

2019-02-01 Service Update on 1 February, 2019 ID: #EQ0ZAN#

This is a phishing attempt first reported to CSULB ITS on **February 01, 2019**.

From: Csulb Support-Team <fsgtew9@granmoo.com>
Sent: Friday, February 1, 2019 9:57 AM
To: Andy Fee
Subject: Service Update on 1 February, 2019 ID: #EQ0ZAN#

Summary

The fraudulent email request recipients to click on the link to update their email. The page has been taken down by web developers.

Intent of the Email

This is an attempt to acquire personal account credentials.

Screenshots

The screenshot shows an email header with the following details:

- From:** Csulb Support-Team <fsgtew9@granmoo.com>
- Sent:** Friday, February 1, 2019 9:57 AM
- To:** Andy Fee
- Subject:** Service Update on 1 February, 2019 ID: #EQ0ZAN#

The body of the email contains the following text:

HI **Andy**,

Your office-365 email is out of date, and you won't be able to send or receive new messages. We recommend you confirm your update within 12hours to avoid being deactivate.

[CONFIRM NOW](#)

Note: failure to confirm your mailbox will result to permanent disable.

Regards,
Microsoft Support

This email was sent to and***@csulb.edu.

AccID : ##6636562

Figure 1: Screenshot of the phishing email

View all Phishing Reports:

[All Phishing Reports](#)