October 2017 Phishing Exercise

# EXERCISE FACTS

* October 24, 2017 at 8:35am exercise was activated scheduled to end on October 29, 2017
* 2203 faculty & staff were sent the phishing exercise. No emails bounced.
* Complication: Email and ISET Ops technical teams reacted to phishing exercise email by removing it from Outlook. This took place around 9am on October 24, 2017.  Affected were: 2,195 items removed, read or unread.
* Abuse@csusb.edu received 49 reports on the exercise.
* First click:
	+ 8:35am apple mail browser[[1]](#endnote-1)[[2]](#footnote-1)
	+ Organization (ISP): CSUSB1
* Last click:
	+ Within exercise 5 day time frame: 10/28/17 12:13 PM
	+ After exercise 5 day time frame: 11/7/2017 11:45 PM
* 86 users clicked the link.
* 353 opened the email only. (“Opened email” includes those who preview the email.

# GRAPHS

## Response in first 8 hours



Even though the Office 365 Team scrubbed the exercise email shortly after release of the phishing exercise there were still almost 75 responses in the first hour.

## Location of those clicking link



Phishing still occurs everywhere.

## Time spent on Education



Educational video is only 1:01 (61 seconds) long

Many people didn’t pay attention to the educational video.

## Browser used to click link



Mobile devices are still most popular browser used to view email. This enables easy clicking of the link but obscures full disclosure of the clicked link being because of the small format of mobile devices.

## Application used to open Email

This chart groups the applications used to open email and shows the number of emails opened.

In total 23 different email viewers were used.

Response Breakdown

* 16.02% of 2203 recipients opened the email equating to 353 recipients.
* 3.9% of 2203 recipients clicked on the email which equals 86 people.

## Unit Participation

Only one unit had zero recipients who opened the phishing exercise email.

# EXERCISE SUMMARY

People accessing campus resources from on and off campus show the exposes the campus to risk.

Regarding the complication: ISET will email office365team@csusb.edu & iset-ops@csusb.edu teams before conducting phishing exercise. A copy of the phishing exercise along with the date and time a phishing exercise will occur will be sent along with instructions to keep the information confidential so to not impact exercise results.

From: DefendID <defendid@csusb.edu>

Date: Tue, Oct 24, 2017 at 8:35 AM

Subject: CSUSB Secure Your Identity

To: Joe Coyote <joe.coyote@csusb.edu>

DefendID®

Image

CSUSB Employee, Secure Your Identity

As you have no doubt been made aware, various CSUSB personnel may have been affected by a cybersecurity incident exposing personally identifiable information of several thousands of individuals.

CSUSB has reached an agreement with defendID® to provide its employees with industry-leading identity protection services at no cost to you. If your information is in the wrong hands, you must act now to protect your identity; follow the link below for more information.

Image

Are you affected?

Find Out

✓ This message and included attachment(s) has been verified as secure. Learn More »

1. PhishMe Scenario 6 – 2017-10-24 – Click-only – Activity Timeline.csv [↑](#endnote-ref-1)
2. PhishMe Scenario 6 – 2017-10-24 – Click-only – Activity Timeline.csv [↑](#footnote-ref-1)