January 2018 Phishing Exercise

# EXERCISE FACTS

* January 30, 2018 at 7:45 AM PST exercise was activated then ended on Sunday, February 4, 2018.
* 2121 faculty, MPP and staff were sent the phishing exercise. No emails bounced.
* [Abuse@csusb.edu](mailto:Abuse@csusb.edu) received 28 reports on the exercise.
* First click: 1/30/2018 7:46, ISP: CSUSB, browser: iPhone
* Last click: 2/3/2018 14:52, ISP: Frontier Communications, browser: Mozilla FF ,
* 89 users clicked the link.
* 135 opened the email only. (“Opened email” includes those who previewed the email.)

## COMPARATIVE RESULTS

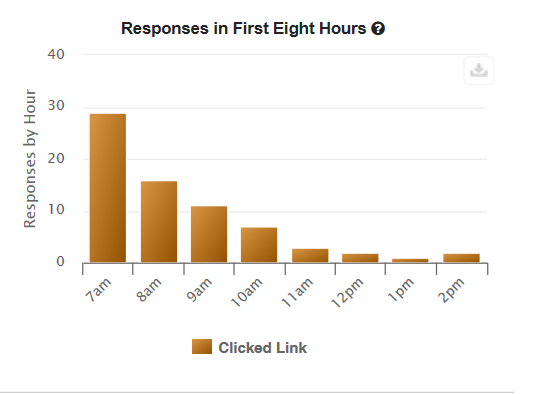
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **EXERCISES** | **OCTOBER, 2017** | | **JANUARY, 2018** | |
| PARTICIPANTS | 2203 | | 2121 | |
| OPENED EMAIL | 353 | 16.024% | 135 | 6.36% |
| CLICKED LINK | 86 | 4.698% | 89 | 4.196% |
| REPORTED TO ABUSE.CSUSB.EDU | 40 |  | 28 |  |

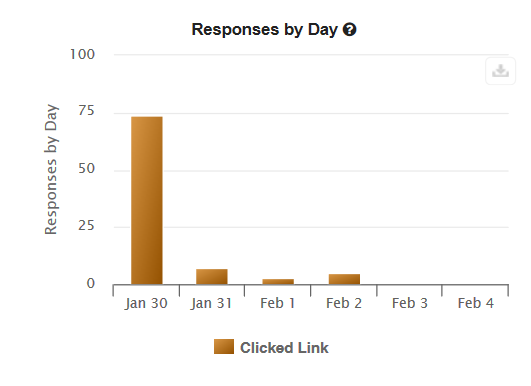
## ANALYSIS OF COMPARATIVE RESULTS

* *Fewer people opened/previewed the email & fewer people reported to abuse.* People too busy to open or report. Question: was exercise conducted too close to classes starting?
* *More people clicked link than last time.* The more susceptible people are making the same mistakes. Education/awareness is not reaching these people. Question: how to make awareness more effective.

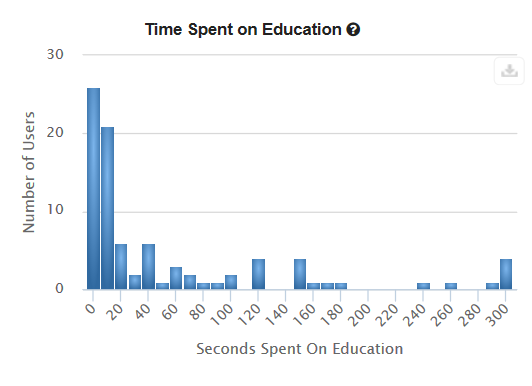
# CLICK RATE ANALYSIS

 PhishMe provided a susceptibility rate on chosen exercise is 16.34%. Compared to CSUSB’s rate – CSUSB Faculty, Staff and Managers are not that susceptible.



Response in First Eight Hours & Responses by Day - Typical exercise progression.

# EDUCATION ANALYSIS

Time Spent on Education – Education launched when someone clicked on the link in the phishing email was one page long document explaining the situation, the potential consequences, and listing how the phishing email could have been identified as a phishing attack. 20 seconds might be long enough for someone to peruse the educational document but it is more realistic that 60 – 180 seconds more appropriate time spent on the education. This means 20 people (22.4% of people clicking the link) actually spent adequate time reviewing the education.

# WEB BROWSER ANALYSIS

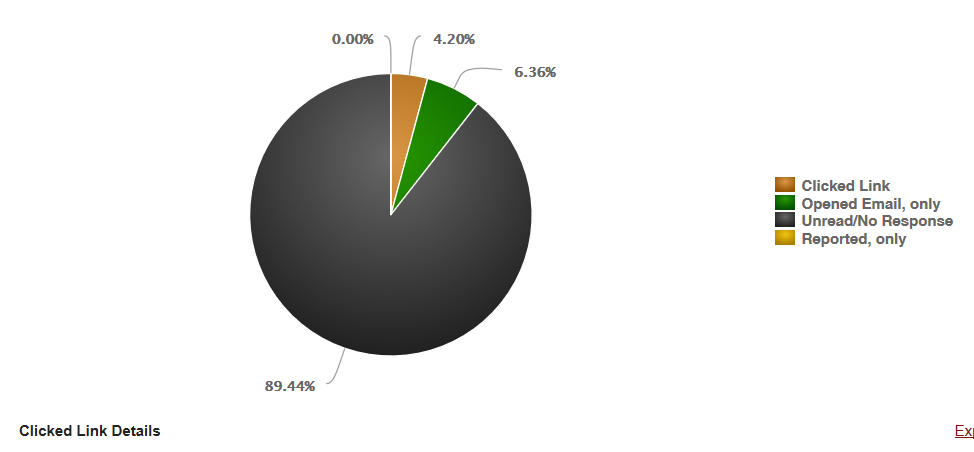
Mobile users account for 62.7% of all opened email.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| BROWSER | Opened Email Tracking | Clicked Link | Total Responses | Percentage |
| Android | 12 | 12 | 24 | 8.39 |
| Apple | 97 | 24 | 121 | 42.31 |
| Chrome | 10 | 27 | 37 | 12.94 |
| Firefox | 3 | 10 | 13 | 4.55 |
| IE | 5 | 8 | 13 | 4.55 |
| Outlook | 20 | 0 | 20 | 7 |
| Safari | 5 | 6 | 11 | 3.85 |
| Thunderbird | 1 | 0 | 1 | 0.35 |
| Unknown | 44 | 2 | 46 | 16.08 |
|  | 197 | 89 | 286 | 100.02 |

## GEOGRAPHICAL MAP OF CLICKED LINK

Geographical map of where phishing email was opened.

Lesson: access can occur anywhere.

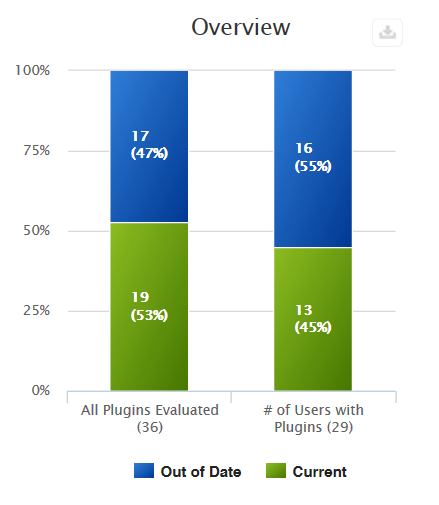


## CLICKED LINK DETAILS - PIE CHART

Unread/No Response = 89.44% of all recipients

Opened Email only = 6.36% of all recipients

Clicked link = 4.2% of all recipients

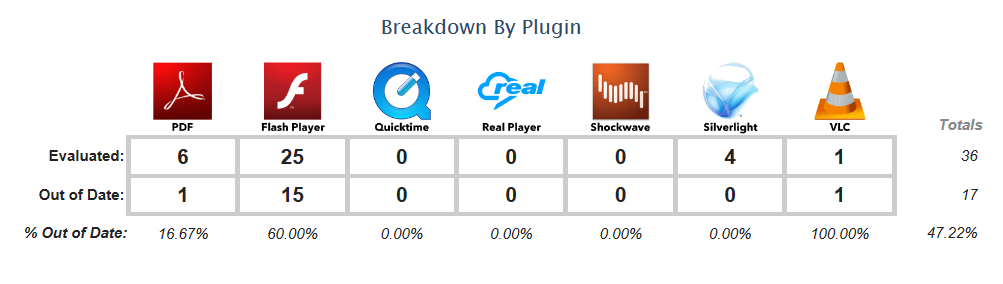


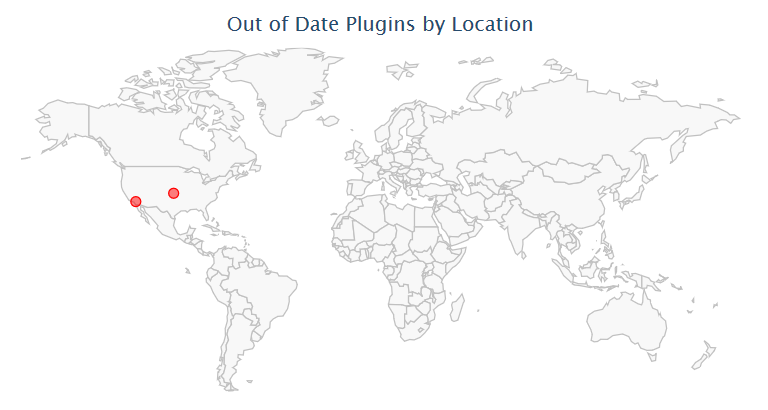
## CLICKED LINK OVERVIEW

Out of the 89 people clicking on the link 16 people had out of date plug-ins. Of those, 17 plug-ins were out of date.

Of the 17 out of date plug-ins 15 were Adobe Flash Player. This plug-in is enhances audio/video viewing but is a medium to high risk for Windows, Macintosh, and Linux machines, and Google Chrome, Microsoft Edge and Internet Explorer browsers. This vulnerability allows for remote code execution.[[1]](#footnote-1)

## MOST VULNERABLE BROWSER PLUG-INS

Adobe Flash accounted for 88% of the vulnerable plug-ins found for those clicking the link.



Out of date plug-ins can affect the campus from anywhere.

# CSUSB COLLEGE AND DIVISION PARTICIPATION & RESPONSE

Analysis: Only PDC has no one clicking the phishing link.

1. CIS Center for Internet Security. Multiple Vulnerabilities in Adobe Flash Player Could Allow for Remote Code Execution (APSB17-33). 14 Feb 2018. https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-adobe-flash-player-could-allow-for-remote-code-execution-apsb17-33\_2017-112/ [↑](#footnote-ref-1)