

# 2019-01-26 Action Required: Deactivation Notification

This is a phishing attempt first reported to CSULB ITS on **January 27, 2019**.

**From:** Outlook Online Team <[emailreactivationervicesdonotreply@office-notices.com](mailto:emailreactivationervicesdonotreply@office-notices.com)>  
**Sent:** Saturday, January 26, 2019 5:55:18 PM  
**To:** Patrick O'Rourke  
**Subject:** Action Required: Deactivation Notification

## Summary

The fraudulent email requests recipients to click on the link to activate their email. The link automatically opens up their email to access personal information. It is highly advised to not open the link as a precaution of any further viruses the email may contain.


## Intent of the Email

This is an attempt to acquire personal account credentials.

## Screenshots

**From:** Outlook Online Team <[emailreactivationervicesdonotreply@office-notices.com](mailto:emailreactivationervicesdonotreply@office-notices.com)>  
**Sent:** Saturday, January 26, 2019 5:55:18 PM  
**To:** Patrick O'Rourke  
**Subject:** Action Required: Deactivation Notification

---



---

## This Office 365 account will be deactivated.

---

Microsoft will disable [porourke@csulb.edu](mailto:porourke@csulb.edu) on 1/27/2019 because you've not taken the actions that were required in our previous email.

To prevent any potential service disruption use the button below and follow the prompts.

**Keep My Account Active**

Your email will no longer be deactivated once you've completed the above request.

---

Thanks for using our services!  
2019 © Microsoft. All rights reserved

Figure 1: Screenshot of the phishing email

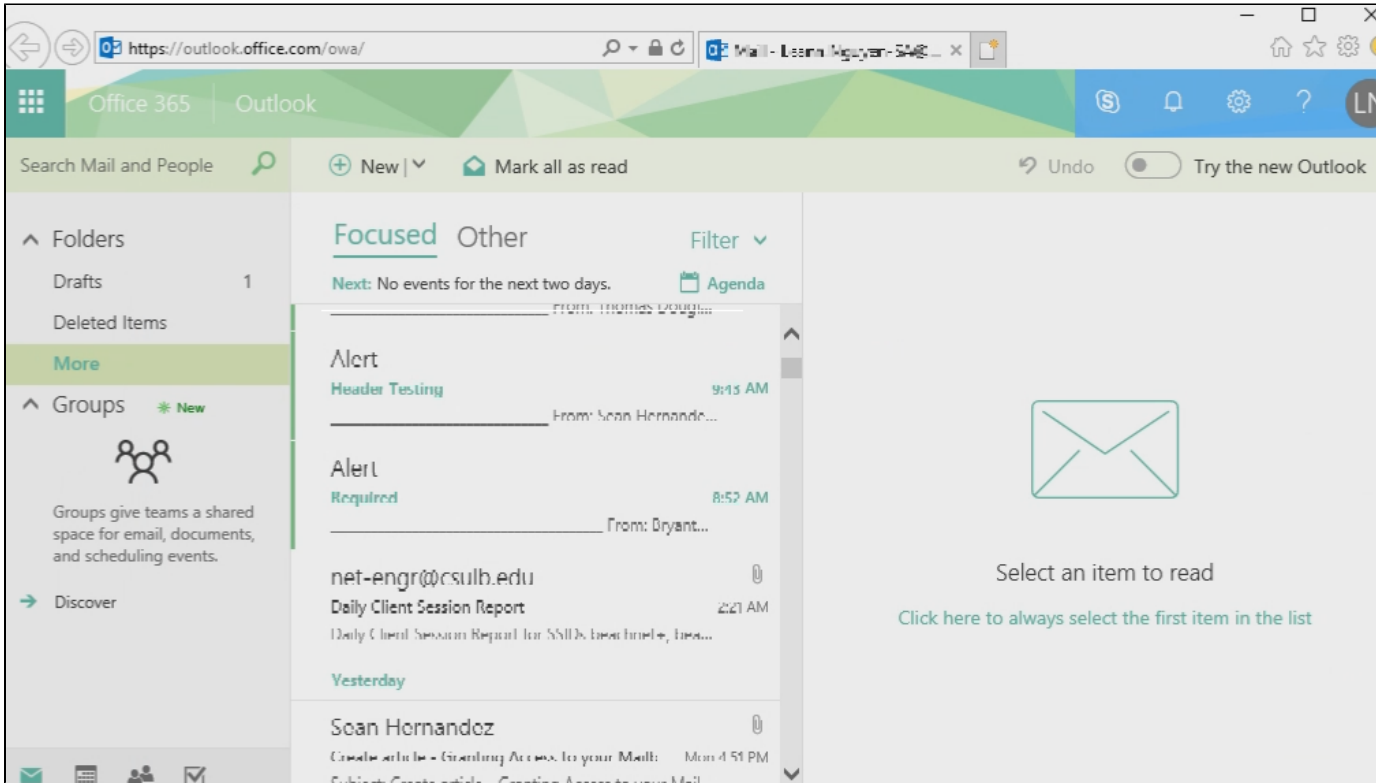


Figure 2: Screenshot of the phishing fraudulent page

View all Phishing Reports:

[All Phishing Reports](#)