CERIAS

The Center for Education and Research in Information Assurance and Security

Phishing Susceptibility: An Investigation Into Human Information Processing of Spear-Phishing

Aiping Xiong[1], Huangyi Ge[2], Jeremiah Blocki[2], Ninghui Li[2] , Robert W. Proctor[1]
[1]Department of Psychological Sciences, [2] Department of Computer Science

Background

Phishing

- Unique campaign increased 29% in Q3 2017 compared to Q3 2016 (APWG, 2018)
- 91% spear phishing in enterprise and organization (GreatHorn, 2017)

Phishing Emails Detection and Prevention

- Microsoft office 365 missed about 9.3% emails containing spam, phishing, and malware (Cyren, 2017)
- Purdue Cisco quarantine
  - filtered most false positives
  - 27 false negatives (spear-phishing emails) received in my Purdue inbox since 07/2017

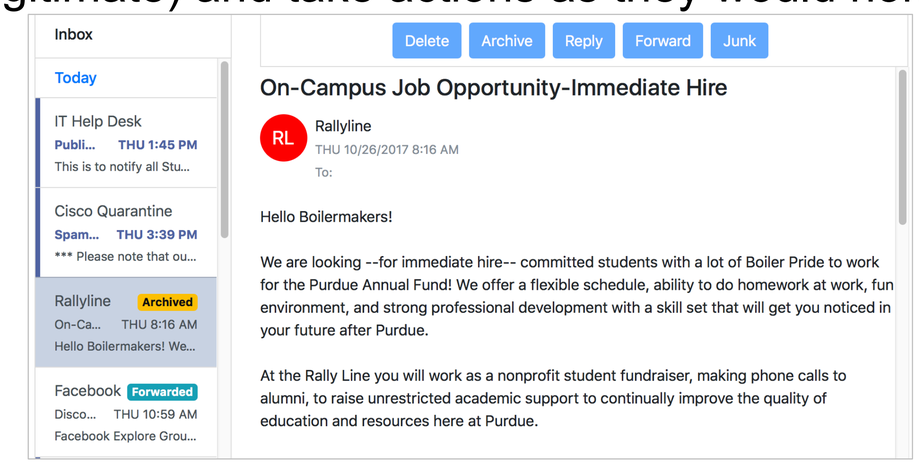
Research Questions:

1. How do Purdue undergraduates process spear-phishing emails and determine whether to respond to them?
2. How does a Cisco quarantine email influence their subsequent decisions?

Online Study

- **Email Management**

Instructed to read 10 emails (2 spear-phishing, 8 legitimate) and take actions as they would normally do

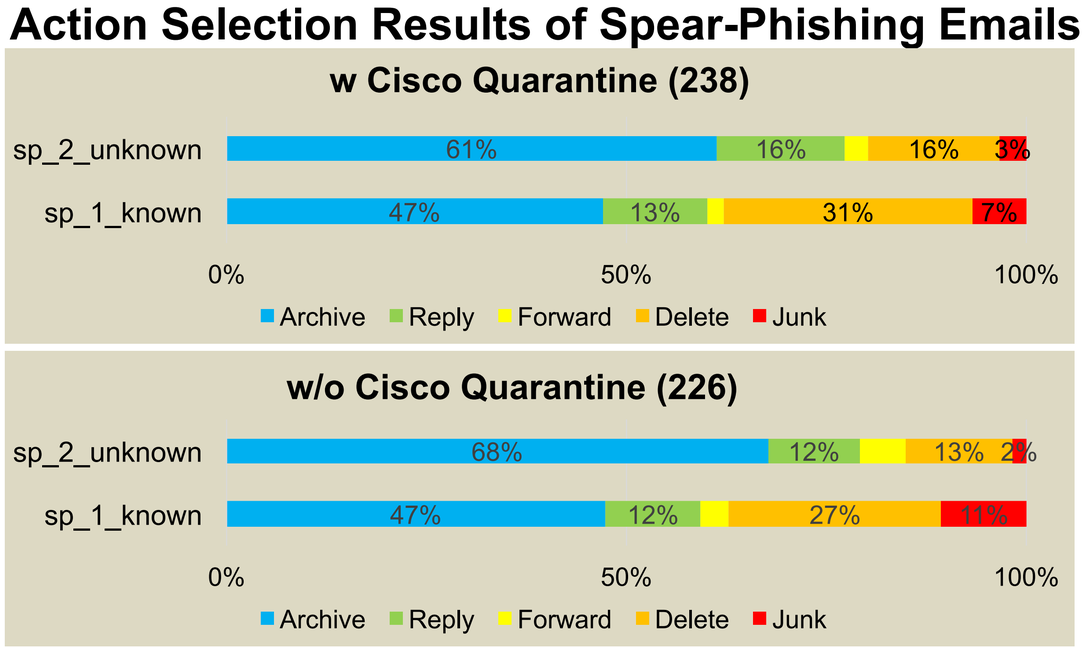


- **2 × 2 Mixed Design**

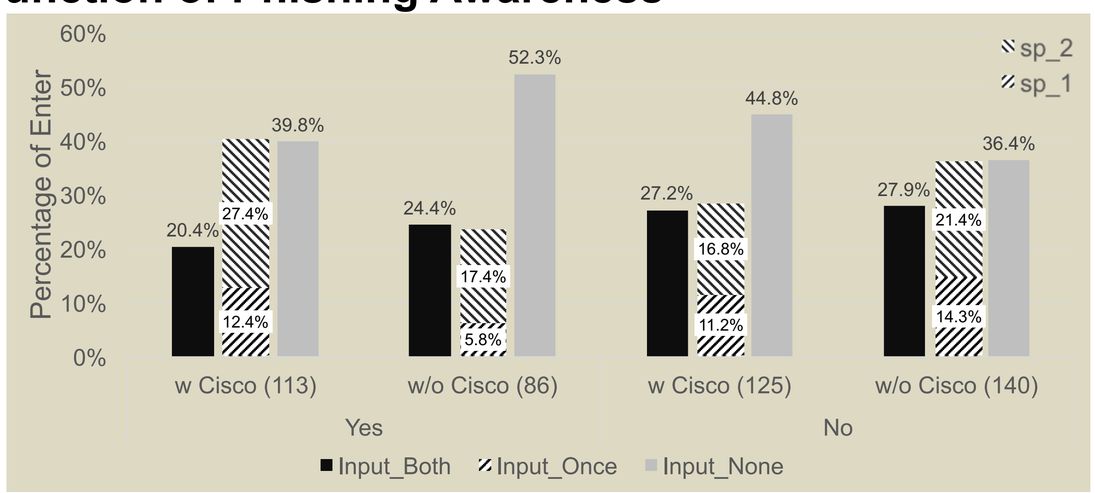
Spear-Phishing Emails (within-subject)	Cisco Quarantine (between-subject): Yes (238)	Cisco Quarantine (between-subject): No (226)
	Known & Unknown	Known & Unknown

Results

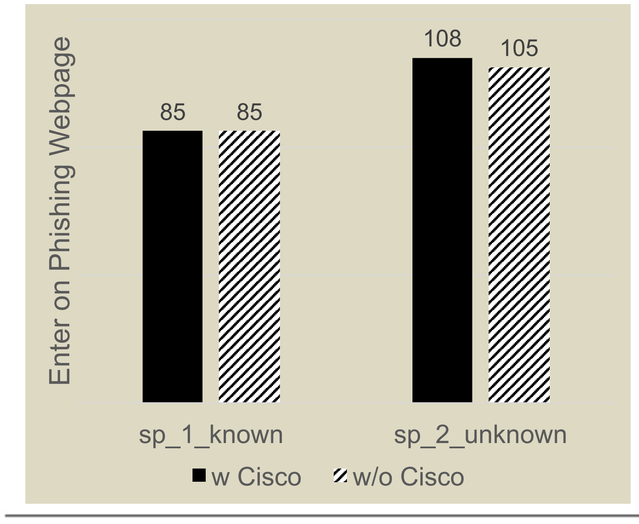
- **Action Selection Results of Spear-Phishing Emails**



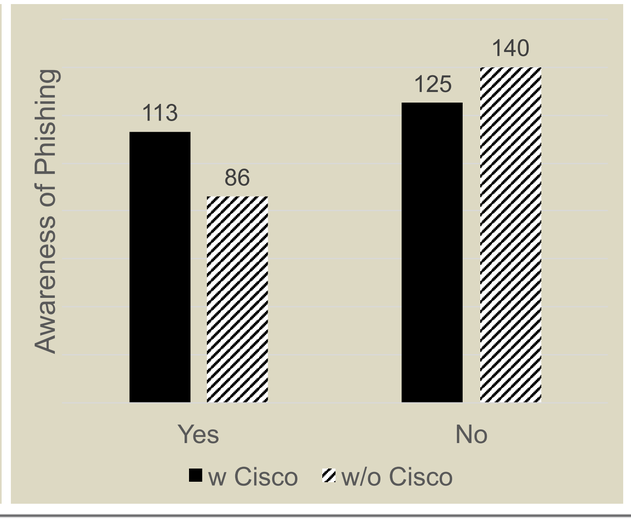
- **Enter Information on Phishing Webpages as a Function of Phishing Awareness**



- **Enter Information on Phishing Webpages**



- **Phishing Awareness Results**



Q1: Participants' responses to spear-phishing emails and phishing webpages varied as a function whether the campaign was known or unknown, indicating a response bias and a lack of knowledge of how to identify phishing scams.

Q2: The presence of a Cisco quarantine email showed an impact on participants awareness of phishing but minimal effect on participants' responses to spear-phishing emails and phishing webpages.

Reference:

- APWG (2018). Phishing activity trends report,3rd Quarter 2017. Retrieved from http://docs.apwg.org/reports/apwg_trends_report_q3_2017.pdf
- GreatHorn (2017). Annual global spear phishing report. Retrieved from https://www.wombatsecurity.com/blog/the-latest-in-phishing-first-of-2017
- Cyren (2017). Email security gap analysis report for Office 365. Retrieved from https://www.darkreading.com/cloud/office-365-missed-34000-phishing-emails-last-month/d/d-id/1330282?

PURDUE UNIVERSITY Discovery Park

CERIAS