‘Hey mum, I dropped my phone down the toilet’: Investigating Hi Mum and Dad SMS Scams in the United Kingdom

Sharad Agarwal[1,2], Emma Harvey[2], Enrico Mariconti[1], Guillermo Suarez-Tangil[3], and Marie Vasek[1]

[1]University College London (UCL), [2]Stop Scams UK, [3]IMDEA Networks Institute

Abstract

SMS fraud has surged in recent years. Detection techniques have improved along with the fraud, necessitating harder-to-detect fraud techniques. We study one of these where scammers send an SMS to the victim addressing mum or dad, pretend to be their child, and ask for financial help. Unlike previous SMS phishing techniques, successful scammers interact with victims, rather than sending only one message which contains a URL. This recent impersonation technique has proven to be more effective worldwide and has been coined the ‘hi mum and dad’ scam. In this paper, we collaborate with a UK-based mobile network operator to access the initial ‘hi mum and dad’ scam messages and related user spam reports. We then interact with suspicious scammers pretending to be potential victims. We collect 582 unique mule accounts from 711 scammer interactions where scammers ask us to pay more than £577*k* over three months. We find that scammers deceive their victims mainly by using kindness and distraction principles followed by the time principle. The paper presents how they abuse the services provided by mobile network operators and financial institutions to conduct this scam. We then provide suggestions to mitigate this cybercriminal operation.

1 Introduction

SMS-based phishing, also known as smishing, is a social engineering attack where the victims are deceived into providing sensitive information (e.g., login credentials, bank account details) over SMS or other online messaging platforms such as WhatsApp or Telegram. This is most commonly done by pretending to be someone else and inducing the user to click on a phishing URL. Some researchers also consider smishing to be SMS with email-ids or phone numbers requesting to send email or call back [54, 55, 85]. Industry reports show smishing has increased 270% globally from the second half of 2020 to the first half of 2021 [75] and is 15 times higher in the UK than in the US [99].

We study a subtype of smishing where fraudsters repeatedly interact with victims. Here, the attackers pretend to be a child in distress and address the victims as mum or dad and ask them for financial help [6]. The novelty of this impersonation scam stands on the scammer providing a new phone number in the body of the initial scam message for the victim to interact with them over text. Industry reports that conversational threats became the highest category of mobile abuse by volume in 2022 and continue in the first quarter of 2023 [51]. In the first half of 2022, Action Fraud, the cybercrime reporting center in the UK, received more than 1,200 reports on scams where scammers deceive victims by posing as their loved ones, which amassed to £1.5*m*. Furthermore, in 2022, UK Finance reported that victims of impersonation scams lost £67.8 million [37]. As per a survey conducted by the Global Anti-Scam Alliance in 2023, cybercriminals stole £7.5 billion as one in ten people in the UK fell victim to these scams [2].

In 2021, the ‘hi mum and dad’ SMS scam was first reported in English-speaking countries like the UK [21] followed by Australia (Fig. 1) and has spread to Germany, Spain, Italy, and the USA, targeting victims globally. Despite the widespread occurrence and severity of this scam, there is a significant absence of systematic studies that examine its anatomy, including: (1) mapping out the actors involved, (2) learning its life cycle, and (3) dissecting its infrastructure.

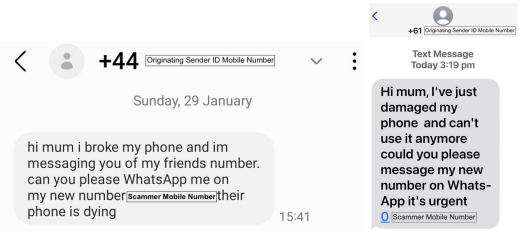


Figure 1: Original ‘hi mum and dad’ SMS scam messages.

With the ever-increasing need for mobile phones and the proliferation of spam, mobile network operators increasingly work on filters to detect and stop spam messages while providing services for users to report spam. In the UK, mobile

network operators run a reporting service, 7726 ('SPAM' on a mobile keypad), where users can forward a suspected spam message. In response, Apple and Google rolled out a one-click reporting button which allows users to report potential scam messages directly to their mobile network operator.

Research Gap. In this paper, we collaborate with a major UK-based mobile network operator. We acquire a corpus of initial 'hi mum and dad' SMS scam messages, identified by our collaborator's filters and users. However, these interactive scams unfold through multiple messages, often hand curated after the initial stage around replies that victims send. Therefore, analyzing only this early data would provide a partial glance of the end-to-end scam operation and limit our understanding of the lure principles used to deceive the victims. This would hinder the effective deployment of mitigating actions.

Contribution. To address this limitation, we tackle the crucial challenge of reconstructing *all* stages involved. We implement a proactive approach by actively engaging with scammers posing as potential victims. This methodology integrates active measurements (e.g., HLR lookups) that allow us to gain deeper insights into the later stages of the scam life cycle beyond what is captured by the passive data collection. By wielding filtered data/user reports to jumpstart our interactions, we aim to present a more holistic understanding of the SMS scams prevalent in the UK, shedding light on their multifaceted nature and potential countermeasures.

Using our collected data, we set out to answer the following research questions:

RQ1 Do scammers target victims based on their gender?

RQ2 How do scammers lure victims into replying to them?

RQ3 How do scammers choose the mobile network operators, and how long do they use these mobile numbers?

RQ4 How do scammers avoid getting flagged by financial institutions?

RQ5 How can we identify connections between different scammers?

This paper provides the following contributions:

- We are the first to study SMS interactive scams, focusing on 'hi mum and dad' scams. Our work interacts with the scammers to investigate this ecosystem in-depth and estimate that UK-based victims lose at least £2.3 million per year (£577*k* was requested over 13 weeks).
- We provide a rigorous analytical methodology in §3.3 that can be applied to study similar scams.
- We uncover the infrastructure criminals abuse to run this campaign. We present insights into key components like specific operators and banks and the fraud operation more broadly.

2 'Hi Mum and Dad': Anatomy of the Scam

SMS phishing (smishing) texts typically impersonate a service or brand and trick recipients into clicking a URL that steals their sensitive information. Smishing has recently gained significant attention [47, 49, 95] due to the surge of attacks leading to significant financial and personal data losses [30, 38, 46].

We focus on 'hi mum and dad' SMS scams, which operates differently than a traditional smishing scam. In this section, we provide a detailed description of the terminology used and how scammers operate this relatively unknown type of scam.

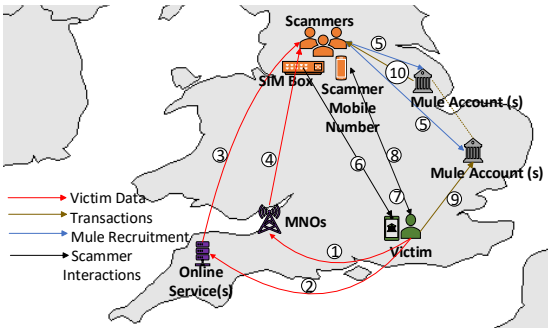


Figure 2: Operational steps of a 'hi mum and dad' SMS scam.

Overview. In a 'hi mum and dad' scam, fraudsters attempt to send SMS messages to parents pretending to be their children and offering a narrative that explains why they are addressing them from a different phone number. Fig. 2 offers an overview of how this scam works. We see various roles and stakeholders involved in every step of the operation. We next describe in detail how an operation works, which we divide into the following phases.

Preparation Phase. In this phase, the attacker plans the scam. Two possible points of failure could leak the user's mobile numbers to the scammers — mobile network operators that store their subscribers' details to provide telecommunication facilities ①, and the online websites where users register their mobile numbers to access the services ②. Scammers receive the users' mobile numbers through datasets leaked from data breaches ③ ④.[1] Scammers also recruit money mules via online job advertisements (cf. §5.1) to receive funds from the victims ⑤. Money mules are individuals or entities deceived into accepting stolen money and forwarding it to scammers [31, 57].

Initiation Phase. Once the scammer receives the target mobile numbers, they initiate the scam using devices like a SIM box/bank to send multiple initial scam messages to several victims simultaneously ⑥[2]. A SIM box/bank is a VoIP gateway

[1] Our interaction pretending to be a reporter with one of the scammers confirms this.

[2] LinkedIn post by DCPCU picturing the confiscated equipment.

device that allows the usage of multiple SIM cards belonging to different mobile network operators simultaneously. We refer to these mobile numbers as the *originating sender ID mobile number*.

Execution Phase. Once the initial scam message is received, some users are deceived into replying to the text message and initiate the conversation to the mobile number sent in the text message ⑦. We call this number the *scammer mobile number* as the scammer uses it to communicate with the victims and is often different from the *originating sender ID mobile number*. Many initial scam messages ask users to reply on *online messaging platforms* such as WhatsApp or Telegram instead of SMS. When the scammer initiates contact, they pose as the victim's child and provide a reason for using a different phone number. The scammer then lures the victim into transferring a particular amount of money to pay an urgent bill as they cannot use their mobile banking app due to the change in the mobile number. For this, the scammer provides the victim with a *mule account* ⑧. Mule accounts are bank accounts owned by individuals or entities who allow them to be used for financial transactions as a part of a scam.

Transaction Phase. Once the victim is persuaded, they transfer the requested amount to the provided mule account(s) ⑨. Here, scammers operate differently: some request a single amount, while others request more than one amount into multiple mule accounts, providing a reason to pay separate bills. As we do not transfer any money to the scammers, we do not know if they return to the victims to ask for more money.

Payouts. As mentioned, scammers use money mules. They rely on them to hide their bank accounts. To evade detection, the money in a mule account might hop to multiple accounts before reaching the scammer ⑩. The transfers to the attacker are untraceable and irreversible as they often include international wire transfers [39]. Scammers attempt to evade detection by the banks by using money laundering techniques like buying gold with cash [92].

3 Methodology

This section explains how we receive the initial 'hi mum and dad' SMS scam message from our partner, a major mobile network operator. We outline our approach to engaging scammers while posing as victims and describe how we enrich the data to measure the infrastructure used by scammers and the methods we use to study the impact of this scam.

3.1 Data Collection

Mobile network operators in the United Kingdom use filtering techniques to detect and identify spam messages. They also run a user spam reporting service, where users can report suspicious texts either by forwarding the spam text or through the one-click reporting system enabled by Apple and Google in their messaging platforms. We collaborated with a UK-based mobile network operator who provided the daily feed of the initial 'hi mum and dad' SMS scam messages between June 20 and September 15, 2023.[3] An example of an initial 'hi mum and dad' scam message is:

> Hi mum, I broke my phone this morning I'm having a nightmare. <*phone number*> is my new number can you give me a text when you see this x.

We refer to the messages received from the mobile network operator as the *initial scam message*. In addition to the text messages, the mobile network operator provided us with the number of times they detected the specific message. From August 18 onwards, the mobile network operator also added the *originating sender ID mobile number* from which the initial scam message originated, where available.

3.1.1 Scammer Interactions

Victims receive initial messages which request for them to contact a mobile number provided within the text message, which we refer to as the *scammer mobile number*. We create three profiles: mum from one profile, dad from the second, and the third does not mention mum or dad. Each profile has ten virtual mobile numbers and we use these to contact the scammers.

To initiate a conversation, we send one SMS from every profile to all active scammer's mobile numbers that appear in our daily data feed.[4] This helps to find out if they would reply only to a message from a mum or dad or alternatively would assume themselves and address us as mum or dad. We use the home location register to check whether a number is active, as we will explain in §3.2. Fig. 3 shows the modified life cycle of a 'hi mum and dad' SMS scam where we act as the victim and interact with the scammers.

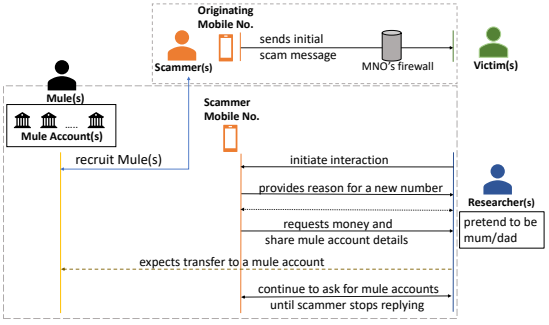


Figure 3: Modified life cycle of a 'hi mum and dad' SMS scam.

Note that the originating sender ID mobile number could be spoofed [96]. Spoofing is a technique that allows a user to

[3] We did not receive a feed on July 16, 21, 22, and September 8.
[4] We do not interact with scammers over the weekend.

replace the actual mobile number from which they call/send a message with the mobile number they want the receiver to see. This technique helps them hide their mobile number to evade detection from the mobile network operators and extend their mobile numbers' lifetime to continue abusing it. Therefore, we do not send messages to the originating sender ID mobile numbers but rather to the phone number provided by the scammer in the body of the text message. This is what scammers expect from the victims and, by doing so, we increase our chances of establishing a dialog with them.

Scammers tend to work in groups [82], and there is a high possibility that the same scammers operate multiple mobile numbers used in the same scam. To receive a better response rate and avoid detection, we change the format of our initial message. As the first scammer message targets potential victims in the UK, we use common British names like David and Hannah to address the scammers and make them believe that a victim has fallen into the trap. We modify our initial message as per the context of the scammer's initial message, such as:

> How did it break Hannah? Are you taking it to get repaired? Mummy x.

Once the scammer responds to our message, we continue the conversation with them. This also indicates that scammers do not verify the mobile number they interact with as they never send us the initial message (cf. §4.2). Here, we notice how scammers develop a narrative to request a transfer of a particular sum of money to a bank account. For example,

> I have a little problem, I have 2 bills that I need to pay as soon as possible but I can't pay them myself because I can't get into my banking app.
>
> I have the banking app on my old phone and this number that i have now is not registered with my bank. It takes about 2 days to get registered due to security rules.

We log these conversations, the details of the payment methods provided by the scammers, and the amount of money requested for both further analysis and responsible disclosure (to the respective banks). We do not transfer any money. Instead, we convince the scammers that the transfer is not going through and collect multiple mule accounts[5] from them to identify networks of scammers cooperating.

We collaborate with an international threat intelligence company that replicates our scammer interaction approach using 100 different accounts on the scammers' preferred online messaging platform. The company sends initial messages to the scammer's mobile numbers identified from their initial data source and they pretend to be victims. In turn, they collect and provide the mule account details, the scammers' mobile numbers that provide the mules, and the amounts they request. Due to business confidentiality reasons, we do not have access to their initial source of 'hi mum and dad' SMS scam messages, including the originating sender ID mobile numbers and their conversations with the scammers. Their data collection is from July 18 – September 8, 2023.

Additionally, we have one conversation with a scammer where we pretend to be a reporter. We do not formally recruit them or conduct an interview. They mention scammers' potential source of target mobile numbers (§2) and the difficulties receiving bigger value transactions (cf. §4.4).

3.2 Data Enrichment

The 'hi mum and dad' SMS scam depends heavily on mobile numbers – scammers need them to send the initial scam message and then additional mobile numbers to continue the conversation with the victim once they lure a victim into replying. We use the Home Location Register (HLR) lookup [59] to investigate these mobile numbers. HLR lookup provides detailed information about a mobile number's current status (live/inactive/dead) and its original and current mobile network operator.

We perform a daily HLR lookup on all scammer mobile numbers (July 11 - September 15, 2023) extracted from the initial 'hi mum and dad' scam message to check the mobile's live status[6] before initiating the conversation. We also perform a daily HLR lookup on the originating sender ID mobile numbers (August 21 -September 15, 2023) and the scammer mobile numbers provided by the threat intelligence company (August 2 - September 15, 2023). We use the service provided by `https://hlrlookup.com` to perform these lookups. Due to technical issues, this service did not run for six days in July and two days in August. We use these results to calculate every mobile number's lifetime and find the various mobile network operators scammers abuse.

We further check for an individual or entity as a recipient's name in the account details scammers provide. If it is an entity, we query against the UK Companies House register to validate whether it is registered as a 'limited company' in the UK [44]. Lastly, we informally discuss the suspicious mule accounts with two UK financial institutions. Again, we do not formally recruit participants or conduct interviews. This provides us with feedback mentioned in §5.1, helping us to suggest potential educational mitigations in §5.2.

3.3 Analysis Methods

We analyze conversations, financial transactions, and network data to answer our research questions (§1). We also perform survival and attribution analysis. Fig. 4 shows the data we require (top) to perform each step of the analysis (bottom). Next, we detail the methods that underpin our approach.

[5] Only the banks investigate and provide confirmation of a mule account.

[6] `https://www.hlrlookup.com/knowledge/full-api-result`

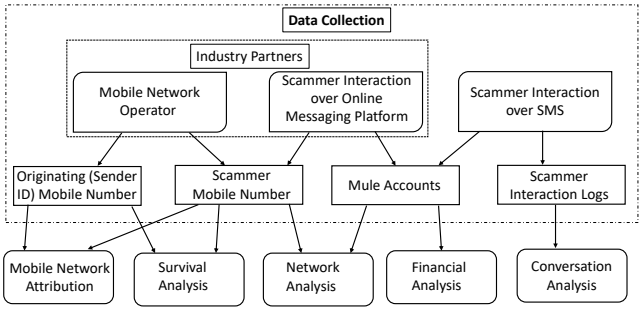


Figure 4: Analysis methods towards understanding 'hi mum and dad' SMS scams.

Conversation Analysis. We conduct an n-gram word thematic analysis using unigrams and bigrams on the 3,402 initial 'hi mum and dad' SMS scam messages and the 231 conversation responses from the scammers between June 20 and September 15, 2023. Since we do not have access to the full conversation data from the threat intelligence company, we do not include their data here. Our conversation analysis thus only uses our collected SMS message data.

We perform a thematic analysis over two different sets: 1) the initial messages we collect from the mobile network operator we partner with and 2) the conversations we elicit from our responses. For the former, unigram analysis helps identify the various reasons and lure principles scammers use in the initial scam messages. For the latter, both a unigram and a bigram analysis offer insights into the three stages of scammer responses. We also reconstruct the entire conversation (initial message and the subsequent responses) and study the target of the attack using a custom-named entity identification tailored to the 'hi mum and dad' scam. This shows which parent attackers target for replies based on gender. We use time series to study responses and identify scammers' work patterns, including when they are most active.

Mobile Network Attribution. We use HLR lookup queries to identify and characterize the mobile network operators scammers abuse. For identification, we selectively query an online HLR register that reveals the original mobile network operator of a phone number. For characterization, we classify the mobile network operators into three main categories — Physical operators provide physical SIM cards, MVNO or mobile virtual network operators provide SIM cards but run on another mobile network operator 's services, and Virtual mobile network operators provide virtual numbers instead of physical SIM cards.

We perform HLR lookup queries on 1,184 scammers mobile numbers and 685 originating sender ID mobile numbers from July 11 to September 15, 2023, to identify the various mobile network operators they abuse to run the scam.

Survival Analysis. To understand the performance of this scam, we study the lifetime of the mobile numbers abused by scammers. We calculate the number of days mobile numbers were active for 1,590 unique mobile numbers (scammers' and originating sender ID mobile numbers)[7] judging by the availability status we retrieve daily from the HLR lookups we performed between July 11 and September 15, 2023.

As of the last day of our data collection, we see 271 active mobile numbers. We conduct survival analysis, which helps reveal patterns of how long mobile numbers have been active. In particular, this technique considers intermittently unavailable data points to be "right-censored"; we only monitor these mobile numbers until September 15, 2023, and censor those still active on that date. We use a Kaplan-Meier estimator [50] to estimate the survival function $S(t)$ from the lifetime we observe in the data. Intuitively, this measure illustrates the fraction of mobile numbers that become inactive after a given date. We then use the probability of a mobile number abused by a scammer being active after x days to estimate the survivability of these numbers.

Financial Analysis. We investigate the financial transactions scammers request victims to (1) identify the categories of financial institutions mule accounts belong to in the UK, (2) study the range of amounts requested over the two messaging platforms, and (3) show how scammers avoid getting flagged by the banks. As mules play a significant role in this scam, the information we extract in this step is crucial to understanding how money flows from victims to scammers.

First, we extract bank account details from the conversations. When a user opens a bank account in the UK, the bank assigns a combination of identifiers: an account number and a sort code. The first two digits of the sort code identify the bank and the last four digits refer to the specific branch of the bank where the user opened the account. In the UK, individuals can send money online to another individual or organization's bank account using their sort code and account number through the Bacs [70] or the Faster Payment System [71]. In thirteen weeks, we collected 582 unique mule accounts from scammers over SMS and an online platform. We classify the mule accounts collected into five broad categories per the handbook of the UK regulator, the Financial Conduct Authority (FCA) [13].

Second, we calculate the minimum, maximum, mean, and median values of all transaction requests from scammers over the two messaging platforms. As the requested amounts range between £100 and £6,000, we group the transaction requests into chunks of £500 which allows us to visualize and better analyze the data. The requests' visualization per category of the financial institution also helps reveal how scammers avoid getting flagged by the banks.

Finally, we geographically locate the banks of the accounts using iban.com's API and the London Borough of Camden council's website [29]. These two services maintain a database that maps all banks to their sort codes. We lever-

[7] This includes numbers provided by the threat intelligence company.

age these to obtain the accounts' associated bank and the branch name. We then manually search for the location of the branches through the bank's branch finder website and use postcodes.io's API to get their coordinates.

Network Analysis. Different scammers' mobile numbers provide us with duplicate mule accounts, and some provide multiple ones. To identify the possible scammer communities, we follow the methodology to group mobile numbers by Christin et al. [23]. We define an undirected graph $G = (V, E)$. We create a vertex $v \in V$ for each mule account and scammer mobile number that provides a mule account. Then, we connect each vertex of the mule account with the vertex of the scammer mobile number that provided the respective mule accounts with an edge $e \in E$. We remove the 'singletons,' i.e., connected subgraphs containing at most two nodes. These singletons represent one mule account and one scammer mobile number that we cannot connect to any other scammer mobile number. To this end, we plot a graph with 334 mule accounts provided by 136 scammer mobile numbers.

3.4 Ethical Considerations

There are some ethical concerns related to this work. Obtaining informed consent for scammer interaction research is not possible. Instead, we can view this work through the light of the beneficence principle and make a risk-benefit assessment. We note that the use of deception in cybercrime research is discussed in the Menlo report [33], which considers the use of deception for research purposes. Following the Belmont report [52], we determine that the risks to any stakeholder are negligible and have broader societal benefits. As a societal benefit, interacting with scammers helps waste their time and resources [86]. Additionally, our research provides an understanding of the ecosystem that will allow the stakeholders to tackle this cybercrime.

We perform data protection impact assessments to minimize risks. The mobile network operator ensures that the data feed contains no personally identifiable information and authorizes us to contact the suspected scammers. We manually exclude false positives. Our collaborator provides the virtual mobile numbers used to interact with scammers and cannot be associated with any individual or organization. We quarantine the numbers for at least six months after the research. We only send three text messages to every identified scammer number from different mobile numbers pretending to be mum, dad, or none to answer one of the identified research questions. We do not impersonate anyone while pretending to be victims. The research is overseen by UK government agencies such as the UK Home Office and the National Crime Agency. We communicated our insights to the DCPCU of the City of London Police. The department's research ethics committee evaluated our assessment, which provided an exemption for this study given the mitigations and principles followed.

4 Measurement and Analysis

In this section, we provide a detailed analysis of the 'hi mum and dad' SMS scam to answer RQ1-5 (see §1). We present novel insights into how scammers abuse mobile network operators and financial institutions to conduct such campaigns.

4.1 Initial Scam Messages

The first step in the 'hi mum and dad' SMS scam is an initial message broadcast over SMS. We refer the reader to §2 for an overview of how scammers get access to victims' phone numbers. We received 3,402 initial 'hi mum and dad' SMS scam messages from our collaborative UK-based mobile network operator between June 20, 2023, and September 15, 2023.

We see that 83.7% (2,850 out of 3,402) original messages received from the mobile network operator reports asked the victims to contact the scammer on an online messaging platform. Scammers prefer their victims to initiate conversations on online instant messaging platforms. It is common for threat actors to use instant messaging platforms, as seen in other types of scams such as romance scams [87, 100], cryptocurrency-related scams [41], and selling illegal drugs online [60]. This aids them in hiding their traffic and geographical locations from the mobile network operators and allows them to send and receive messages from anywhere in the world without additional costs.

Addressed to	Initial messages
Mum	2,465
Dad	921
Mum and Dad (both)	16

Table 1: Distribution of initial SMS scam messages addressed to mum and dad ($n = 3,402$); scammers target mum over dad.

Targets. Table 1 shows the distribution of the token 'mum' and 'dad' in the initial message. We see that 72.5% of the initial scam messages are addressed to 'mum' whereas only 27.1% are addressed to 'dad.' It could mean that the scammers think females are more susceptible to these scams.

Lure principles. Next, we examine how scammers lure victims into replying to their initial scam messages. We identify the reasons scammers provide in Table 2 by analyzing the tokens from the initial scam messages. The scammers provide reasonable narratives describing how the mobile phone of the person they are impersonating is damaged (61.5%) or lost (6.4%). In 188 (5.5%) initial scam messages, scammers ask the potential victims to delete the existing mobile number of the person they are impersonating or mention that the old number is not in use anymore; this leads the victim to not to be able to recheck with the actual person. The remaining 721 (21.2%) messages either mention that it is the new num-

Reasons provided by scammers	Initial messages
Broke/damaged	1,228
Smash/shatter/crack/drop/crash	565
Lost/stolen	216
Down the toilet/loo/sink	214
Switched number	188
Upgraded to a new contract or device	112
Water damage	84
Changed SIM card	65
Car crash	9
No reason	721

Table 2: Distribution of reasons provided in the initial SMS scam messages to lure victims ($n = 3,402$).

ber of the person they are impersonating or that they do not have access to their phone without providing any reason. We also uncover 29 messages which ask the victims to call, indicating that some scammers are ready to communicate and impersonate over a voice call[8].

Principles	Definitions
Kindness	The scammer impersonates a family member so the users will be willing to help.
Distraction	The scammer provides various reasons to distract the users.
Time	The scammer puts time pressure on users so they make a rushed decision.

Table 3: Definition of three scam lure types using Stajano and Wilson's typology [88].

Following Stajano and Wilson's lure principles [88], we find that all scammers use *distraction* and *kindness* principles (Table 3). Table 1 shows that scammers always address their mum or dad in the messages, explain why they are messaging from a different mobile number, and ask for a financial favor. The scammers take advantage of the potential victim, i.e., a parent who would ensure their child does not go through stress and trouble with bill payments, especially when their phone is not working, and fall prey to this scam. We also find that 749 messages contain urgency cues with words such as 'urgently,' 'quickly,' 'important,' 'now,' 'ASAP,' and 'soon,' pointing to the *time* principle as one of the lure types being used to rush the users into making an impulsive decision.

Takeaway. This subsection addresses **RQ1** by highlighting that scammers target female victims. We also find that scammers use distraction, kindness, and time principles to lure victims into replying to their messages, addressing **RQ2**.

[8]Voice scams impersonating family members, maybe by using AI, are on the rise, as the FTC warns [76]. These scams often target the elderly who might be prone to pretend to recognize the user to mask deficiencies [16].

4.2 Understanding Scammer Interactions

We build on the insights we obtained in the previous subsection to understand the lure mechanisms in further stages of the scam. We send out new initial messages daily after receiving our new feed for a total of 859 unique numbers reached out to as well as continuing old conversations.

Platforms	Profiles	Mobiles used	Scammers contacted	Responses received	Response rate
SMS	Mum	10	881	116	13.17%
	Dad	10	514	63	12.26%
	No label	10	419	52	12.41%
Online Messaging	-	100	2,313	167	7.22%

Table 4: Number of unique scammers ($n = 859$, $m = 2313$) contacted per profile and the initial responses received ($n = 231$, $m = 167$) over SMS and online messaging platforms; the response rate is similar in all three cases over SMS and better compared to the online messaging platform ($p > 0.05$ using proportion test).

First, after observing that scammers tend to target mums in their initial scam message attempts, we want to confirm whether they continue to prioritize messages when receiving a follow-up from a victim based on the type of victim. To this end, we send one message from three different profiles (mum/dad/no label). Table 4 shows that the response rate of the scammers is almost the same for mum, dad, and an unspecified label. We also see that attackers use the content of our reply to follow up on their scam, suggesting that their initial message was sent to multiple recipients and they lack context when they receive the first response from a victim. Where we explicitly mention mum or dad, the scammers will use this in their subsequent messages to target the response. In the absence of context, scammers will provide a neutral response while trying to progress the scam to the next stage.

Since the scammers did not send us the original scam message, receiving a response confirms that they do not verify they are interacting with a phone number that has been previously targeted. This is intuitive given the existing dependencies in the commoditization of cybercrime [93], whereby initial messages may be sent by a different actor altogether (e.g., spammer) hired in an underground forum. Our work is the first to study this scam, so we do not have a baseline. However, we consider the initial response rate reasonable because we interact promptly with scammers despite their frequently changing mobile numbers to avoid being shut down by law enforcement and communicating with multiple potential victims at any given time.

Next, we thematically analyze the scammers' responses to understand how they lure the victims. Fig. 5 presents the top fifteen popular unigrams scammers use in their first three responses. We refer the reader to the heatmap for an analysis of the bigrams. We next analyze the different themes we observe in the three subsequent stages of a conversation.

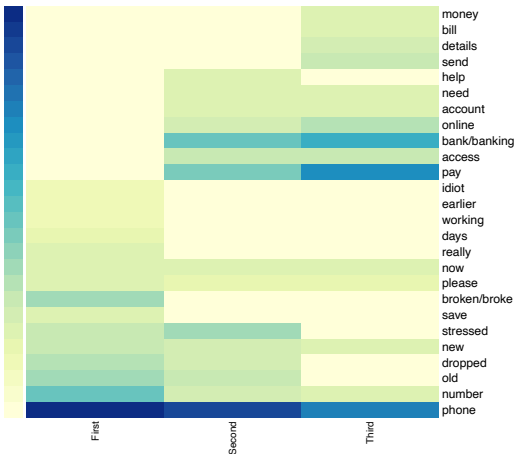


Figure 5: Fifteen most popular Unigrams from the first three scammers' responses ($n = 26$); the words 'mum,' 'dad,' 'one,' and 'yes' are excluded.

First Response. In this, scammers convince the victim that they 'broke' their 'phone' and show emotions like being an 'idiot' or 'stressed' attempting to act distressed or frustrated to gain sympathy, mapping to the *distraction* and *kindness* lure principles. They ask the potential victim to 'save' their 'new number' so the victim cannot crosscheck with the person being impersonated and mention that they are reaching out from a 'new' or a 'temporary number.'

Second Response. Scammers continue to convince and express emotions like 'stressed' abusing the kindness of the victims at this stage. They shift the conversation by asking for 'help' to 'pay' as they cannot 'access' their 'online bank accounts.' These themes relate to the *kindness* lure principle.

Third Response. The scammer stops using emotional keywords and smoothly shifts focus to the financial angle of the scheme. They reassure the victim *consistently* about being unable to access their 'online banking,' requesting to make the payment urgently and confirming with the victim if they can send the 'bank account details' to transfer the 'money.'

Scammers continue to use the words 'now' and 'please' throughout the conversation to lure the victims through the *kindness* and *time* principles so the victim would make the impulsive decision to send the money. Scammers also convince the victims by promising to return the money as soon as their mobile is fixed and they regain access to their online banking. For example,

> ... i will pay you back when i got my phone fixed Thankyouu x
>
> ... I promise I'll send every penny back then xx.

Finally, to identify when the scammers are active during the time and day of the week, we plot the scammers' responses' time of the day per week in Fig. 6. We notice that most scammers are active between 10:00-15:00 UK time on weekdays (with medians: Mon - 13:11:18, Tues - 13:30:51, Wed - 13:41:02, Thurs - 12:18:19, Fri - 11:51:41). These are the times when a victim would be comparatively more busy in a typical work setting and might not take rational decisions. This shows that scammers are likely based in the UK [97] or engage with victims according to the UK timezone. The distribution of scammers' active time for each weekday is different. The p-value for the two-sample Kolmogorov-Smirnov test for all weekday combinations is significant ($p < 0.05$). As we do not interact with scammers over the weekends, we received only 21 messages (18 on Saturdays and 3 on Sundays).

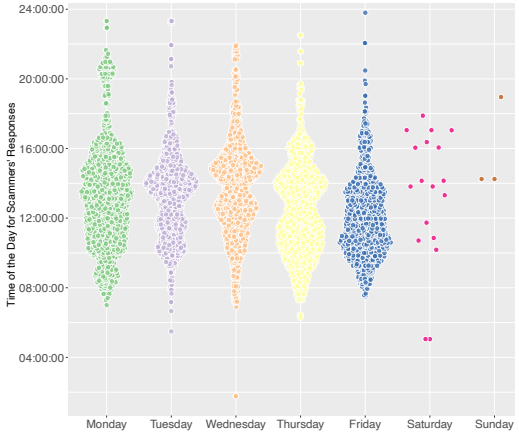


Figure 6: Time of the day per week when scammers respond to our messages ($n = 5768$). The pair-wise two-sample KS test is significant with $p < 0.05$.

Takeaway. While we demonstrate in §4.1 that scammers target female victims, the response rate in Table 4 suggests that scammers engage with both female and male victims equally, addressing **RQ1**. This shows that scammers want to deceive the victim into sending money regardless of gender. Adding on to **RQ2**, Fig. 6 points out that scammers use the distraction principle by engaging with victims during a busy work week.

4.3 Mobile Numbers

The sender ID of the initial SMS scam message is called the *originating sender ID mobile number*. Scammers ask the victims to reply to another mobile number provided in the initial scam messages. We refer to this as the *scammer mobile number*. In this subsection, we present the mobile network operators that scammers abuse for this scam campaign and analyze the lifetime of the mobile numbers.

4.3.1 Mobile Network Attribution

Mobile network operators are one of the main stakeholders that scammers abuse to run the 'hi mum and dad' scam. Ta-

ble 5 presents the 14 different mobile network operators.[9] Comparing the originating sender ID mobile number with the mobile number used to continue the conversation (scammer's mobile number), we find that they differ 72.7% (498/685) of the time. We also observe that 59.6% (408/685) of the time, the scammer's mobile number and the originating sender ID mobile number have the same (*continuing*) mobile network operator, pointing out that scammers do have a preference for the mobile network operator. Scammers employ two distinct types of mobile numbers to enhance the resilience of their campaigns against anti-abuse mechanisms implemented by mobile network operators. Mobile network operators detect when phones send a large number of initial scam messages and might block those numbers, but they do not deep-inspect the messages in the look for the second type of numbers (what we call scammer's mobile numbers). Thus, after receiving the initial message, victims may continue to engage with scammers even when the originating number is blocked.

Looking at the breakdown among mobile network operators in Table 5, we see that 67.1% of the originating sender ID mobile numbers belong to MNO 1, and 23.5% to MNO 2. We identify that scammers largely abuse MNO 1 to conduct this scam, followed by MNO 2 and MNO 3, answering RQ3. The SIM cards provided by MNO 1, 2, and 3 support the GSM technology required by a SIM box/bank, and we attribute their popularity to this fact. Scammers abuse SIM boxes/banks to broadcast an enormous amount of the initial scam messages and have multiple conversations simultaneously. An arrest by the Dedicated Card and Payment Crime Unit in the UK in June 2023 shows that the suspected criminals of 'hi mum and dad' scams use SIM boxes [97]. There could be other potential factors that might influence scammers' preference towards the particular mobile network operators. The services of the mobile network operator might be more available in the areas where the scammers are based or otherwise it might be easier and more cost-effective to procure their SIM cards. Alternatively, the filters of the mobile network operator may not be able to detect the outgoing scam messages on their services in real time.

Surprisingly, we see a landline and a pager number as two originating sender ID mobile numbers. This is probably because the scammers spoofed these two sender IDs without checking to send the initial scam message.

4.3.2 Lifetime of Mobile Numbers

We run HLR lookups and find that 127 mobile numbers became active after being inactive for awhile, i.e., changed their availability status from ABSENT_SUBSCRIBER to LIVE. This change means that scammers switch off their devices or remove SIM cards and reuse them to send the initial scam messages and/or interact with the victims. While 628 numbers were inactive for the entire period, 271 unique numbers remain LIVE as of 15 September 2023. We ignore the queries where the HLR lookup returned INCONCLUSIVE.

[9]We refrain from naming mobile network operators specifically in compliance with the confidential agreement we have with our partners.

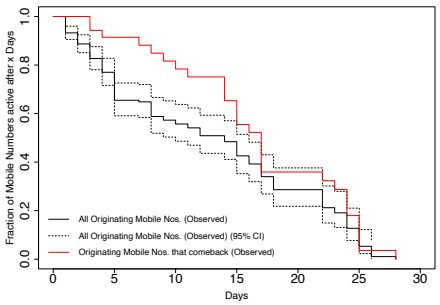
Mobile Network Operators	Type	SMS			Online Messaging	
		Originating	Scammer	Continuing	Originating	Scammer
		mobile phone numbers			*mobile phone numbers*	
MNO 1	Physical	326	601	321	-	96
MNO 2	Physical	114	272	76	-	30
MNO 3	Physical	23	150	8	-	22
MNO 4	Physical	8	81	2	-	14
MNO 5	Physical (MVNO)	1	18	0	-	3
MNO 6	Virtual	4	8	0	-	0
MNO 7	Virtual	0	8	0	-	2
MNO 8	Physical (MVNO)	10	4	1	-	0
MNO 9	Virtual	0	1	0	-	0
MNO 10	Virtual	0	1	0	-	0
MNO 11	Virtual	0	1	0	-	0
MNO 12	Virtual	0	1	0	-	0
MNO 13	Pager	0	1	0	-	0
MNO 14	Landline	0	1	0	-	0
Total		486	1,148	408		167

Table 5: Original mobile network operator distribution of originating sender ID mobile numbers, scammer mobile numbers, and continuing mobile numbers over SMS and online messaging platforms; MNO1 is the most abused.

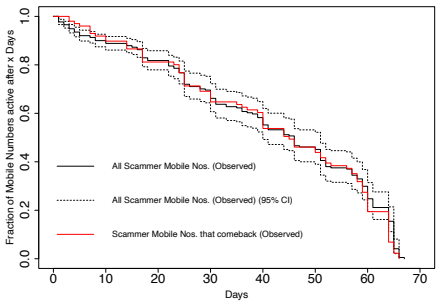
We study the lifetime of mobile numbers to understand how long scammers have used the same mobile number to scam their victims. We plot a survival curve to visualize the lifetime of the mobile numbers with overall survival probability in Fig. 7. The dotted lines in the plot are the 95% confidence interval. The red line shows the survival probability for mobile numbers that became active after being inactive (comeback).

Thomas et al. demonstrated that the median lifetime of phone numbers tied to abuse is less than one hour [94]. In comparison, our research finds that the median lifetime of originating sender ID mobile numbers abused to send initial 'hi mum and dad' scams is 14 days. Whereas the scammer's mobile numbers used to interact with the victims have a median lifetime of 46 days. While 88.7% of originating sender ID mobile numbers are active after two days, 42.6% remain active after 15 days. On the other hand, 96.6% scammer mobile numbers are active after two days, and 87.3% remain active after 15 days. This shows that the mobile network operators are unable to confirm when mobile numbers are sending 'hi mum and dad' SMS scam messages in the early stages of the campaign and cannot swiftly block these numbers. Blocking mobile numbers within a day would be highly effective, as potential victims would not be able to reply to the scammer's mobile number present in the initial scam message, protecting them from being lured.

Takeaway. This subsection addresses **RQ3** by indicating that scammers prefer MNO 1 followed by MNO 2 and MNO 3, likely because they support GSM required by SIM boxes. We also identify the median lifetime of the originating sender ID and scammer mobile numbers as 14 days and 46 days, respectively, evidencing how long affected numbers are currently used, also addressing **RQ3**.



(a) Survival analysis of originating sender ID mobile numbers lifetime ($n = 486$) along with the mobile numbers that become active after being inactive ($n = 35$); comeback numbers follow a similar trend ($p = 0.05$ using a log-rank test of difference).



(b) Survival analysis of scammer mobile numbers lifetime ($n = 1,184$) along with the mobile numbers that become active after being inactive ($n = 101$); comeback numbers follow a similar trend ($p = 0.2$ using a log-rank test of difference).

Figure 7: Survival analysis of mobile numbers lifetime along with the mobile numbers that become active after being inactive; more than 55% originating sender ID mobile numbers and over 88% scammer mobile numbers survive for over 10 days.

4.4 Mule Accounts

In 'hi mum and dad' scams, scammers use multiple financial institutions' accounts that do not belong to them. These accounts are termed mule accounts as they are used to receive money from the victims. These can be witting [27] or unwitting [31]. If the account owner is unaware then only banks can investigate. Mules later re-transfer these illicit funds to the scammers.

During 13 weeks of interactions, 270 unique scammer mobile numbers provided us with 582 unique mule accounts[10] over SMS and an online messaging platform (cf. Table 9 in the Appendix). During the interactions, we convinced the scammers about the unsuccessful transfers to the mule account provided and requested alternative accounts until they stopped replying. This engagement helped us collect multiple mule accounts per phone, ranging between one and twelve, with a median of two mule accounts. We found four mule accounts belonging to companies registered in the UK.

Table 6 presents the distribution of all transaction requests. We see that the minimum and maximum values are similar, but the median requested amount over the online messaging platform is higher than over SMS. This suggests that scammers have different preferences over different venues (perhaps due to perceived differences in ability to pay or different scam operations targeting different communication vectors). The average amount requested in this scam is 5 times more than in technical support scams [53]. We aggregate all 564 unique transaction requests from the scammers, resulting in a total amount of £577,792.

Once we collect a corpus of mule accounts, we seek to understand the various types of financial institutions abused in this scam.[11] This understanding helps in recognizing fraudulent activities that might target specific customer demographics. We use the UK FCA handbook to create a taxonomy of various identified financial institutions, as shown in Table 7. The number of accounts leveraging electronic money institutions (EMIs) is significantly higher than others, almost double the number of accounts in high street banks. This could be because (1) EMIs provide entirely online services, and mules might find it easy to open and operate these accounts via apps; (2) it is more convenient for users to transfer money using EMIs; (3) the transaction requests may not get flagged by the bank, allowing them to reuse mule accounts.

Platform	Median	Mean	Min.	Max.	Requests
SMS	880	1,102	100	5,924	344
Online Messaging	1,244	1,453	180	6,000	220
Total		*£577,792*			564

Table 6: Distribution of all transaction requests (£).

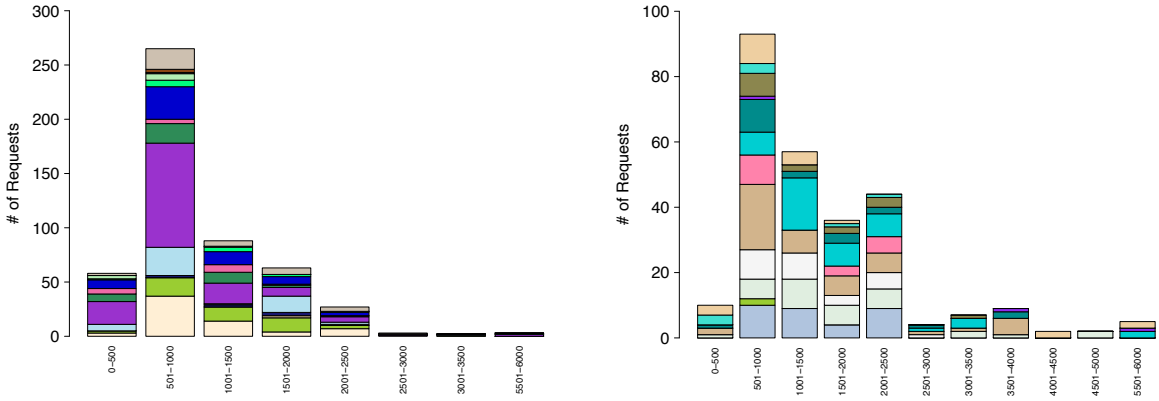
Category	Financial institutions	Mule accounts (unique)
Electronic Money Institution	14	374
High Street	12	196
EEA Authorised (International)	2	6
Authorised Payment Institution	5	5
Small Electronic Money	1	1

Table 7: Distribution of unique mule accounts ($n = 582$) aggregated with their respective category of financial institutions ($n = 34$) as per the UK's FCA handbook [13].

To examine whether the scammers have also identified the transaction amounts that the EMIs or high street banks allow without flagging, we explore the range of amounts requested

[10] We report all mule accounts to the respective banks and request them to investigate.

[11] We refrain from naming them specifically in compliance with the confidential agreement we have with our partners.



(a) Electronic money inst. ($n = 14$) transaction req. ($n = 509$). (b) High street banks ($n = 12$) transaction requests ($n = 269$).

Figure 8: Distribution of amounts (£) scammers request into electronic money institutions (EMIs) and high street banks per transaction. The different colors represent the different institutions in that category. EMIs have only 8 requests above £2,500 compared to 29 requests above £2,500 into high street banks.

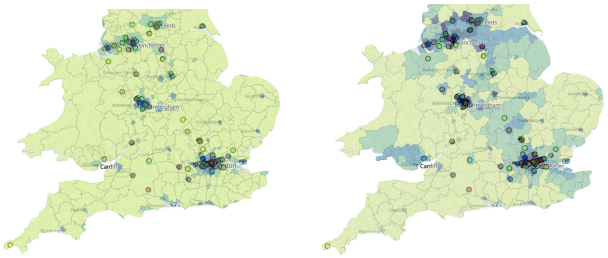
in Fig. 8. We see that 79% (403/509) of the transaction requests to mule accounts in EMIs are less than £1,500 compared to 59% (158/269) of the transaction requests to mule accounts in high street banks. The most common range is £501-£1,000 for both. While we received only eight requests worth more than £2,500 to mule accounts in EMIs, we received 29 such transaction requests to mule accounts in High Street banks. This likely points to EMIs flagging transactions above £2,500, so scammers prefer to use particular high street banks for high-value requests, answering **RQ4**. Scammers reported difficulties receiving transactions above £2,500 due to a bank warning sent to their customers after we interacted with one pretending to be a reporter.

4.4.1 Geo-locating Mule Accounts

High street banks are the only category with physical branches in most cities, providing facilities for opening a bank account or executing transactions in person, to name a few. We plot the coordinates of the 96 mule accounts associated with a physical branch in the UK in Fig. 9. The different colors represent the 12 high street banks.

We query the population density and unemployment rates from the UK Office for National Statistics and overlay the location of high street banks that mules use over a map. The concentration of the mule accounts follows the population density and the unemployment history of people aged 16 years or above in the UK as shown in Figs. 9a and 9b respectively.

There is a possibility that people living in cities with higher density populations and unemployment rates are more prone to becoming money mules [11]. However, there are some outliers. For example, we see mules around Wiltshire and Cornwall, areas with no significant unemployment rates. Our findings could help law enforcement devise targeted interventions in these areas (see potential mitigations in §5.2).



(a) Population Density (b) Unemployment Rates

Figure 9: Distribution of the identified mule accounts ($n = 96$) in high street banks ($n = 12$) follows the population density and unemployment rates in the UK. The different colored circles represent 12 different high street banks.

Takeaway. This section addresses **RQ4**. Fig. 8 indicates that scammers evade detection by financial institutions by determining transaction amounts that would not trigger alerts. They provide suspect mule accounts of high-street banks for higher-value requests.

4.5 Identifying Scammer Networks

We observe that different scammers' mobile numbers provide us with duplicate mule accounts. This indicates that multiple scammers abuse the same mule account, or they tend to work in groups, as discussed by work in other types of scams [82]. To identify possible groups of threat actors working together, we create a network graph shown in Fig. 10. Via this network graph, we identify six communities with four or more scammer mobile numbers connected, answering RQ5.

Groups 1, 2, 5, and 6 from Table 8 constitute mule accounts from electronic money institutions (EMIs) and high street banks. On the other hand, Groups 3 and 4 contain mule

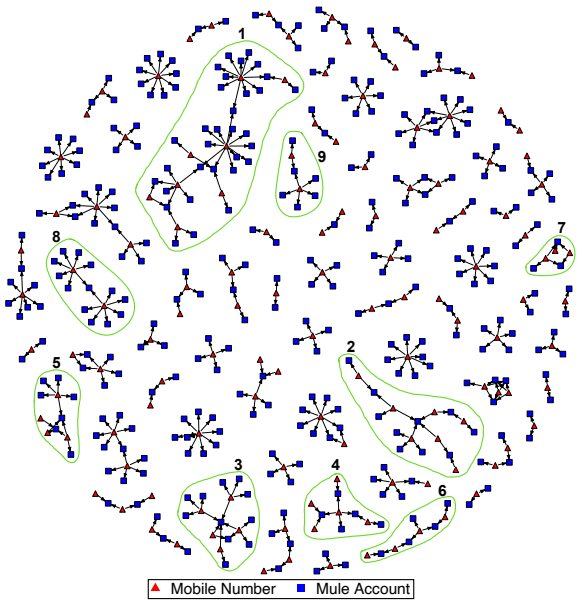


Figure 10: Network graph of nodes representing scammers' mobile numbers ($n = 136$) and mule accounts ($n = 334$). We identify six communities with four or more scammer mobile numbers. Three additional communities request more than £10k each.

Group	Scammer mobile phone numbers	Mule Accounts	Financial institutions	Amount requested (£)
1	8	31	8	41,125
2	7	10	7	14,487
3	5	11	4	9,452
4	5	5	5	11,400
5	4	7	6	14,231
6	4	5	4	11,728
7	3	3	3	18,000
8	2	13	7	10,700
9	2	6	6	10,965

Table 8: Breakdown of amounts requested (round-off to nearest decimal) by the nine communities identified in Fig. 10.

accounts from EMIs only. The requested amount indicates that groups with only EMIs request less amount compared to the ones with both EMIs and high street banks. Group 1 has considerably more mule accounts and the amount requested because we interacted with two scammer mobile numbers for a longer time.

Furthermore, we identify three communities (Groups 7, 8, and 9) that request more than £10k. Group 7 comprises only high street banks' mule accounts with more than £3,500 requested for each transaction. However, Groups 8 and 9 also include one or two mule accounts belonging to EMIs. Group 8 only contains transaction requests above £2,100, whereas Group 9 has requests between £1,300 and £3,500. This also supports that groups with only high street banks request more money than the ones with both EMIs and high street banks. We are limited by some scammers who may not provide all the mule accounts they can access, which would make the network sparser.

Takeaway. Towards **RQ5**, this subsection presents Fig. 10, demonstrating six criminal networks with four or more scammer mobile numbers. We identify three additional smaller criminal networks, each requesting over £10k, significantly more than the others.

5 Discussion

We next discuss the findings, limitations, and mitigations we derive from our analysis of the 'hi mum and dad' scam.

5.1 Findings, Implications, and Limitations

Scammers use kindness, distraction, and time lure principles. While the financial and authoritative principles are mostly used in cryptocurrency investment scams [5, 84], the financial principle in 419 scams and the authoritative principle in phishing [36, 98], we identify a different subset of lures (kindness and distraction) that is prominent in this scam. Verifying the intended recipient of a message can be challenging, especially since sender IDs are susceptible to spoofing. Furthermore, calling individuals directly for identity confirmation may not always be feasible, or the scammers may prevent it using an effective lure. Hence, an understanding of the lures scammers use is necessary.

Scammers prefer mobile network operators that SIM boxes/banks support. SIM boxes/banks allow automation and simultaneously broadcast messages, but they require GSM support. Scammers prefer mobile network operators that offer this support. This indicates that scammers likely have such equipment, a key to targeting a broader population. While Singapore and a few mobile network operators in the USA and Australia shut the GSM services entirely in 2017 [12, 65, 81], the UK expects to phase out by 2033 [62]. This means that scammers could potentially abuse SIM boxes for another decade.

A lucrative profit center responsible for massive financial losses. There is currently no annual report of losses to victims in the UK due to this threat. Besides, cybercrime loss numbers are notoriously full of noise [9, 10]. Towards this end, we attempt to estimate the losses using both our data and data reported to the UK government agency, Action Fraud, which collects data on online fraud. Both data sources are necessarily imperfect. We only have response requests from the scammers we manually interacted with during a limited scope of time. We know that most victims who reach this stage likely go through with the scam from work in other fraud, but cannot prove this empirically for this scam [101]. Alternatively, many victims in the UK would report Authorized Push Payment (APP) scams to their respective banks

instead of Action Fraud. Fraud, in general, is significantly under-reported to the authorities [83].

As per Action Fraud, victims in 2022 lost £1.5*m* in less than 20 weeks (∼£3.9*m*/year) [78] and £500*k* in 17 weeks in 2023 (∼£1.53*m*/year) [24]. During the 13 weeks of our research, we received transaction requests worth £577,792 from the scammers. Extrapolating to a 52 week period, we can estimate that the minimum annual financial loss to the victims is at least £2.3*m* in the UK. Annual losses in Australia in 2022 because of this scam resulted in over $7.2*m* (∼£3.8*m*) [14]. 95 reports in Spain amounted to over €410*k* (∼£352*k*) [45]. Considering all of this, we believe the estimate of £2.3*m* per year across the UK derived from our data is reasonable.

This amount is expected to grow as the scam progresses. The scammer requires a minimal investment to run this campaign, earning a direct profit. They may inject this money into other scams or profit centers [93]. APP fraud was nonexistent a decade ago and has grown to £236*m* by 2019 [9, 10]. Our work adds a new category in APP fraud, and the minimum losses mentioned above increase the previously calculated cost of this crime.

Informal discussions with stakeholders indicate young mules. We discuss our findings with stakeholders to understand this scam better. They indicate that most mule accounts we report belong to adults aged 15-21. Previous research [11, 19], banks [27] and law enforcement [35] also mention similar age groups of money mules.

Mule recruitment and the UK Companies House. Money mules are essential for the scammers to receive funds from the victims. While in some cases, money mules wittingly take part in the scam [27], benefiting from commissions, in others, they are themselves victims of a larger scam [31] (e.g., work-from-home job scams). They are recruited through online advertisements, recruitment websites [1, 31, 42, 56] or approached in person [35].

We do not know if there is a separate entity that provides mule accounts to scammers [42] or if they recruit mules themselves. Until the new UK company law [43], the UK Companies House did not verify the data provided by the registrants. This allowed the scammers to abuse the UK Companies House, similar to online Ponzi schemes [7]. Further research is required to investigate how threat actors and mules abuse company registration in the UK.

We investigate a latent threat with a profound impact. As per UK Finance, more than 28*k* victims fell for impersonation scams [37]. On the other hand, the NFIB and Action Fraud received only 414 reports in the first five months of 2023 of 'hi mum and dad' SMS scams [24]. Considering the number of scammer interactions in our research, this scam is likely under-reported [17]. The UK Office for National Statistics notes that fewer than one in seven fraud offenses are reported to law enforcement [40]. We make an in-depth analysis of the various stages of this scam life cycle for the first time. Our findings constitute a crucial step forward towards the understanding of this scam.

Limitations. We receive 'hi mum and dad' scam reports from only one mobile network operator in the UK. Access to all UK mobile network operators data would provide an accurate distribution of the originating sender ID and scammer mobile network operators. We interact with the scammers during working hours in the UK and not 24/7, which might have reduced some scammers' responses. Even though scammers prefer an online messaging platform, they actively engage over SMS and provide mule accounts. Despite the limitations of our research, we present the first measurement of the ecosystem surrounding 'hi mum and dad' scams, shedding light on the services exploited by scammers to perpetrate this fraudulent activity.

5.2 Potential Mitigations

We derive mitigations from our findings across three complementary axes, as we discuss next.

Educational. The current awareness programs focus on university students [74]. As we find from the stakeholders' informal interviews, mules' ages are between 15 and 21, so these programs must extend to high schools. Users of messaging applications should be made aware of the lures identified to stop them from falling prey to such scams. The areas we pinpoint in our geo-location analysis can assist in identifying regions where education awareness campaigns are necessary.

Technical measures. Faster reporting is required to shut down the numbers scammers abuse. Investigating SMS scams is more challenging than emails due to metadata unavailability. Mobile network operators should collaborate with other stakeholders to include metadata in the SMS protocol. GSM support should be disabled by default, and checks should be enforced to enable it. Deep inspecting SMSs could help identify and block scammer mobile numbers. However, this would raise privacy concerns, and scammers may abuse this with adversarial attacks. Online messaging platforms should implement better scam detection algorithms and work with mobile network operators and financial institutions for scammer takedowns. Scammers can identify the maximum amounts financial institutions allow without flagging transactions. Institutions should enhance their fraud detection and prevention mechanisms and collaborate with mobile network operators to find connections to block scammers. As fraud constitutes 40% of all crime in the UK [63], there is an urgent need for a universal reporting system categorized by fraud type.

Law and regulatory frameworks. The telecom regulators should mandate the mobile network operators to implement privacy-preserving Know Your Customer (KYC) checks before issuing pay-as-you-go mobile numbers. Even though SIM boxes/banks are banned by the UK government [64], scammers still access and use them. Law enforcement should

work with mobile network operators to detect and confiscate such devices. Committing fraud offenses should be punished appropriately regardless of age to deter young adults aged 15-21 from getting involved in such activities [97].

6 Related Work

We draw upon methods used to study other phone-based scams. We conduct HLR lookups on the mobile phone numbers in a similar manner to Costin et al. who worked to understand the role of phone numbers in cybercrime [28]. We only send a message to a mobile number the first time we encounter it following from from the work of Clayton and Mansfield, who assumed little new information from redialing numbers [25]. While they redial numbers that did not pick up, we use HLR lookups to ensure we send messages only to active mobile numbers.

In order to measure SMS scams, some have collated victim reports [80, 91] or crowdsourced them [22, 95]. Others used intensive techniques like in-depth interviews [34, 77] and analyzing news articles [18]. However, our approach of personally interacting with scammers towards this fraud has allowed us to collect a sizeable set of novel data, from mule accounts to mobile numbers, about this relatively new scam with no available training data for machine learning approaches.

Our work fits in the broader literature of interaction scams; researchers investigated interactions over platforms like email [3, 15, 69], social media [3, 66], and voice [20, 53]. Some of this work automatically interacted with scammers integrating technology like ChatGPT [15]. There has been work on robocalls [72, 73], particularly in developing systems to combat them [67, 68]. Our research is the first to investigate interaction scams over mobile messaging.

SMS fraud has taken off recently, and researchers have focused on SMS spam [8, 32, 48, 91] and smishing [95]. Using spam datasets [8, 22], researchers have developed models to detect smishing messages and otherwise distinguish smishes from legitimate messages [47, 49, 54, 55, 85]. Our work focuses on a scam where victims directly interact with scammers via SMS or an online messaging platform, while previous literature considers call-back, SMS-to-email interactions, or no direct interaction (click a URL) at all.

We investigate concentrations in cybercrime, a broader research thrust coined by Clayton, Moore, and Christin [26]. They suggest working with regulators and infrastructure operators to remove this fraud at an ecosystem level [26]. This is contrasted to work which unintentionally encourages playing whack-a-mole by identifying concentrations, allocating resources to abused infrastructure operators, and then miscreants react by popping up again on other operators. Illustratively, Stone-Gross et al. investigated the payment infrastructure of fake AntiVirus scams, which resulted in this fraud disappearing [90]. Online Ponzi schemes have had multiple money systems shut down, thanks in part to the research from Moore, Han, and Clayton [58]. Noroozian et al. worked with law enforcement to take down and analyze a bulletproof hosting provider [61].

7 Conclusion

The paper unveils the ecosystem and presents the first detailed analysis of 'hi mum and dad' SMS scams. We explain how scammers lure victims into a text-back scam and estimate the minimum amount lost by victims in the UK. The findings show that this scam sits at the intersection of three sectors — banking, telecom, and tech and we leverage it to identify criminal networks. As this scam has recently evolved and continues to grow globally, automating the process of scammer interactions and expanding the research outside the UK would enable us to conduct this experiment at scale.

APP fraud has increased since 2018 and is expected to double by 2026 [4] with most value lost from telecommunication-originated cases [37]. This paper shows that criminals identify the amounts above which financial institutions raise a flag and inform their customers. We also see that the mules have a broader age range and exist in regions with scarce population density and unemployment rates. Regulators should help financial institutions identify mule accounts with better fraud detection mechanisms.

There has been a significant decline in SMS usage in the UK [89]. One factor is likely due to the surge in SMS fraud [79]. The analysis shows that scammers also abuse other platforms as they prefer victims to initiate the conversation on an online messaging platform. The mobile numbers used to run this campaign have a median lifetime of 30 days, indicating that the mobile network operators cannot confirm the abuse. Telecom regulators and law enforcement should work with mobile network operators to detect the abuse of SIM boxes and pay-as-you-go SIMs. A cross-sector collaboration with regulators, mobile network operators, and financial institutions could identify criminal networks and faster reporting to curb this cybercrime.

Acknowledgments

We thank the reviewers and anonymous shepherd for their feedback. Additionally, a very warm thank you to all the Stop Scams UK members who participated in this project. Particularly, many thanks to Mark Davis and Jack Bowerman from Stop Scams UK who helped with the data collection. G. Suarez-Tangil has been appointed as 2019 Ramon y Cajal fellow (RYC-2020-029401-I) funded by MICIU/AEI/10.13039/-501100011033 and ESF Investing in your Future. He was also supported by project PID2022-143304OB-I00 funded by MICIU/AEI/10.13039/501100011033/ and by the ERDF, EU; and TED2021-132900A-I00 funded by MICIU/AEI/10.-13039/501100011033 and the EU-NextGenerationEU/PRTR.

References

[1] Mohd Irwan Abdul Rani, Sharifah Nazatul Faiza Syed Mustapha Nazri, and Salwa Zolkaflil. A systematic literature review of money mule: Its roles, recruitment and awareness. *Journal of Financial Crime*, 2023.

[2] Jorij Abraham, Marianne Junger, Sam Cajiga, Luka Koning, Clement Njoki, and Sam Rogers. The state of scams in the United Kingdom report (2023). Technical report, GASA, 2023.

[3] Bhupendra Acharya, Muhammad Saad, Antonio Emanuele Cinà, Lea Schönherr, Hoang Dai Nguyen, Adam Oest, Phani Vadrevu, and Thorsten Holz. Conning the crypto conman: End-to-end analysis of cryptocurrency-based technical support scams. In *IEEE Symposium on Security and Privacy*, 2024.

[4] ACI Worldwide. Growth in APP Scams Expected To Double by 2026 – Report by ACI Worldwide and GlobalData. https://bit.ly/4he2N3x, 2022.

[5] Sharad Agarwal, Gilberto Atondo-Siu, Marilyne Ordekian, Alice Hutchings, Enrico Mariconti, and Marie Vasek. DeFi deception—uncovering the prevalence of rugpulls in cryptocurrency projects. In *Financial Cryptography and Data Security*, 2024.

[6] Sharad Agarwal, Emma Harvey, and Marie Vasek. Poster: A comprehensive categorization of sms scams. In *Internet Measurement Conference (IMC)*, 2024.

[7] Sharad Agarwal and Marie Vasek. Investigating the concentration of high yield investment programs in the United Kingdom. In *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 2022.

[8] Tiago A. Almeida, José María G. Hidalgo, and Akebo Yamakami. Contributions to the study of sms spam filtering: new collection and results. In *ACM Symposium on Document Engineering*, page 259–262, 2011.

[9] Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Carlos Ganán, Tom Grasso, Michael Levi, Tyler Moore, and Marie Vasek. Measuring the changing cost of cybercrime. In *Workshop on the Economics of Information Security (WEIS)*, 2019.

[10] Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Michel JG van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. Measuring the cost of cybercrime. In *Workshop on the Economics of Information Security (WEIS)*, 2013.

[11] Manuel Aston, Stephen McCombie, Ben Reardon, and Paul Watters. A preliminary profiling of internet money mules: an Australian perspective. In *Workshops on Ubiquitous, Autonomic and Trusted Computing*, 2009.

[12] AT&T. 2G Sunset Brings Faster Speeds, Newer Technologies. https://bit.ly/40xdKIc, 2017.

[13] Financial Conduct Authority. FCA Handbook. https://handbook.fca.org.uk/handbook, 2024.

[14] Jessica Bahr. 'Hi mum' scam arrest: What you need to know about text message scams. https://bit.ly/4jhPRLO, 2023.

[15] Piyush Bajaj and Matthew Edwards. Automatic scambaiting using ChatGPT. In *International Workshop on Applications of AI, Cyber Security and Economics Data Analytics*, pages 1941–1946, 2023.

[16] Silva Banovic, Lejla Junuzovic Zunic, and Osman Sinanovic. Communication difficulties as a result of dementia. *Materia socio-medica*, 30(3):221, 2018.

[17] Alex Barton. Parents warned 'hi mum' scam has spread to text messages. https://bit.ly/3PArvQ0, 2023.

[18] Marzieh Bitaab, Haehyun Cho, Adam Oest, Penghui Zhang, Zhibo Sun, Rana Pourmohamad, Doowon Kim, Tiffany Bao, Ruoyu Wang, Yan Shoshitaishvili, Adam Doupé, and Gail-Joon Ahn. Scam pandemic: How attackers exploit public fear through phishing. In *APWG Symposium on Electronic Crime Research*, 2020.

[19] Ian Brunton-Smith and Daniel J. McCarthy. Explaining young people's involvement in online piracy: An empirical assessment using the offending crime and justice survey in england and wales. *Victims & Offenders*, 11(4):509–533, 2016.

[20] J. Carrillo-Mondéjar, J.L. Martinez, and G. Suarez-Tangil. On how voip attacks foster the malicious call ecosystem. *Computers & Security*, 119:102758, 2022.

[21] Chartered Trading Standards Institute (CTSI). Whatsapp family member message scam targets public. https://bit.ly/40gCOlf, 2021.

[22] Tao Chen and Min-Yen Kan. Creating a live, public short message service corpus: the nus sms corpus. *Language Resources and Evaluation*, 47:299–335, 2013.

[23] Nicolas Christin, Sally S. Yanagihara, and Keisuke Kamataki. Dissecting one click frauds. In *ACM Conference on Computer and Communications Security*, 2010.

[24] Jess Clark and Alex Hern. 'I felt stupid and embarrassed': victim of 'hi mum' fraud on WhatsApp lost £1,600. https://bit.ly/4jce3PV, 2023.

[25] Richard Clayton and Tony Mansfield. A study of whois privacy and proxy service abuse. In *Workshop on the Economics of Information Security*, 2014.

[26] Richard Clayton, Tyler Moore, and Nicolas Christin. Concentrating correctly on cybercrime concentration. In *Workshop on the Economics of Information Security*, 2015.

[27] Patrick Collinson. Fraud: here's how scammers get away with it. https://bit.ly/4jbmiLX, 2018.

[28] Andrei Costin, Jelena Isacenkova, Marco Balduzzi, Aurélien Francillon, and Davide Balzarotti. The role of phone numbers in understanding cyber-crime schemes. In *Conference on Privacy, Security and Trust*, pages 213–220, 2013.

[29] Camden Council. United kingdom - sort code to bank branch name. https://bit.ly/4gR0OlX, 2020.

[30] European Payments Council. 2019 Payments Threats and Fraud Trends Report. https://bit.ly/3Cb9zZ3.

[31] Lorrie Faith Cranor. Can phishing be foiled? *Scientific American*, 299(6):104–111, 2008.

[32] Sarah Jane Delany, Mark Buckley, and Derek Greene. Sms spam filtering: Methods and data. *Expert Systems with Applications*, 39(10):9899–9908, 2012.

[33] David Dittrich and Erin Kenneally. The menlo report: Ethical principles guiding information and communication technology research. Technical report, US Department of Homeland Security, 2012.

[34] Julie S. Downs, Mandy B. Holbrook, and Lorrie Faith Cranor. Decision strategies and susceptibility to phishing. In *Symposium on Usable Privacy and Security*, page 79–90, 2006.

[35] Europol. Money Muling. https://bit.ly/4jgA2Fq, 2023.

[36] Ana Ferreira and Gabriele Lenzini. An analysis of social engineering principles in effective phishing. In *Workshop on Socio-Technical Aspects in Security and Trust*, 2015.

[37] UK Finance. Over £1.2 billion stolen through fraud in 2022, with nearly 80 per cent of app fraud cases starting online. https://bit.ly/3PByyaY.

[38] Finextra. Singapore banks act to tackle spate of SMS phishing scams. https://bit.ly/40y4gfC, 2022.

[39] Dinei Florêncio and Cormac Herley. Phishing and money mules. In *IEEE International Workshop on Information Forensics and Security*, 2010.

[40] Office for National Statistics (ONS). Crime in england and wales: year ending september 2023. https://bit.ly/4gRkMNH, 2024.

[41] J.T. Hamrick, Farhang Rouhi, Arghya Mukherjee, Amir Feder, Neil Gandal, Tyler Moore, and Marie Vasek. An examination of the cryptocurrency pump-and-dump ecosystem. *Information Processing & Management*, 58(4):102506, 2021.

[42] Shuang Hao, Kevin Borgolte, Nick Nikiforakis, Gianluca Stringhini, Manuel Egele, Michael Eubanks, Brian Krebs, and Giovanni Vigna. Drops for stuff: An analysis of reshipping mule scams. In *ACM Conference on Computer and Communications Security*, page 1081–1092, 2015.

[43] UK Companies House. Changes to uk company law. https://bit.ly/4agq1nn, 2023.

[44] UK Companies House. Companies house. https://bit.ly/3PAPVsu, 2024.

[45] Simon Hunter. Spain's police make 65 arrests in bust of cybercrime gang using the 'hi mum!" scam. https://bit.ly/3WGqGJx, 2024.

[46] FBI IC3. Internet Crime Report 2020. https://bit.ly/427tm6l, 2020.

[47] Ankit Kumar Jain and BB Gupta. Rule-based framework for detection of smishing messages in mobile environment. *Procedia Computer Science*, 125:617–623, 2018.

[48] Nan Jiang, Yu Jin, Ann Skudlark, and Zhi-Li Zhang. Greystar: Fast and accurate detection of SMS spam numbers in large cellular networks using gray phone space. In *USENIX Security Symposium*, 2013.

[49] Jae Woong Joo, Seo Yeon Moon, Saurabh Singh, and Jong Hyuk Park. S-detector: an enhanced security model for detecting smishing attack for mobile computing. *Telecommunication Systems*, 66:29–38, 2017.

[50] Edward L Kaplan and Paul Meier. Nonparametric estimation from incomplete observations. *Journal of the American statistical association*, 1958.

[51] Adam Mcneil. Trash talk: Pig butchering and conversational attacks were the fastest growing mobile threats of 2022. https://bit.ly/3WhxhtI, 2022.

[52] Vickie A Miracle. The belmont report: The triple crown of research ethics. *Dimensions of critical care nursing*, 35(4):223–228, 2016.

[53] Najmeh Miramirkhani, Oleksii Starov, and Nick Nikiforakis. Dial one for scam: A large-scale analysis of technical support scams. *Network and Distributed System Security (NDSS) Symposium*, 2017.

[54] Sandhya Mishra and Devpriya Soni. Smishing detector: A security model to detect smishing through sms content analysis and url behavior analysis. *Future Generation Computer Systems*, 108:803–815, 2020.

[55] Sandhya Mishra and Devpriya Soni. DSmishSMS–a system to detect smishing SMS. *Neural Computing and Applications*, 35(7):1–18, 2023.

[56] Tyler Moore and Richard Clayton. The impact of incentives on notice and take-down. In *Managing Information Risk and the Economics of Security*, 2008.

[57] Tyler Moore, Richard Clayton, and Ross Anderson. The economics of online crime. *Journal of Economic Perspectives*, 23(3):3–20, September 2009.

[58] Tyler Moore, Jie Han, and Richard Clayton. The postmodern Ponzi scheme: Empirical analysis of high-yield investment programs. In *Financial Cryptography and Data Security*, pages 41–56, 2012.

[59] David Morris. What is a HLR Lookup? https://bit.ly/428FyDV, 2021.

[60] Leah Moyle, Andrew Childs, Ross Coomber, and Monica J Barratt. # drugsforsale: An exploration of the use of social media and encrypted messaging apps to supply and access drugs. *International Journal of Drug Policy*, 63:101–110, 2019.

[61] Arman Noroozian, Jan Koenders, Eelco van Veldhuizen, Carlos H. Gañán, Sumayah Alrwais, Damon McCoy, and Michel van Eeten. Platforms in everything: Analyzing Ground-Truth data on the anatomy and economics of Bullet-Proof hosting. In *USENIX Security Symposium*, pages 1341–1356, August 2019.

[62] Ofcom. 3G and 2G switch-off. https://bit.ly/40iHcQV, 2023.

[63] UK Home Office. Online Fraud Charter 2023 (accessible). https://bit.ly/4fSh0C9, 2023.

[64] UK Home Office. Preventing the use of SIM farms for fraud: government response (accessible). https://bit.ly/40woPcg, Nov 2023.

[65] Optus. Optus to complete 2G network turn off. https://bit.ly/4afD6NQ, 2017.

[66] Marilyne Ordekian, Antonis Papasavva, Enrico Mariconti, and Marie Vasek. A sinister fattening: Dissecting the tales of pig butchering and other cryptocurrency scams. In *APWG Symposium on Electronic Crime Research*, 2024.

[67] Sharbani Pandit, Jienan Liu, Roberto Perdisci, and Mustaque Ahamad. Applying deep learning to combat mass robocalls. In *IEEE Security and Privacy Workshops*, pages 63–70, 2021.

[68] Sharbani Pandit, Krishanu Sarker, Roberto Perdisci, Mustaque Ahamad, and Diyi Yang. Combating robocalls with phone virtual assistant mediated interaction. In *3USENIX Security Symposium*, 2023.

[69] Youngsam Park, Jackie Jones, Damon McCoy, Elaine Shi, and Markus Jakobsson. Scambaiter: Understanding targeted nigerian scams on craigslist. *system*, 1:2, 2014.

[70] PayUK. Bacs Payment System. https://bit.ly/4hx9NJh, 2023.

[71] PayUK. Faster Payment System. https://bit.ly/3DV4zZ6, 2023.

[72] Sathvik Prasad, Elijah Bouma-Sims, Athishay Kiran Mylappan, and Bradley Reaves. Who's calling? characterizing robocalls through audio and metadata analysis. In *USENIX Security Symposium*, pages 397–414, 2020.

[73] Sathvik Prasad, Trevor Dunlap, Alexander Ross, and Bradley Reaves. Diving into robocall content with SnorCall. In *USENIX Security Symposium*, 2023.

[74] Underworld TV Production. New figures reveal 3 in 5 students have been targeted by criminals to become money mules. https://bit.ly/40jfymL, 2023.

[75] Proofpoint. The Human Factor 2022. https://bit.ly/4haqv0H, 2022.

[76] Alvaro Puig. Scammers use ai to enhance their family emergency schemes. https://bit.ly/3DSekau, 2023.

[77] Md Lutfor Rahman, Daniel Timko, Hamid Wali, and Ajaya Neupane. Users really do respond to smishing. In *ACM Conference on Data and Application Security and Privacy*, page 49–60, 2023.

[78] Tali Ramsey. Notorious 'Hi Mum and Dad' scam spreads from WhatsApp to text message. https://bit.ly/4ak4hY4, 2022.

[79] Markus Riek, Rainer Böhme, and Tyler Moore. Measuring the influence of perceived cybercrime risk on online service avoidance. *IEEE Transactions on Dependable and Secure Computing*, 13(2):261–273, 2015.

[80] Sayak Saha Roy, Unique Karanjit, and Shirin Nilizadeh. Evaluating the effectiveness of phishing reports on twitter. In *APWG Symposium on Electronic Crime Research (eCrime)*, 2021.

[81] Andrew Sadauskas. Telstra says goodbye to 2g. https://bit.ly/3DXxk7G, 2016.

[82] Hamed Sarvari, Ehab Abozinadah, Alex Mbaziira, and Damon Mccoy. Constructing and analyzing criminal networks. In *IEEE Security and Privacy Workshops*, pages 84–91, 2014.

[83] Alex Scroxton. Fraud and cyber crime still vastly under-reported. https://bit.ly/4fYuEE7, 2021.

[84] Gilberto Atondo Siu, Alice Hutchings, Marie Vasek, and Tyler Moore. "Invest in crypto!": An analysis of investment scam advertisements found in bitcointalk. In *APWG Symposium on Electronic Crime Research*, 2022.

[85] Gunikhan Sonowal and KS Kuppusamy. SmiDCA: an anti-smishing model with machine learning approach. *The Computer Journal*, 61(8):1143–1157, 2018.

[86] Tom Sorell. Scambaiting on the spectrum of digilantism. *Criminal Justice Ethics*, 38(3):153–175, 2019.

[87] Tom Sorell and Monica Whitty. Online romance scams and victimhood. *Security Journal*, 32:342–361, 2019.

[88] Frank Stajano and Paul Wilson. Understanding scam victims: seven principles for systems security. *Commun. ACM*, 54:70–75, March 2011.

[89] Statista. SMS and MMS messages sent in the United Kingdom (UK) from 2012 to 2022. https://bit.ly/3Ch2p5t, 2023.

[90] Brett Stone-Gross, Ryan Abman, Richard A. Kemmerer, Christopher Kruegel, Douglas G. Steigerwald, and Giovanni Vigna. The underground economy of fake antivirus software. In *Economics of Information Security and Privacy III*, pages 55–78, 2013.

[91] Siyuan Tang, Xianghang Mi, Ying Li, XiaoFeng Wang, and Kai Chen. Clues in tweets: Twitter-guided discovery and analysis of sms spam. In *ACM Conference on Computer and Communications Security*, 2022.

[92] Fabian Maximilian Johannes Teichmann. Twelve methods of money laundering. *Journal of money laundering control*, 20(2):130–137, 2017.

[93] Kurt Thomas, Danny Huang, David Wang, Elie Bursztein, Chris Grier, Thomas J. Holt, Christopher Kruegel, Damon McCoy, Stefan Savage, and Giovanni Vigna. Framing dependencies introduced by underground commoditization. In *Workshop on the Economics of Information Security*, 2015.

[94] Kurt Thomas, Dmytro Iatskiv, Elie Bursztein, Tadek Pietraszek, Chris Grier, and Damon McCoy. Dialing back abuse on phone verified accounts. In *ACM Conference on Computer and Communications Security*, page 465–476, 2014.

[95] Daniel Timko and Muhammad Lutfor Rahman. Commercial anti-smishing tools and their comparative effectiveness against modern threats. In *ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2023.

[96] Huahong Tu, Adam Doupé, Ziming Zhao, and Gail-Joon Ahn. Users really do answer telephone scams. In *USENIX Security Symposium*, 2019.

[97] James Twomey. Two arrests made in national £3.6m 'hi mum' text scam. https://bit.ly/4hx8uKn, 2023.

[98] Amber van der Heijden and Luca Allodi. Cognitive triaging of phishing attacks. In *USENIX Security Symposium*, 2019.

[99] Which? Smishing attacks in the UK grew by nearly 700% in the first six months of 2021, Which? reveals. https://bit.ly/4g2JRnj, 2021.

[100] Monica T Whitty. The scammers persuasive techniques model: Development of a stage model to explain the online dating romance scam. *British Journal of Criminology*, 53(4):665–684, 2013.

[101] Lei Yu, Gary Mottola, Christine N Kieffer, Robert Mascio, Olivia Valdes, David A Bennett, and Patricia A Boyle. Vulnerability of older adults to government impersonation scams. *JAMA Network Open*, 6(9):e2335319–e2335319, 2023.

Appendix

Platform	Median	Max.	Total	Scammer mobile phone numbers
	mule accounts			
SMS	2	10	385	135
Online Messaging	2	5	302	166
Total unique	2	12	582	270

Table 9: Distribution of mule accounts ($n = 582$) used by scammers ($n = 270$) on two different messaging platforms.