Understanding User Behaviors When Phishing Attacks Occur

Yi Li
University of South Florida
Tampa, USA
yli13@mail.usf.edu

Kaiqi Xiong
University of South Florida
Tampa, USA
xiongk@usf.edu

Xiangyang Li
Johns Hopkins University
Baltimore, USA
xyli@jhu.edu

***Abstract*—To study user security-related behaviors, we conduct an experimental study where participants take part in our experiments in a lab contained environment. We used a set of emails including phishing emails from the real world. We collect data including participants' basic information and time measurement. We check whether or not factors such as intervention, phishing types, and incentive mechanisms play a major role in user behaviors when phishing attacks occur.**

***Index Terms*—User behaviors, phishing email, intervention**

I. Introduction

In this research, we aim at studying user behavior factors, such as intervention, phishing type, and a monetary incentive, to understand how a user behaves during phishing email attacks and what mechanism may prevent a user from being a victim of such attacks. Here, intervention is defined as a mechanism that helps users be aware of the phishing attacks more easily by modifying phishing types to make them appear more obvious [1]. A monetary incentive is introduced to motivate users to pay attention to phishing attacks [2]. Specifically, in our experiments, we recruit participants to conduct email sorting tasks. There are three kinds of phishing types in the phishing emails: (1) Suspicious senders' email addresses; (2) Suspicious links or attachments; (3) Malicious email contents. Performance of each participant, such as sorting correctness and time, is recorded in each experiment. The goal is to understand how user behaviors are correlated to phishing victims through an analysis of the collected experimental data.

II. The Study Design

In order to thoroughly understand user behaviors when phishing attacks occur, it is important to set up our study to be correspond to user behaviors when a user read emails in the real-world. Checking emails in our daily life can be viewed as an email sorting task because when we look at an email, we will first decide whether or not it is a legitimate email. We mimic an email opening, reading, and decision atmosphere for participants to sort emails into either a "phishing" or "normal" folder based on the information within the email.

1. Participant Recruitment: The IRB had been approved before we started to recruit participants (The approval number is: Pro00026240.) We have recruited 40 participants to perform this user study. We introduce a monetary incentive in our study to see whether the monetary incentive will affect a user's performance or not.

2. Experimental Rounds: We let participants perform three rounds of email sorting tasks. We collected data of each participant from each round. The average time spend in each round is about 15 minutes. Intervention is only used in the second round.

III. Evaluation

Our analysis have showed that participants with intervention and a monetary incentive perform better than other cases. Phishing type 1, tends to be more harmful to users compared to other two phishing types.

TABLE I
Email Round Score and Time

Attributes (Mean)	*Round1*	*Round2*	*Round3*	*R2-R1*	*R3-R2*
Phish_Score	10.18	11.6	10.02	1.42	-0.15
Total_Score	14.2	15.23	14.25	1.025	0.05
Phish_Time(s)	437.58	413.45	433.25	-24.13	19.8
Total_Time(s)	630.88	600.4	568.35	-30.48	-32.05

TABLE II
Different Types of Phishing Score and Time

Phishing Type	*Mean Score*	*Mean time(s)*	*Intervention Frequency*
Type 1	9.5	447.425	17
Type 2	11.35	431.875	8
Type 3	10.95	404.975	15

TABLE III
Monetary Incentive Analysis

Condition	*Phish_Score*	*Total_Score*	*Phish_Time*	*Total_time*
Control	30.1	42.65	1148.95	1580.5
Incentive	33.5	44.7	1419.6	2018.75

References

[1] W. Yang, J. Chen, A. Xiong, R. W. Proctor, and N. Li, "Effectiveness of a phishing warning in field settings," in *Proceedings of the Symposium and Bootcamp on the Science of Security*. ACM, 2015, p. 14.

[2] G. L. Brase, "How different types of participant payments alter task performance," *Judgment and Decision Making*, p. 419, 2009.

978-1-7281-2504-6/19/$31.00 ©2019 IEEE