

# 2018-02-09 Notice

This is a phishing attempt first reported to CSULB ITS on **February 07, 2018**.

**From:** Roberto Calderon  
**Sent:** Friday, February 9, 2018 4:54 AM  
**Subject:** Notice

## Summary

The fraudulent email claims the recipient will lose their CSULB email account unless they login and update it. This email provides a link which goes to a fraudulent page to capture password information. CSULB never asks employees to click on a link to verify or update their email account.

## Intent of the Email

The phisher/sender is attempting to capture email account credentials for their own malicious purposes.

## Screenshots

**From:** Roberto Calderon  
**Sent:** Friday, February 9, 2018 4:54 AM  
**To:** Roberto Calderon <[Roberto.Calderon@csulb.edu](mailto:Roberto.Calderon@csulb.edu)>  
**Subject:** Notice

**California State University, Long Beach (CSULB)**

Dear User,

Your account has not been updated for a long time, we strongly recommend that you [login](#) and update your account in order to avert loss of account.

[Log in.](#)

Thanks,

CSULB Maintenance Department.

Copyright © Regents of the California State University, Long Beach. All Rights Reserved.

Figure 1: Screenshot of the phishing email

View all Phishing Reports:

[All Phishing Reports](#)