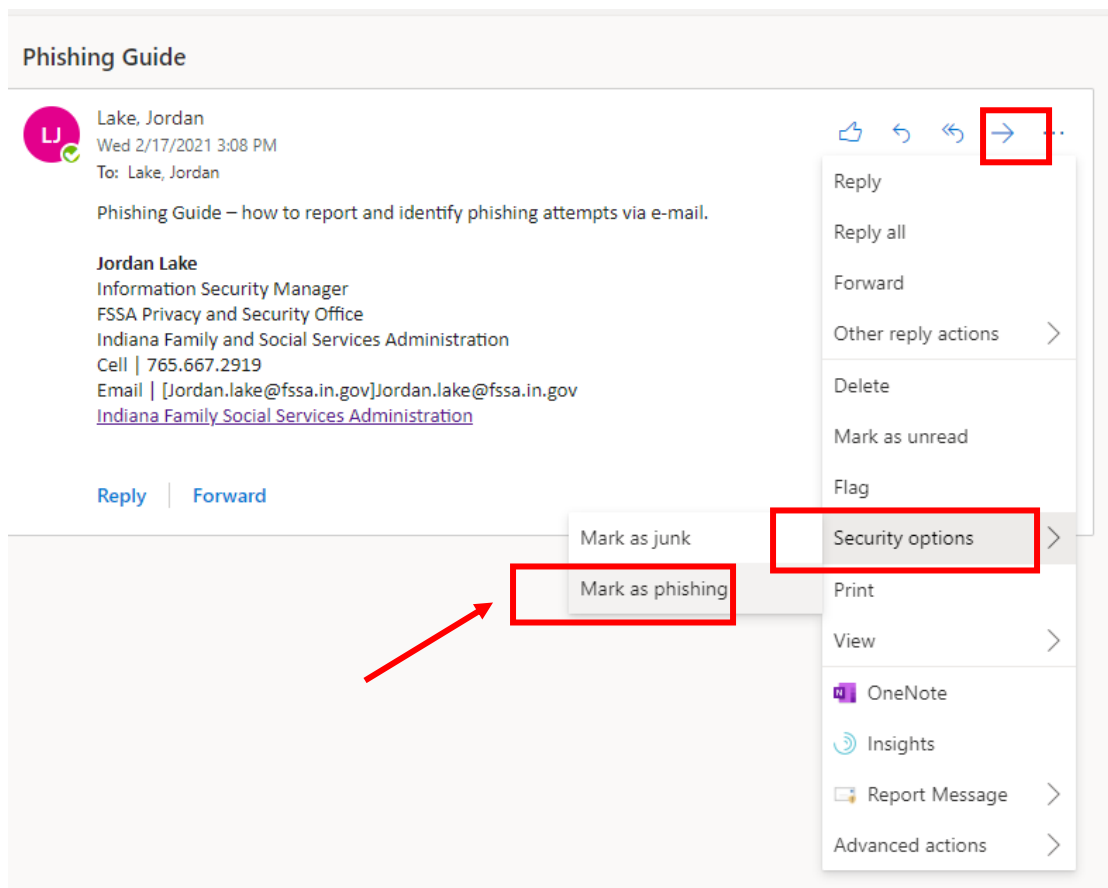
Messages reported as Junk will move to Junk Email folder. Phishing messages will be deleted. Messages reported Not Junk will be moved back to Inbox. Selecting Don't Report will still process the message but not send a report to IOT.



## 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**".



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](mailto:FSSA.PrivacyOffice@fssa.in.gov)**