Poster: Users Really Do Respond To Smishing

Muhammad Lutfor Rahman¹, Daniel Timko¹, Hamid Wali¹, Ajaya Neupane²
California State University San Marcos¹, Palo Alto Network²
San Marcos, CA, USA¹, Santa Clara, CA, USA²
mlrahman@csusm.edu, timko002@csusm.edu, wali003@csusm.edu, aneupane@paloaltonetworks.com

Abstract

Text phish messages, referred to as Smishing (SMS + phishing) is a type of social engineering attack where fake text messages are created, and used to lure users into responding to those messages. These messages aim to obtain user credentials, install malware on the phones, or launch smishing attacks. They ask users to reply to their message, click on a URL that redirects them to a phishing website, or call the provided number. Drawing inspiration by the works of Tu et al. on Robocalls and Tischer et al. on USB drives, this paper investigates why smishing works. Accordingly, we designed smishing experiments and sent phishing SMSes to 265 users to measure the efficacy of smishing attacks. We sent eight fake text messages to participants and recorded their CLICK, REPLY, and CALL responses along with their feedback in a post-test survey. Our results reveal that 16.92% of our participants had potentially fallen for our smishing attack. To test repeat phishing, we subjected a set of randomly selected participants to a second round of smishing attacks with a different message than the one they received in the first round. As a result, we observed that 12.82% potentially fell for the attack again. Using logistic regression, we observed that a combination of user REPLY and CLICK actions increased the odds that a user would respond to our smishing message when compared to CLICK. Additionally, we found a similar statistically significant increase when comparing Facebook and Walmart entity scenario to our IRS baseline. Based on our results, we pinpoint essentially message attributes and demographic features that contribute to a statistically significant change in the response rates to smishing attacks.

BIBLIOGRAPHIC REFERENCE

Users Really Do Respond To Smishing
Muhammad Lutfor Rahman¹, Daniel Timko¹, Hamid Wali¹, Ajaya Neupane²
California State University San Marcos¹, Palo Alto Network²

1. Introduction

Motivation
- Social engineering attacks are increasing, new mediums of attacks are emerging.
- Very few or limited users’ studies in the domain of smishing.
- Inspiration from prior studies.
- Users Really Do Plug in USB Drives They Find [1]
- Users Really Do Answer Telephone Scams [2]

Research Questions
- What is the success rate of smishing?
- Do different attributes of messages have an impact on the success rate of smishing?
- How does smishing impact different demographics?

2. Background

Attributes of Phishing SMS
- Entity - Organization or subject intending to reach a user with a message.
- Scenario - The content of the message sent to the victim user.
- Area Code - The area code from which a user receives the text.
- Method - The approach used by the attacker to get the victim to fall for smishing.
- Motivation - How an attacker urges their victim to adopt some call to action.

Ways a victim can fall for smishing
- Reply through text
- URL redirect to a website
- Call Back

3. Methodology

Experiment Procedure

Experiment Design

Smishing Experiment
- Bulk messaging to participants through Twilio.
- Post experiment survey through Qualtrics.
- Tracked user activity through Bitly links.
- Two rounds of smishing messages.
  - Seven messages sent in first round.
  - Five messages sent in second round.

4. Results

Potential Success Rate of Smishing

Impact of Message Attributes
- Entity Scenario
  - Statistically significant in fear-based comparisons FB vs IRS and Walmart vs IRS.
- User Action
  - CLICK+REPLY user action had significant increase in success rate vs others.

Impact of Demographics
- Error code 30003, 30005 and 30006 were undelivered due to unknown or unreachable destinations.
- Error Code:30007 corresponds to messages being filtered by either Twilio or the carrier.

Undelivered Messages

5. Discussion

Survey Responses
- Received a survey response rate of 1.76% compared to 1.17% from prior research [2].

Stop replies
- Participants instinctively replied STOP to messages, even when not an option.

6. Conclusion

- Smishing is a cybersecurity threat that is on the rise.
- We conducted a systematic and thorough empirical study on smishing with 265 unique users.
- We found that our participants potentially fell into smishing across user action, entity scenario, and several demographic features when compared to baseline values.
- Due to curiosity, more knowledgeable users may also become victims of smishing scams.
- To combat smishing, there is a need for greater user awareness and automatic SMS phish detection mechanisms.

Bibliographic References