Poster: A Comprehensive Categorization of SMS Scams

Sharad Agarwal
sharad.agarwal@ucl.ac.uk
UCL & Stop Scams UK
London, UK

Emma Harvey
emma.harvey@stopscamsuk.org.uk
Stop Scams UK
London, UK

Marie Vasek
m.vasek@ucl.ac.uk
University College London (UCL)
London, UK

ABSTRACT

SMS scams have surged over the recent years. However, little empirical research has been done to understand this rising threat due to the lack of an updated dataset. In the UK, mobile network operators run a firewall to block illicit messages. To this end, we collaborate with a major UK mobile network operator, which provides us with 3.58m SMS messages flagged by their firewall. These messages originated from over 42k unique sender IDs and were sent to 2.23m mobile numbers between December 2023 and February 2024. This is the first research to examine the current threats in the SMS ecosystem and categorize illicit SMS messages into eight sectors, including spam. We present the distribution of SMS messages successfully blocked by the mobile network operator's firewall and those that successfully evade detection.

ACM Reference Format:
Sharad Agarwal, Emma Harvey, and Marie Vasek. 2024. Poster: A Comprehensive Categorization of SMS Scams. In *Proceedings of the 2024 ACM Internet Measurement Conference (IMC '24), November 4–6, 2024, Madrid, Spain.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3646547.3689664

1 INTRODUCTION

SMS has become an essential medium for services like banks and delivery companies to communicate with their customers. Scammers have started taking advantage of this by impersonating various brands and luring victims by sharing a legitimate-looking malicious URL or deceiving them into calling/texting back on a phone number. Proofpoint, an international cybersecurity firm, detected a staggering 27x increase in SMS phishing from the second half of 2020 to the first half of 2021 [4]. The US Federal Trade Commission reported an increase in impersonation scams over text message in 2023 compared to 2020 [8] and a loss of $330 million in 2022 because of text scams, a 151% increase compared to 2021 [9]. UK Finance reports that most losses from authorised push payment (APP) fraud in 2023 originated from telecommunication [7] and the Global Anti-Scam Alliance reported SMS as the second most common medium [2].

Previous research has collated victim reports of spam and smishing from social media [5] or crowdsourced them [1, 6]. However, these are biased towards countries with no reporting mechanisms, primarily focused on spam, or contain data that is over a decade old or very small. This limits an up-to-date overview of the SMS threat landscape.

UK mobile network operators (MNOs) run a firewall that blocks illicit SMSs [3]. They also run a reporting service, 7726, to which customers can report a suspicious text, which they use to update their firewalls. To this end, we collaborate with a major UK MNO that provides us with two months of SMS messages flagged by their firewall.

2 METHODOLOGY

We receive a daily feed of SMS messages flagged by our collaborating MNO's firewall between December 14, 2023, and February 13, 2024. It groups all messages based on the sender IDs and adds a unique campaign ID depending on the content of the text message. This results in 2.3k unique campaign IDs containing 3.58m SMS messages.

An updated, labeled SMS scam dataset does not exist, limiting our options. We applied named-entity recognition (NER) to extract and identify the brands being impersonated. However, this does not produce satisfactory results, as criminals modify the entity names in the text to evade detection: *e.g.* using 'Evr1' instead of 'EVRI.' The pre-trained NER algorithm also fails to identify most European brands.

To this end, we manually identify and categorize one day's messages into different sectors. Using this, we categorize the others in the same campaign programmatically. Two authors manually categorized the remaining text messages. Unidentified messages are overwhelmingly false positives and removed from the analysis.

3 SMS SCAMS CATEGORIZATION

Criminals lure victims into clicking on a malicious URL or initiating a conversation to build relationships and steal their financial details.

Delivery Impersonation Scams. The different types of delivery scams are: (1) Missed parcel: a parcel could not be

IMC '24, November 4–6, 2024, Madrid, Spain

ACM ISBN 979-8-4007-0592-2/24/11
https://doi.org/10.1145/3646547.3689664

delivered and needs to be rescheduled; (2) Parcel waiting to be collected: a parcel needs to be collected and there's a link to access it; and (3) Payment due: a parcel requires payment before it can be shipped, or delivered. This is the most prevalent scam (Table 1). However, Fig. 1 indicates a peak for delivery scams closer to occasions like Christmas.

Table 1: Distribution of SMSs ($n = 2.82m$) into eight categories, including spam.

Category	Recipients	Successful Msgs	Blocked Msgs	Sender IDs
Wrong Number	24.5k	2.4k	23.9k	17.2k
Hi Mum	490.1k	64.3k	519k	10.2k
Delivery	830.2k	132.4k	**1.3m**	8.4k
Banking	61.6k	24.5k	47k	1.7k
Telecom	256.0k	138.4k	140.8k	600
Government	81.8k	4.2k	80.1k	200
Others	769	322	1k	130
Spam	164.5k	71.4k	282.6k	880

Telecom Impersonation Scams. We identify three subcategories: (1) Missed payment: pay now to avoid cancelled service after a failed payment; (2) Contract issues: log in for contract renewal or urgent service issues; and (3) Rewards: click to claim or redeem prizes earned from loyalty rewards or gifts. Surprisingly, these scams are the most successful in evading detection.

Government Impersonation Scams. The three subtypes are: (1) Vehicle/Revenue tax: claim the overpaid tax on revenue or vehicles; (2) Routine verification: perform a routine verification and take action by clicking on a URL; and (2) Passport forms: check approved passport-related forms.

'Hi Mum and Dad' Scams. Criminals pretend to be a child in distress, address the victims as a parent, and ask them for financial help. Unlike others they lure victims into directly transferring money into their accounts. Fig. 1 shows the constant presence of this scam. They use the second most sender IDs to initiate the text messages (Table 1).

Wrong Number Scams. These start with a random, irrelevant message sent to a victim. Once the victim replies inquisitively, the criminals claim they messaged the wrong person and then try to establish a relationship by continuing the conversation. The criminals eventually lure them into bogus cryptocurrency investment schemes or fall for a romance scam. Table 1 indicate the maximum exploitation of the mobile numbers to initiate the conversations.

Banking Impersonation Scams. We identify multiple modus operandi: (1) luring victims into providing information via malicious URLs; (2) asking to text back 'Y' or 'N,' followed by a call; and (3) asking the victim to call on a phone number. The various reasons provided include: (1) providing a one-time password; (2) a fake purchase attempt; (2) adding a new device, payee, or direct debit to the bank account; (3) cautioning about a flagged payment for vehicle finance; or (4) request to change their associated phone number. To our surprise, these scams are less prevalent than others.

We identify a few messages impersonating **other**, less common brands, such as online streaming providers or those without brand names. We also find **spam** messages, unsolicited messages promoting but not impersonating brands.

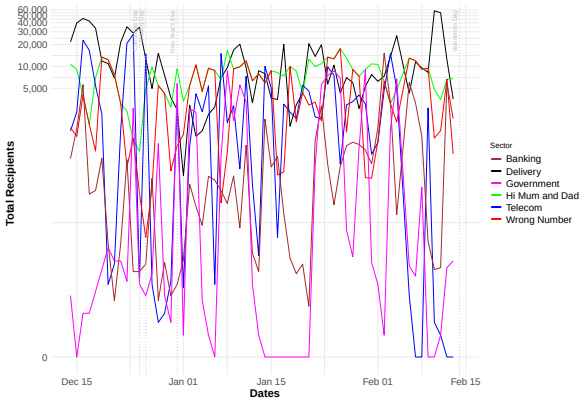

Figure 1: Top six SMS scam categories that target victim mobile numbers ($n = 1.9m$) over time.

4 CONCLUSION

Our research provides novel insights into the current threat landscape in the SMS ecosystem. The number of SMSs blocked by the mobile network operator's (MNO) firewall indicates their effectiveness. However, quite a few of them successfully evade initial detection. This indicates that threat actors continue to rephrase, update the text, and use multiple sender IDs. While users are shifting to online messaging, this paper serves as evidence that criminals continue to abuse MNOs to target victims over SMS. Our future work will focus on the infrastructure criminals abuse to conduct scams and the lures used to deceive victims.

REFERENCES

[1] Tao Chen and Min-Yen Kan. 2012. Creating a Live, Public Short Message Service Corpus: The NUS SMS Corpus. *Language Resources and Evaluation* (Aug. 2012).
[2] GASA. 2024. The Global State of Scams - 2023. https://bit.ly/4eSIHM9.
[3] Mobile UK. 2022. Industry implemented strengthened customer protections result in substantial reduction in scam texts. https://bit.ly/3xPMg4Z.
[4] Proofpoint. 2022. The Human Factor 2022. https://bit.ly/4cUEdCK.
[5] Siyuan Tang, Xianghang Mi, Ying Li, XiaoFeng Wang, and Kai Chen. 2022. Clues in Tweets: Twitter-Guided Discovery and Analysis of SMS Spam. In *ACM Conference on Computer and Communications Security*. 2751–2764.
[6] Daniel Timko and Muhammad Lutfor Rahman. 2024. Smishing Dataset I: Phishing SMS Dataset from Smishtank.com. (2024), 289–294.
[7] UK Finance. 2024. Annual Fraud Report 2024. https://bit.ly/465lXVc.
[8] US FTC. 2024. Impersonation scams: not what they used to be. https://bit.ly/3zBxAXE.
[9] US FTC. 2024. New FTC Data Analysis Shows Bank Impersonation is Most-Reported Text Message Scam. https://bit.ly/4603SI2.