Poster: Users Really Do Respond To Smishing

Muhammad Lutfor Rahman[1], Daniel Timko[1], Hamid Wali[1], Ajaya Neupane[2]
California State University San Marcos[1], Palo Alto Network[2]
San Marcos, CA, USA[1], Santa Clara, CA, USA[2]
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

Md Lutfor Rahman, Daniel Timko, Hamid Wali, and Ajaya Neupane. 2023. Users Really Do Respond To Smishing. In Proceedings of the Thirteenth ACM Conference on Data and Application Security and Privacy (CODASPY '23). Association for Computing Machinery, New York, NY, USA, 49–60. https://doi.org/10.1145/3577923.3583640

Users Really Do Respond To Smishing

Muhammad Lutfor Rahman[1], Daniel Timko[1], Hamid Wali[1], Ajaya Neupane[2]

California State University San Marcos[1], Palo Alto Network[2]

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

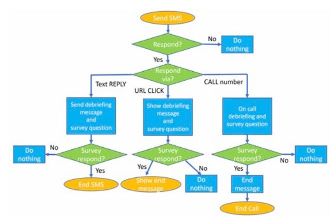
Bibliographic References

[1] Tischer, M., Durumeric, Z., Foster, S., Duan, S., Mori, A., Bursztein, E., & Bailey, M. (2016, May). Users really do plug in USB drives they find. In 2016 IEEE Symposium on Security and Privacy (SP) (pp. 306-319). IEEE.

[2] Tu, H., Doupé, A., Zhao, Z., & Ahn, G. J. (2019). Users really do answer telephone scams. In 28th USENIX Security Symposium (USENIX Security 19) (pp. 1327-1340).

3. Methodology

Experiment Procedure



Experiment Design

No.	Message	SMS sender ID	Area code location	Entity Scenario	Scenario	User Action	Motivation
E1	M1	1-833-222-9721	Toll-free	Walmart	Gift Card	CLICK	Reward
E2	M2	1-914-529-6528	Westchester, NY	Bank	Bank Transaction	REPLY	Fear
E3	M3	1-xxx-xxx-1803	Local	Law Enforcement	Arrest Warrant	CALL	Fear
E4	M4	1-855-777-8616	Toll-free	Facebook	Account Login	CLICK + REPLY	Fear
E5	M5	1-xxx-xxx-1803	Local	IRS	Lawsuit	CALL	Fear
E6	M6	1-xxx-xxx-1803	Local	Video website	Private video	CLICK	Fear
E7	M7	1-833-222-9721	Toll-free	FORTUNE 500 Co.	Job offer	REPLY	Reward
E8	M1	1-833-222-9721	Toll-free	Walmart	Gift Card	CLICK	Reward
E9	M3	1-855-777-8616	Toll-free	Law Enforcement	Arrest Warrant	CALL	Fear
E10	M5	1-855-777-8616	Toll-free	IRS	Lawsuit	CALL	Fear
E11	M7	1-914-529-6528	Westchester, NY	FORTUNE 500 Co.	Job offer	REPLY	Reward
E12	M8	1-xxx-xxx-1803	Local	FedEx	iPhone 13	CLICK	Reward

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

No.	Message	#Attempts	#Sent	#Undelivered	#Delivered	CALL	REPLY	CLICK	Total	%Success Rate
E1	M1	86	4	52	30	1*	-	8	9	30.00%
E2	M2	84	0	34	50	-	6	-	6	12.00%
E3	M3	75	0	44	31	1	2*	-	3	9.68%
E4	M4	85	4	55	26	1*	0	8	9	34.62%
E5	M5	96	0	32	64	5	3*	-	8	12.50%
E6	M6	105	0	75	30	-	-	4	4	13.33%
E7	M7	91	4	58	29	1*	4	-	5	17.24%
1st Round Total		622	12	350	260	9	15	20	44	16.92%
E8	M1	50	7	2	41	1*	-	4	5	12.20%
E9	M3	50	1	40	9	0	-	-	0	0.00%
E10	M5	50	10	3	37	2	-	-	2	5.41%
E11	M7	49	0	2	47	-	7	-	7	14.89%
E12	M8	99	0	39	60	1*	-	10	11	18.33%
2nd Round Total		298	18	86	195	4	7	14	25	12.82%
Grand Total		920	30	436	454	13	22	34	69	15.20%

Undelivered Messages

	Experiments												
	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	E11	E12	**Total**
Error Code:30003	3	9	16	9	4	7	7	2	0	1	0	0	58
Error Code:30005	2	0	0	6	0	1	8	0	0	2	0	0	19
Error Code:30006	47	25	28	40	28	67	43	0	0	0	2	5	285
Error Code:30007	0	0	0	0	0	0	0	0	40	0	0	34	74
Error Code Sum	52	34	44	55	32	75	58	2	40	3	2	39	436

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.

- **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.**

Impact of Demographics

Demographic(Baseline)	β	$CI_{95\%}$	T-value	*p*-value
Gender (vs Male):				
Female	0.090	[-0.98, 1.16]	0.165	0.870
Age(vs 25-34):				
18-24	-3.338	[-5.67,-1.00]	-2.800	0.005*
35-44	-.392	[-1.89, 1.11]	-0.512	0.608
45+	.573	[-1.62, 2.76]	0.513	0.608
Education(vs Bachelors degree):				
<High School	.137	[-2.84, 3.11]	0.090	0.928
High school graduate	.466	[-1.41, 2.35]	0.486	0.627
Some college	.112	[-1.31, 1.53]	0.155	0.877
Associate degree	-.429	[-1.83, 0.98]	-0.598	0.549
Masters degree	1.510	[-1.21, 4.23]	1.086	0.277
Doctoral degree	-.999	[-3.73, 1.73]	-0.717	0.473
Ethnicity(vs White):				
African American	1.879	[0.51, 3.25]	2.696	0.007*
Asian American	.374	[-1.93, 2.67]	0.319	0.750
Mexican American	2.368	[0.42, 4.31]	2.387	0.017*
American Indian	-18.132	[-14901, 14864]	-0.002	0.998
Other His./Lat.	-19.000	[-19343, 19305]	-0.002	0.998
Native Hawaiian	3.604	[-0.93, 8.14]	1.558	0.119
Other	-18.463	[-51004, 50967]	-0.001	0.999
Mobile Usage(vs 6-10):				
1-5 hours	-.346	[-3.04, 2.35]	-0.252	0.801
11-20 hours	2.208	[0.67, 3.75]	2.801	0.005*
21-31 hours	1.493	[-0.10, 3.09]	1.834	0.670
31+ hours	1.048	[-1.05, 3.14]	0.981	0.327
Profession(vs Student):				
Management professional	-1.542	[-3.55, 0.47]	-1.506	0.132
Sales and office	-1.183	[-3.19, 0.82]	-0.983	0.247
Technician	-20.322	[-12467, 12427]	-0.003	0.997
Service	-.366	[-2.52, 1.79]	-0.332	0.739
Software Engineer	-2.527	[-5.62, 0.57]	-1.601	0.109
Teacher	-20.401	[-21959, 21919]	-0.002	0.999
Construction and maintenance	-1.761	[-4.54, 1.02]	-1.242	0.214
Farming fishing and forestry	-.556	[-3.29, 2.18]	-0.398	0.691
Production transportation	-.826	[-3.87, 2.22]	-0.532	0.595
Government	-1.124	[-4.37, 2.12]	-0.679	0.497
Other	-2.478	[-5.47, 0.52]	-1.601	0.105

5. Discussion

- Well crafted smishing messages can be very effective for smishing attacks.
- Fear of losing social media account access received the highest smishing success rate of 34.62%
- Walmart Gift Cards and free iPhone reward messages were second and third highest success rates.
- Many messages filtered by either Twilio or Mobile Carriers.

Survey Responses

No.	Action	Reasons for response	Aware?
E1	CLICK	Curiosity.	Yes
E2	REPLY	Because we do not spend that kind of money at any Walmart	Yes
		Credit card fraud	Yes
E5	CALL	The fact that the area code for the phone number was the city of my school. So it made it like more realistic, rather than a random area code from a different city-state or country.	No
		Important government information, just because it has to do with taxes, it has to do with security numbers and all kinds of personal information.	No
		The fact that you were threatening me about my tax information.	No
E7	REPLY	If this is legit where do you get your contact list from?	Yes
E12	CLICK	I often find them funny, so I still open them even if I know it's fake. Also helps me educate myself on how these cons work.	Yes

- 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.

Experiment	Stop option	Stop Count	%
E7	Yes	4	18.18
E6	No	4	
E5	No	2	31.82
E3	No	1	

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.