Report Suspicious Email

With the increased threat of cyber attacks, the Lynn University IT Department has partnered with Microsoft Defender to help reduce our vulnerability to these threats. Please be aware no one from Lynn University will ever ask you for your password and if you are being prompted to enter your bank information, contact your Lynn University financial counselor before proceeding. Gift card scams are also quite appealing. Please do not purchase any gift cards and give the number to anyone via email request or text message. They are scamming you, and there is no recourse to recover these funds. If you receive an email for a job offer, please reach out to the Career Connections team to confirm the legitimacy of this offer before providing any personal information.

If you are on a device that does not have the "Report" button described below, please use the Outlook Web Access (OWA) information instructions to report suspicious emails.

Step-by-step guide

Outlook for Windows

Reporting suspicious emails using the Microsoft Defender Report Message Outlook plugin is a simple process that can help protect your organization from potential cyber threats. Follow these steps to report suspicious emails using the plugin:

1. Open the email that you want to report as suspicious in Outlook.
2. In the top menu bar, click on the "Report Message" button, which is located in the "Report Message" group of the "Home" tab.
3. A window will pop up asking you to confirm that you want to report the message. Click on "Yes" to continue.
4. The plugin will automatically scan the email and its attachments for potential threats. If any threats are found, you will be notified and given the option to remove them.
5. Once the scan is complete, the plugin will automatically submit the email to Microsoft for analysis.
6. You will receive a confirmation message that the email has been successfully reported.

By following these steps, you can help protect our organization from potential cyber threats by reporting suspicious emails to Microsoft for further analysis. Always be cautious when dealing with unfamiliar emails, and never open attachments or click on links from unknown sources.

Outlook for iOS

Reporting suspicious emails using the Microsoft Defender Report Message Outlook plugin in Office 365 OWA is a simple process that can help protect you and Lynn University from malicious emails. Follow these steps to report suspicious emails using the plugin:

1. Open your Outlook Mobile app on your iPhone or iPad and select the suspicious Email
2. Tap the three dots nearest the top right corner of the screen
3. Choose the “Report Junk” option
4. Choose “Phishing”
5. The email will be reported and removed from your inbox

By following these steps, you can help protect our organization from potential cyber threats by reporting suspicious emails to Microsoft for further analysis. Always be cautious when dealing with unfamiliar emails, and never open attachments or click on links from unknown sources.

Outlook Web Access

Reporting suspicious emails using the Microsoft Defender Report Message Outlook plugin in Office 365 OWA is a simple process that can help protect you and Lynn University from malicious emails. Follow these steps to report suspicious emails using the plugin:

1. Open the email in question in your Office 365 OWA inbox.
2. In the top menu bar, click on the arrow next to the "Report" button, which is located on the "Home" tab.
3. In the drop-down, select the reason you are reporting the email, "Report Phishing" or "Report Junk."
4. Select "Report Phishing" if you believe the email is trying to trick you into giving away sensitive information, such as passwords or credit card numbers.
5. The plugin will automatically scan the email and its attachments for potential threats. If any threats are found, you will be notified and given the option to remove them.

After you have reported the suspicious email, Microsoft's Defender Team will review the report and take appropriate action, such as blocking the sender or removing the email from your inbox.

Remember, it is always important to be cautious when receiving emails from unknown sources and to never click on links or download attachments from suspicious emails.

Content by label

There is no content with the specified labels