Phish Finders: Analyzing Patterns in Email and Website Scams

Florida Gulf Coast University

Thomas Baratta & William Murphy

Introduction

- Companies and organizations face the challenge of effectively safeguarding their systems from phishing attacks.
- Our research utilizes data generated from a crowdsource initiative where volunteers tested their ability to effectively detect malicious emails and websites.

Research Question

How should organizations allocate their cybersecurity training to effectively decrease the victimization rate of their employees?

Background

- Our goal is to investigate patterns within email and website scams, aiming to identify common cue types that help facilitate employees identify malicious content.

Discussion

Precaution on Websites

- Malicious Websites have a higher victimization rate when compared to malicious emails.

Appeal to Authority & Greed Cue types

- The “appeal to authority” and “appeal to greed” cue types were over looked the most out of all other cue types.

Conclusion

- Organizations should take extra precaution for malicious websites and appeal cue types.

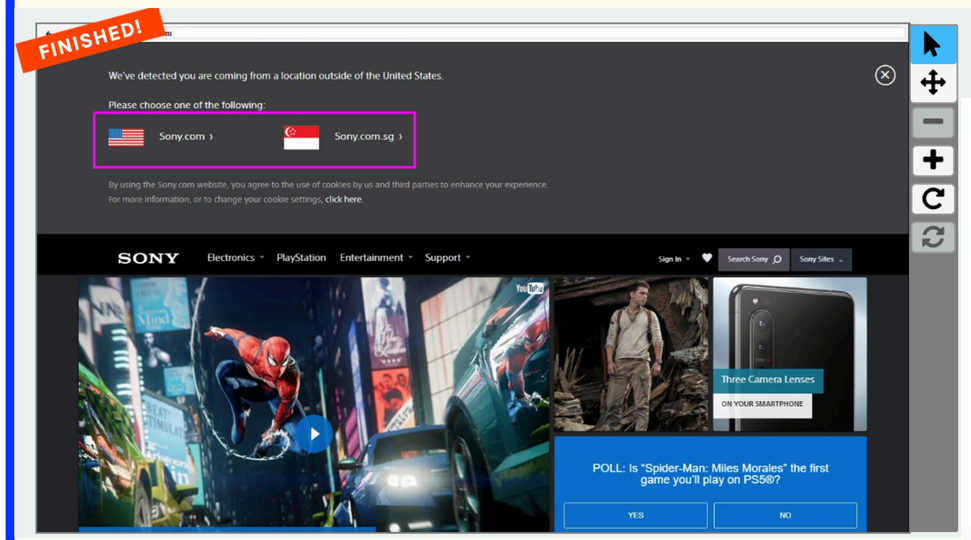
Method

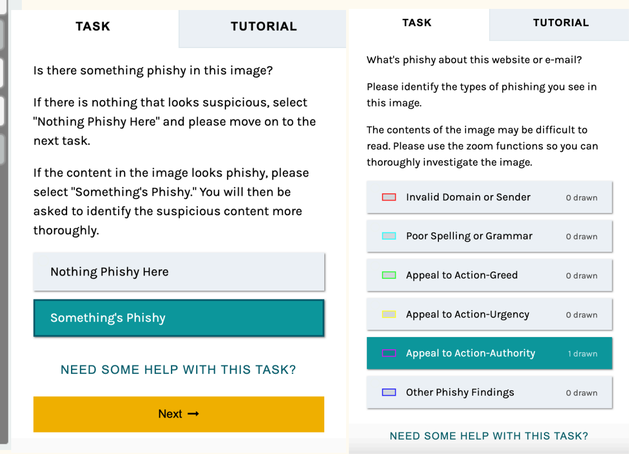
Data Collection

- The data retrieved within the Phish Finders project, hosted on the Zooniverse platform, involved participants evaluating images of both malicious and non-malicious content.

Data Filtering and Analysis

- Our goal is to Identify and filter valuable data that could inform and enhance employers’ cybersecurity training programs by identifying common patterns within the Phish Finders data.





Findings