Phishing Program

**MAP for Review and Recommendation**

# Introduction

Technological advancements improve quality of life through easier access to information, better customer service, and greater convenience. However, the darker side uses this to exploit technical vulnerabilities and human frailties. Enhanced technologies, like antivirus, spam filters and intrusion detection systems, address some issues. Human susceptibilities are strengthened by information security awareness and phishing programs. Of these, the most difficult to improve is human nature. Phishing and spear-phishing take advantage mankind’s helpful nature to spread malware like ransomware, and steal information like passwords and identities. The increasing sophistication and frequency of these attacks are a chief concern of IT security professionals.

# Details

CSUSB’s Phishing Program will use ethical phishing to help end users learn about the dangers of phishing attacks. Using email, the most common delivery method of phishing attacks, the campus community will receive a message similar to a real phishing email. Those who clicking on email message link will receive an educational message on the dangers of phishing and how the end user can recognize the email as phishing. The program is not punitive and individual results will not be shared. Those identifying phishing emails before clicking can forward those messages to abuse@csusb.edu. Positive reinforcement, like recognition or rewards, can encourage participation and improve retention. Exercises will be easy in the beginning and increase in difficulty over time. Initially, faculty and staff will be targeted.

# Challenges(s)

* People use business equipment for personal activities creating potential risks
* Even application of training – large number of people, busy faculty & staff
* Single sign-on (SSO) enables access to multiple systems if one person is compromised
* People are recognized as being the weakest link in information security

# Alternatives

* Continue current practices of user education and awareness training
* Roll out a Phishing exercise and training program to educate and train faculty and staff to prevent phishing attacks.

# Impact(s) if we do nothing

* Increased risk of compromised systems leading to exposing student or personnel records.
* Possibility of successful ransomware attack leading to data loss, system loss and university shut down.

# Recommendation

1. Use Chancellor Office PhishMe to facilitate phishing program – free to campus, ease of use, excellent support and many options to improve and increase exercise difficulty
2. Conduct several phishing exercises each year – improves retention, indoctrinates newcomers
3. Increase difficulty annually
4. Add students to the list of exercise participants

# Budget Considerations

None – PhishMe is provided by the Office of the Chancellor

# Assessment

Program is not punitive. Results are shared as a summary while individual results not.

## KPIs

Provide a minimum of two(2) key performance indicators (KPI) will best indicate project success:

1. Increased reporting of phishing attempts to abuse@csusb.edu
2. Fewer people clicking on links in phishing emails
3. Lower risk insurance due to increased vigilance by campus community.

## Estimated Timeline

Start Date: February 2017

Completion Date: 2020

## Departmental Resource Allocation

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| [ ] ACBI | [ ] ATI | [ ] DDTS | [ ] ECS | [x] ISET  | [ ] TNS | [ ] PMO | [ ] Web |

# Approval

[ ]  This project will require IT Governance review during the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ monthly meeting.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Submitting MPP Submittal Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Approving MPP Approval Date