

2018-03-08 Attention dgerhart@csulb.edu Update Now !

This is a phishing attempt first reported to CSULB ITS on **March 8, 2018**.

From: "Support Team" <dorene@fpc-kingwood.org>

Sent: Thursday, March 8, 2018 8:35 AM

Subject: Attention dgerhart@csulb.edu Update Now !

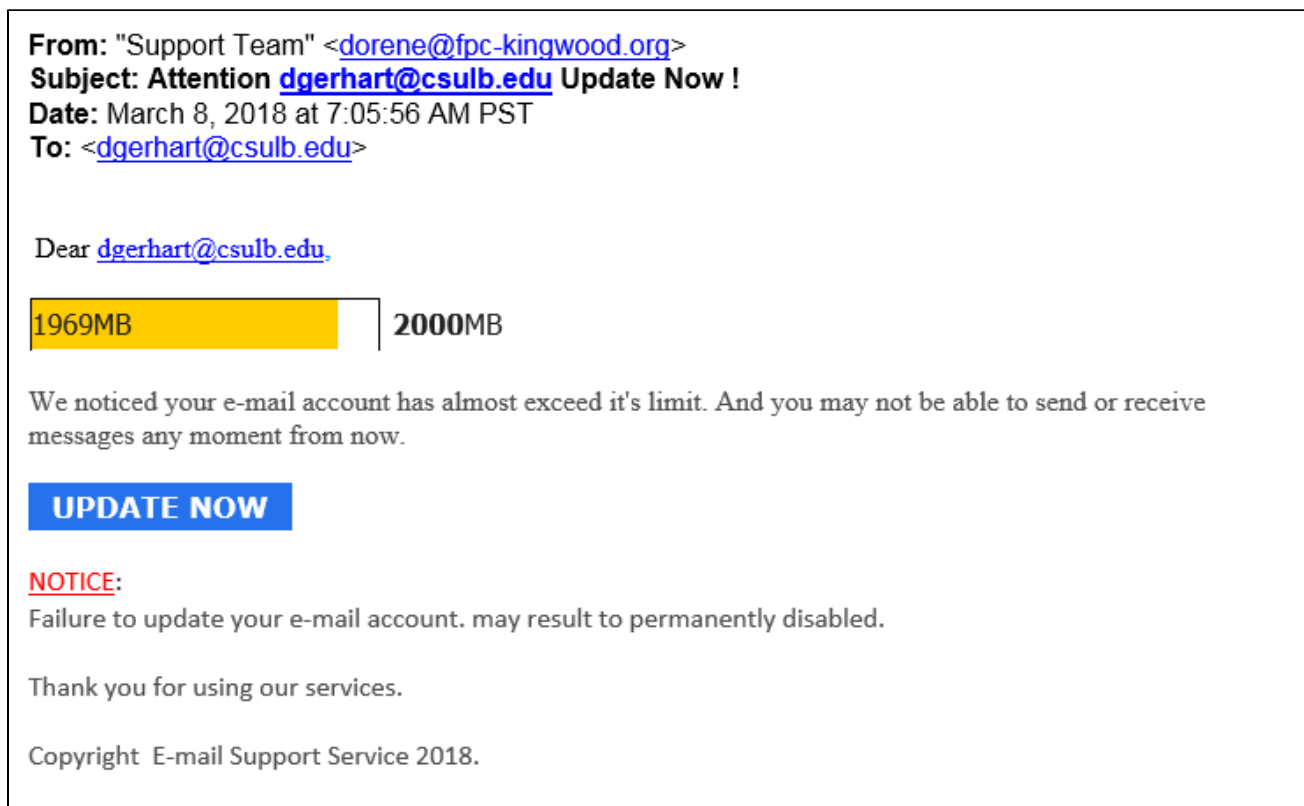
Summary

The fraudulent email is a very targeted phishing attempting that uses a variation of the recipient's CSULB email address in the subject line. It claims the recipient has almost exceeded their email quota and to click on a link to update their account before the account is disabled. CSULB never asks employees to click on links to provide information in order to avoid account closure. All employees maintain access to CSULB email accounts throughout the duration of employment.

Intent of the Email

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

Screenshots



From: "Support Team" <dorene@fpc-kingwood.org>
Subject: Attention dgerhart@csulb.edu Update Now !
Date: March 8, 2018 at 7:05:56 AM PST
To: <dgerhart@csulb.edu>

Dear dgerhart@csulb.edu,

1969MB | 2000MB

We noticed your e-mail account has almost exceed it's limit. And you may not be able to send or receive messages any moment from now.

UPDATE NOW

NOTICE:
Failure to update your e-mail account. may result to permanently disabled.

Thank you for using our services.

Copyright E-mail Support Service 2018.

Figure 1: Screenshot of the phishing email

View all Phishing Reports:

[All Phishing Reports](#)