

**IT Governance Executive Committee Meeting**

**Regular Meeting –September 2018**

**Recommendation to Activate Two-Step Authentication (DUO)**

**To Identify Risk Accounts**

**ITS Strategic Plan Alignment:** Stable and Secure Infrastructure 4.4.1- Deploy secure and mobile multi-factor authentication

**Background**

In April 2017 the IT Governance Executive Committee approved the recommendation from the ITS Team to implement two-step authentication (DUO) Multifactor Authentication to faculty and staff with access to sensitive data in PeopleSoft Student System. The project was successfully completed by March 6, 2018 securing 313 users.

In October 2017, the ITGEC approved the recommendation from the ITS Team to implement two-step authentication (DUO) MFA for Common Financial Services (CFS) users across the campus. The project was successfully completed in May 11, 2018, securing 316 additional user accounts for a total of 629 user accounts enabled with two-step authentication (DUO).

In May 17, 2017 the ITGEC approved the recommendation from the ITS Team to engage the campus community in Phishing exercises with the aim of bringing awareness and education to faculty and staff across the campus regarding the dangers of opening unsolicited and suspicious messages from known and unknown senders; 5 Phishing exercises were conducted throughout the past academic year.

**Challenges**

Despite the ongoing communication and education to Campus users regarding the risks involved with opening e-mail messages that are suspicious, a considerable number of users continue to allow their accounts to be compromised by responding to phishing e-mails. At least 96 user accounts across the campus were compromised during the recent targeted phishing attacks over the July 4th weekend.

Even though our Proofpoint e-mail protection system blocks most of the phishing attacks, users opening e-mails from the mobile devices are still vulnerable

**Alternatives**

Do nothing. Not expand MFA to other groups of employees across campus.

**Recommended Action**

Expand the Implementation of the use of two-step authentication (DUO) for the all IT Employees across Campus, and all MPP’s , and proceed to implement two-step authentication (DUO) as part of the incident response for those who compromise their accounts.

**Rationale:**

User accounts that are compromised are used as staging accounts to propagate SPAM and phishing attacks on other users on Campus, opening the Campus to further vulnerabilities, as well as millions of users across the globe. When one of our CSUSB.EDU accounts is compromised and is used as a staging account to send tens of thousands of messages outside Campus, providers such as Google, Microsoft and others start blacklisting CSUSB.EDU accounts, crippling our efforts to communicate to the outside world.

Also, when CSUSB user accounts are compromised, there is a greater possibility of their personal bank and other accounts being compromised if they use the same password for multiple accounts.

**Recommended Time line:**

a. Roll out the implementation of two-step authentication (DUO) for employees by January 2019 in phases as follows:

 i. All campus IT Staff

 ii. MPP’s

b. Ongoing: When user accounts are compromised during real phishing attacks, users will be prompted to setup two-step authentication (DUO) on their accounts as part of the incident response.

Recommended by IT Governance ISET Subcommittee: September 19, 2018