2018-03-06 IT Desk

This is a phishing attempt first reported to CSULB ITS on **March 15, 2018**.

From: Morgan Scott <Scott.M018@student.cbsd.org>
Sent: Tuesday, March 6, 2018 9:32 AM
Subject: IT Desk

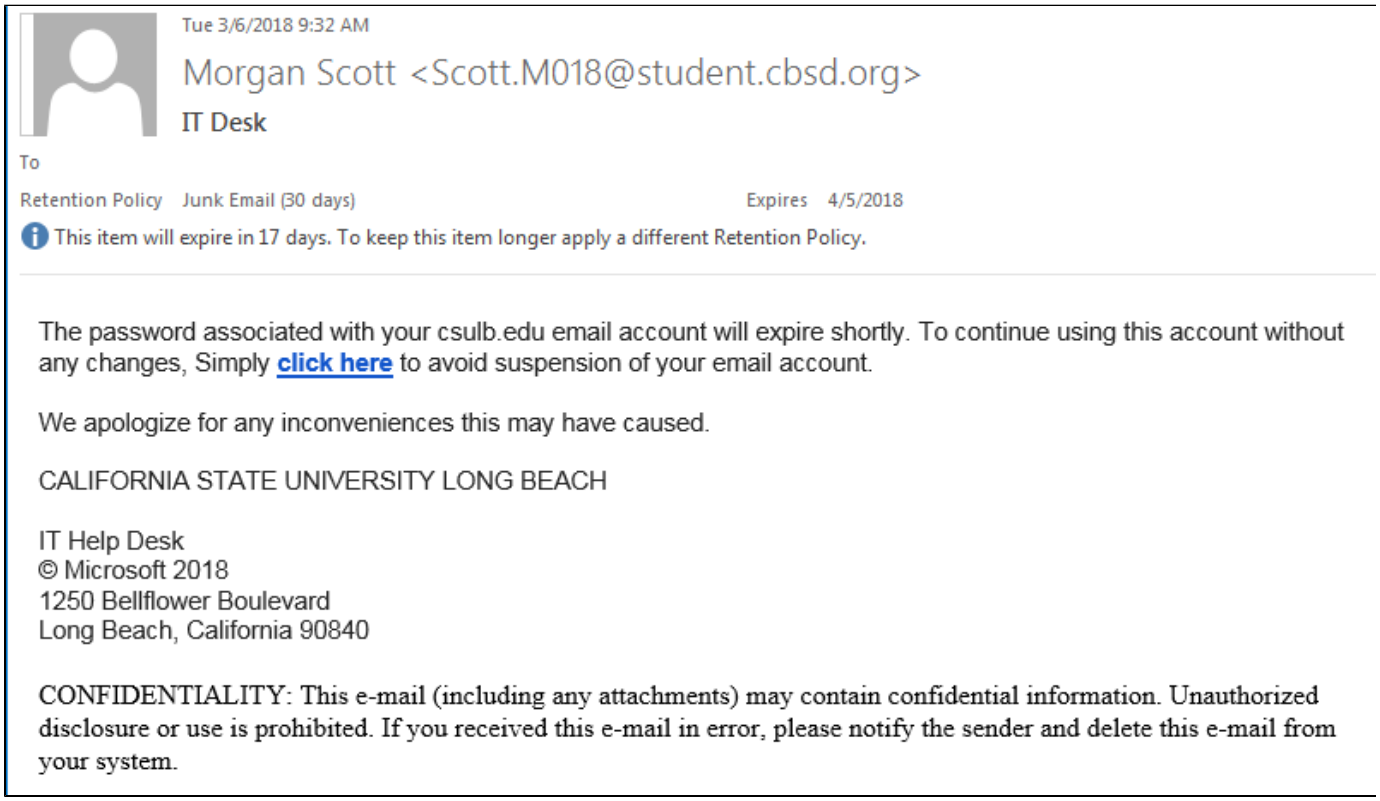
Summary

The fraudulent email claims the recipient's email password will expire and to click on the link to avoid suspension of the account. CSULB never asks employees to click on a link to avoid suspension of email accounts.

Intent of the Email

The phisher/sender is attempting to capture email account credentials for their own malicious purposes. The link goes to a page that is no longer accessible.

Screenshots



Tue 3/6/2018 9:32 AM

Morgan Scott <Scott.M018@student.cbsd.org>

IT Desk

To

Retention Policy Junk Email (30 days) Expires 4/5/2018

This item will expire in 17 days. To keep this item longer apply a different Retention Policy.

The password associated with your csulb.edu email account will expire shortly. To continue using this account without any changes, Simply **click here** to avoid suspension of your email account.

We apologize for any inconveniences this may have caused.

CALIFORNIA STATE UNIVERSITY LONG BEACH

IT Help Desk
© Microsoft 2018
1250 Bellflower Boulevard
Long Beach, California 90840

CONFIDENTIALITY: This e-mail (including any attachments) may contain confidential information. Unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.

Figure 1: Screenshot of the phishing email

View all Phishing Reports:

All Phishing Reports