Commercial Anti-Smishing Tools and Their Comparative Effectiveness Against Modern Threats

Daniel Timko, Muhammad Lutfor Rahman
California State University San Marcos
San Marcos, CA, USA
timko002@csusm.edu, mlrahman@csusm.edu

Abstract

Smishing, also known as SMS phishing, is a type of fraudulent communication in which an attacker disguises SMS communications to deceive a target into providing their sensitive data. Smishing attacks use a variety of tactics; however, they have a similar goal of stealing money or personally identifying information (PII) from a victim. In response to these attacks, a wide variety of anti-smishing tools have been developed to block or filter these communications. Despite this, the number of phishing attacks continue to rise. In this paper, we developed a test bed for measuring the effectiveness of popular anti-smishing tools against fresh smishing attacks. To collect fresh smishing data, we introduce Smishtank.com, a collaborative online resource for reporting and collecting smishing data sets. The SMS messages were validated by a security expert and an in-depth qualitative analysis was performed on the collected messages to provide further insights. To compare tool effectiveness, we experimented with 20 smishing and benign messages across 3 key segments of the SMS messaging delivery ecosystem. Our results revealed significant room for improvement in all 3 areas against our smishing set. Most anti-phishing apps and bulk messaging services didn't filter smishing messages beyond the carrier blocking. The 2 apps that blocked the most smish also blocked 85-100\% of benign messages. Finally, while carriers did not block any benign messages, they were only able to reach a 25-35\% blocking rate for smishing messages. Our work provides insights into the performance of anti-smishing tools and the roles they play in the message blocking process. This paper would enable the research community and industry to be better informed on the current state of anti-smishing technology on the SMS platform.

BIBLIOGRAPHIC REFERENCE

Daniel Timko and Muhammad Lutfor Rahman. 2023. Commercial Anti-Smishing Tools and Their Comparative Effectiveness Against Modern Threats. In Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '23). Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3558482.3590173

Commercial Anti-Smishing Tools and Their Comparative Effectiveness Against Modern Threats

Daniel Timko, Muhammad Lutfor Rahman

California State University San Marcos

1. Introduction

Motivation

To counter the threat of smishing, anti-smishing tools and regulations have been developed to help combat smishing.

- SMS filtering can be applied at several phases of the messaging process.
- Each tool implements their own techniques to stop malicious SMS.
- SMS messages are regulated through the Telephone Consumer Protection Act (TCPA).

Despite these efforts, smishing continues to increase.

- Within first six months of 2021, smishing increased by 700%. [1]

Through analyzing the current landscape of commercial anti-smishing tools we can discover how effective these tools are at detecting and mitigating attacks.

Contributions

Define the role that our tested SMS filters play on the messaging process

- We explore 5 bulk messaging services, 5 carriers, and 10 anti-smishing apps.

Smishtank – A collaborative resource for Smishing datasets

- We provide a live SMS feed of unfiltered smishing messages.

Data Characterization

- We analyze our collected phishing SMS across several categories.

Comparative Analysis of Anti-Smishing Tools developed to help combat smishing.

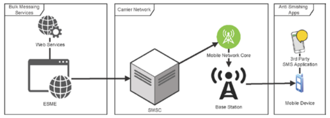
- We conducted a 3-part experiment to isolate the point where messages are being blocked.
- We compare the efficacy of each tool and their contributions to filtering smishing.

2. Background

Bulk Messaging Services
Sends and receive message data.

Mobile Carrier Network
Store and route text messages through carrier networks.

Anti-Smishing Apps on phone
Work on-top of the existing features to block/filter messages.



Bibliographic References

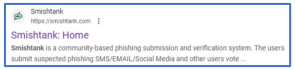
[1] itpro. Smishing attacks increased 700% in first six months of 2021. https://www.itpro.com/security/scams/360873/smishing-attacks-increase-700-percent-2021, 2021. [Online; accessed 24-July-2022]

3. Methodology

SMS Collection

Smishing

- To collect "fresh" smishing messages, we created smishtank.com.
- 75 messages submitted.
- 55 verified through a security professional.
- 20 selected for delivery.



Smishtank
https://smishtank.com

Smishtank: Home

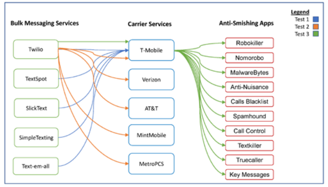
Smishtank is a community-based phishing submission and verification system. The users submit suspected phishing SMS/EMAIL/Social Media and other users vote ...

Benign

- From the UCI Machine learning repository.

UCI Machine Learning Repository

Testing Process



Performance Metrics

- **Smish Hit Rate**: The true positive rate(TPR) of smishing messages correctly identified.
- **Benign Strike Rate**: The false positive rate(FPR) of benign messages incorrectly identified

Bulk Messaging Services

twilio, TextSpot, SlickText, SimpleTexting, text-em-all

Mobile Carriers

verizon, AT&T, T Mobile, mint mobile, metro by T-Mobile

3rd Party Anti-Smishing Apps

iOS: Nomorobo, Malwarebytes, Spamhound, Textkiller, Robokiller

Android: Calls Blacklist, Anti Nuisance, Truecaller, Call Control, Key Messages

4. Results

Virus and Domain Info

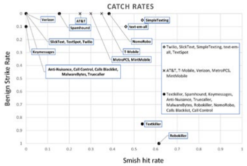
VirusTotal Scores

Type	#N	VT>1	VT>5	VT>10	VT-M	VT-MW	VT-P
URLS(ALL)	46	43.48%	15.22%	8.70%	28.26%	19.57%	26.09%
Domains(ALL)	44	25.00%	11.36%	9.09%	20.45%	6.82%	20.45%
URLS(Selected)	18	72.22%	11.11%	11.11%	50.00%	22.22%	38.89%
Domains(Selected)	17	29.41%	5.88%	5.88%	23.53%	11.76%	23.53%

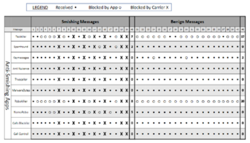
Domain History

- (30/46) created within 1-3 months of us receiving the message.
- (36/46) if last updated is considered.
- (3/46) could not be confirmed.
- (5/46) used authentic domains (e.g., social media smishing).

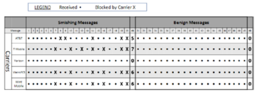
Tool Performance



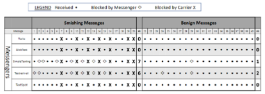
LEGEND Received • Blocked by App ○ Blocked by Carrier X


Smishing Messages
Benign Messages
Anti-Smishing Apps
Textkiller
Spamhound
Keymessages
Anti-Nuisance
Truecaller
MalwareBytes
Robokiller
NomoRobo
Calls Blacklist
Call Control

LEGEND Received • Blocked by Carrier X


Smishing Messages
Benign Messages
Carriers
AT&T
T-Mobile
Verizon

LEGEND Received • Blocked by Messenger ◇ Blocked by Carrier X


Smishing Messages
Benign Messages
Messengers
Twilio
SlickText
SimpleTexting

Data Characterization

Squatting Techniques

- Most messages (28/46) had none.
- Combosquatting and Wrong TLD most common (9/46).

URL types

- Most used Deceptive Top-Level Domains (33/46) or an Unintelligible URL.

Named entities

- The plurality of messages contained no entities (23/55).
- Banks impersonated most often with (14/55).

Message Subcategories

- Account Alerts (14/55) and Prize/Contest (12/55) were the most frequently observed types in the dataset.

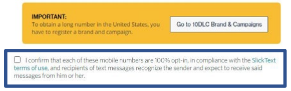
5. Discussion

Opt-In And Opt-Out

- Opt-In compliance was loosely enforced.
- Easy to find services that don't require Opt-Out dialogue.

Recommendations

- Require brand registration and Opt-In before allowing bulk messaging campaigns.



IMPORTANT:
To obtain a long number in the United States, you have to register a brand and campaign.

Go to 10DLC Brand & Campaigns

☐ I confirm that each of these mobile numbers are 100% opt-in, in compliance with the SlickText terms of use, and recipients of text messages recognize the sender and expect to receive said messages from him or her.

Message Blocking

- Similar messages blocked across carries on the same network implies shared filtering.
- Most of the tested Anti-Smishing Apps and bulk messaging services blocked no additional messages over what the carrier already blocked.

6. Conclusion And Future Work

- We provide a public repository called smishtank.com for future researchers.
- We scanned messages through VirusTotal and characterized the dataset.
- Some bulk messaging services, carriers and anti-smishing apps performed significantly different than one another on our smishing sets.
- Our comparative analysis of these tools found room for improvement against new smishing attacks.
- In future, we will investigate the role of Machine Learning in commercial anti-smishing technology.
- Explore the filtering of other types of mobile messaging systems such as Over The Top (OTP) (e.g., Whatsapp, Telegram and Facebook Messenger.)