A Comprehensive Categorization of SMS Scams

Sharad Agarwal[1,2], Emma Harvey[2], and Marie Vasek[1]

[1]University College London (UCL) [2]Stop Scams 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, SpamShield, 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.

Methodology

- We collaborate with a major UK mobile network operator to access SpamShield (`https://bit.ly/40c406o`) data between December 14, 2023, and February 13, 2024.
- SpamShield groups SMS messages based on the sender IDs and adds a unique campaign ID as per the content of the text message, resulting in 2.3k unique campaign IDs containing 3.58m SMS messages.
- We apply named-entity recognition (NER) to extract and identify the brands being impersonated. However, the pre-trained model fails to identify most European brands. Also, criminals modify the entity names in the text to evade detection: *e.g.* using 'Evr1' instead of 'EVRI.'
- We manually identify and categorize one day's messages into different sectors. Using this, we programmatically categorize the others in the same campaign.
- Two authors manually categorized the remaining text messages.

Results

While users are shifting to online messaging, this paper serves as evidence that criminals continue to abuse mobile network operators to target victims over SMS.

Top Scam Messages Received over Time

Delivery impersonation scams are the most prevalent (Table 1). However, Fig. 1 indicates a peak for delivery scams closer to occasions like Christmas.

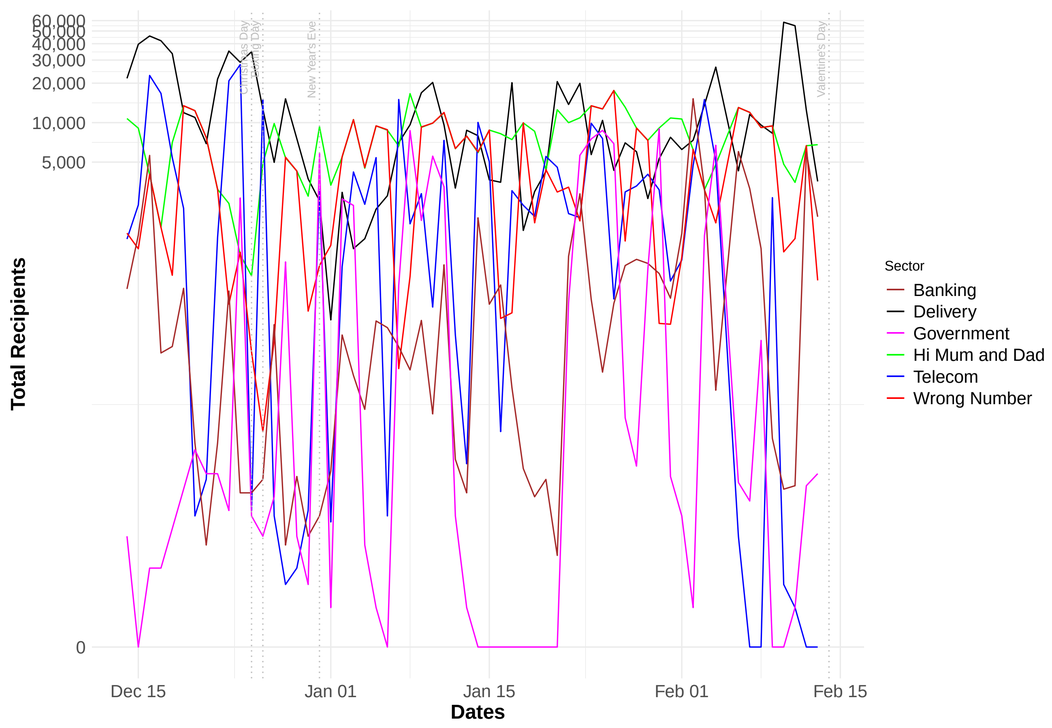

Figure 1: Top six SMS scam categories that target victim mobile numbers ($n = 1.9m$) over time.

Scam Categories

The 'Wrong number' and 'Hi mum and dad' scam messages abuse most mobile numbers as sender IDs (P2P) to initiate messages and continue interacting with victims, luring them into providing financial details (Table 1).

Telecom impersonation scams are the most successful in evading detection.

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	**1.3**m	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

Originating Mobile Network Operators (MNOs)

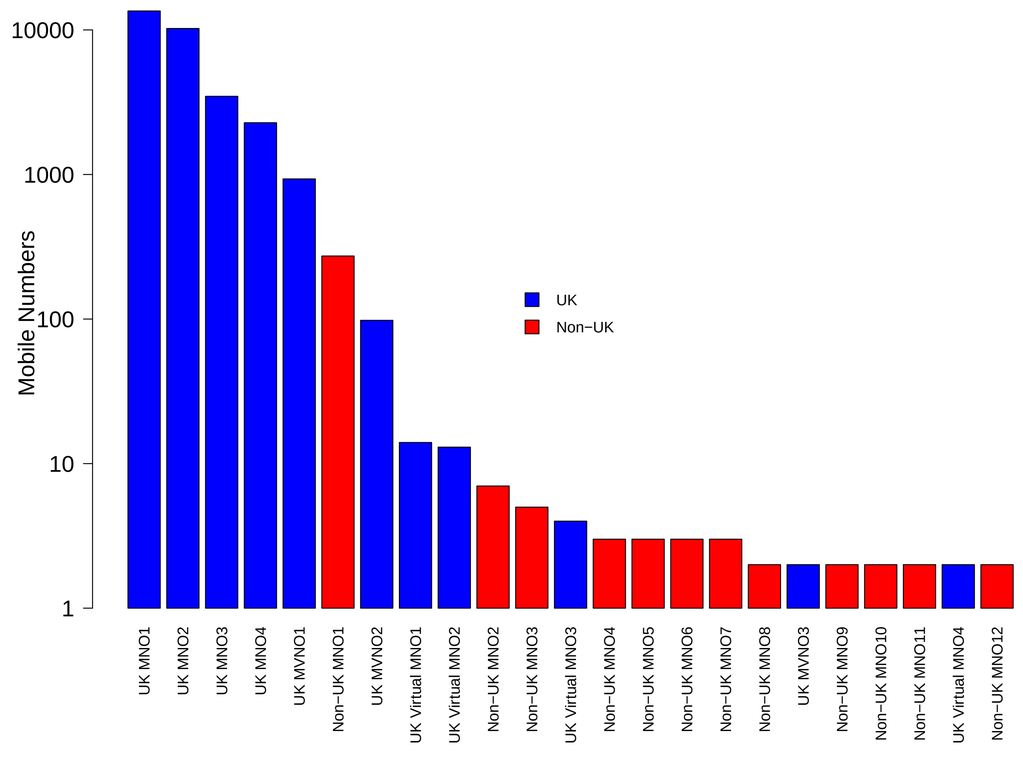

Figure 2: Distribution of top 23 originating mobile network operators ($n = 30,892$) abused to broadcast scam messages. The y-axis is on a log scale.

Recommendations

Scammers significantly abuse peer-to-peer (P2P) routes and broadcast SMS to deceive users by impersonating organizations/brands and family/friends. We recommend know your customer (KYC) checks for SIM registrations.

Figure 3: Sim box confiscated by the City of London Police from scammers sending 'hi mum and dad' SMS messages (`https://bit.ly/3NuqjwD`).

Scammers abuse SIM boxes/banks to broadcast scam messages and communicate with the victims (Fig. 3). We suggest penalizing SIM farms' supply and use for illegitimate use.

Scammers send hundreds to thousands of messages per sender ID mobile number to broadcast scam messages. We suggest implementing standardized SMS volume limits for personal use.

In the future, we aim to utilize LLMs to classify and categorize scam messages to overcome the issues of NER and other NLP algorithms. Read our extended abstract – >

sharad.agarwal@ucl.ac.uk
emma.harvey@stopscamsuk.org.uk
m.vasek@ucl.ac.uk