**Phishing Exercise**

**Pilot Project**

**Scope**

On April 26, 2017 CSUSB conducted a phishing exercise to establish a baseline response to a phishing simulation. 100 faculty, staff & student assistant campus email accounts received a “phishing” email announcing they failed to appear for jury duty with instructions to open the attachment for additional details. When the attachment was opened a message displayed that the situation was an authorized phishing simulation. In addition, more information was provided on how to avoid falling prey to phishing situations in the future.

**Results**

All 100 emails were successfully delivered. 45 recipients opened the email and 13 recipients opened the attachment, which contained a lesson on “phishing”. The lesson is included in the Appendix. Opening a phishing email potentially enables malware to be downloaded through pictures embedded in the email. 

Outlook’s “preview” mode is considered “opening” an email. However, there’s a setting where Outlook’s preview mode can prevent auto downloading of embedded images thereby reducing the threat. Opening or previewing a phishing email is less risky than those who actually open attachments or click links in phishing email.

**Ancillary information**

Phishing exercises provide insight into other important activities – like how the campus responds to phishing attacks. How support services respond is just as important. In this instance 4 people forwarded the suspected email to abuse@csusb.edu, ISET’s mechanism for collecting and responding to such attacks.

* IT personnel supporting email forwarded the offending email to vendor to update the campus spam filter.
* Technology Support Services Help Desk received one walk-in.

**Summary**

The susceptibility rate for this phishing attack scenario as reported by the vendor is 10.25% while in our institution is 13.0%. That is, we have a higher risk for phishing as compared to other populations who have used this phishing scenario.

Future exercises are planned to lower number of people who open the attachment.

In closing, phishing emails are an easy way to deliver a multitude of threats:

* Spear phishing – a targeted attack using accurate information to give validity to the phishing email ploy.
* Whale phishing – where the target provides a huge payload either in the form of money or information
* Ransomware – spread through attachments or clicked links holds for ransom either the machine or any information it touches.
* General malware – some secretly collect usernames and passwords, while others steal information of contacts to spread spam, others run silently in the background utilizing the computer to share illegal downloads, pornography and more.

Phishing statistics[[1]](#footnote-1) to be concerned about include:

* Phishing email is #1 delivery vehicle for malware including ransomware.
* 9 out of 10 phishing emails carry ransomware as of March 2016
* More sophisticated and targeted (spear phishing) attacks have risen by 22%.
* National average shows 30% of opened phishing emails get clicked.

Consistent application of phishing exercises should reduce the number of potential victims and help reduce the campus risk exposure.

Prepared by: Michelle Behne

Appendix: Attachment for phishing email exercise

APPENDIX

|  |  |
| --- | --- |
|

|  |
| --- |
|  |

 |

1. Jonathan Crowe. Barkly. <https://blog.barkly.com/phishing-statistics-2016> 8.May.2017 [↑](#footnote-ref-1)