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

Agarwal, S.[1,2], Harvey, E.[2], Mariconti, E.[1], Suarez-Tangil, G.[3], and Vasek, M.[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. 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. We present 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.

Scammer Interaction

We collaborate with Stop Scams UK to access 711 engaged conversations from 3,402 initial ‘Hi mum and dad’ SMS scam texts.

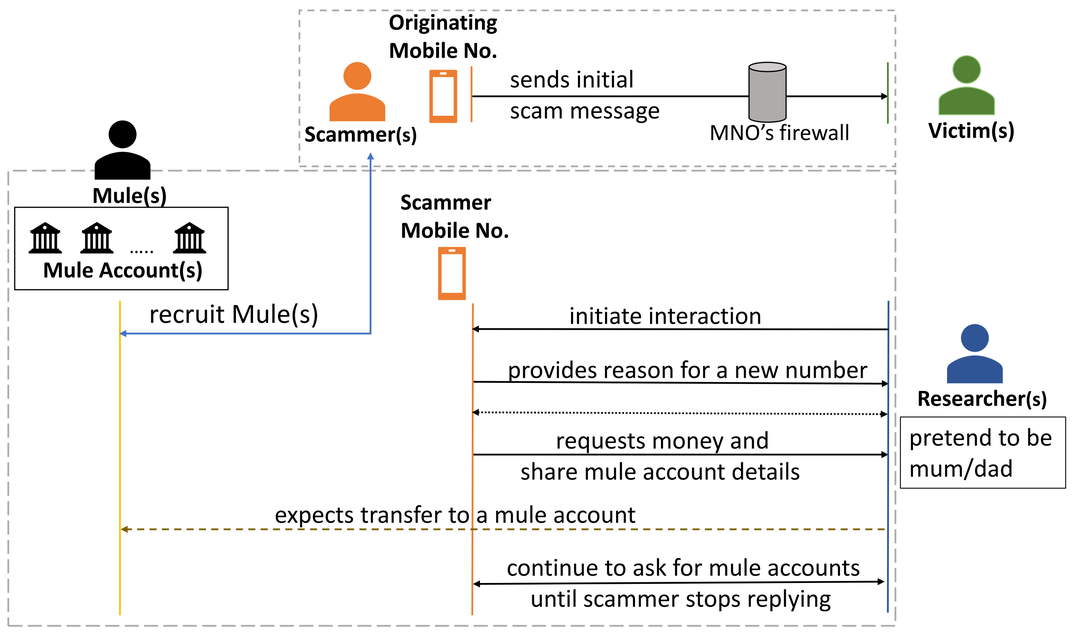

Figure 1: Modified life cycle of a ‘hi mum and dad’ SMS scam.

Results

We estimate that UK-based victims lose at least £2.3m per year.

Conversation Analysis

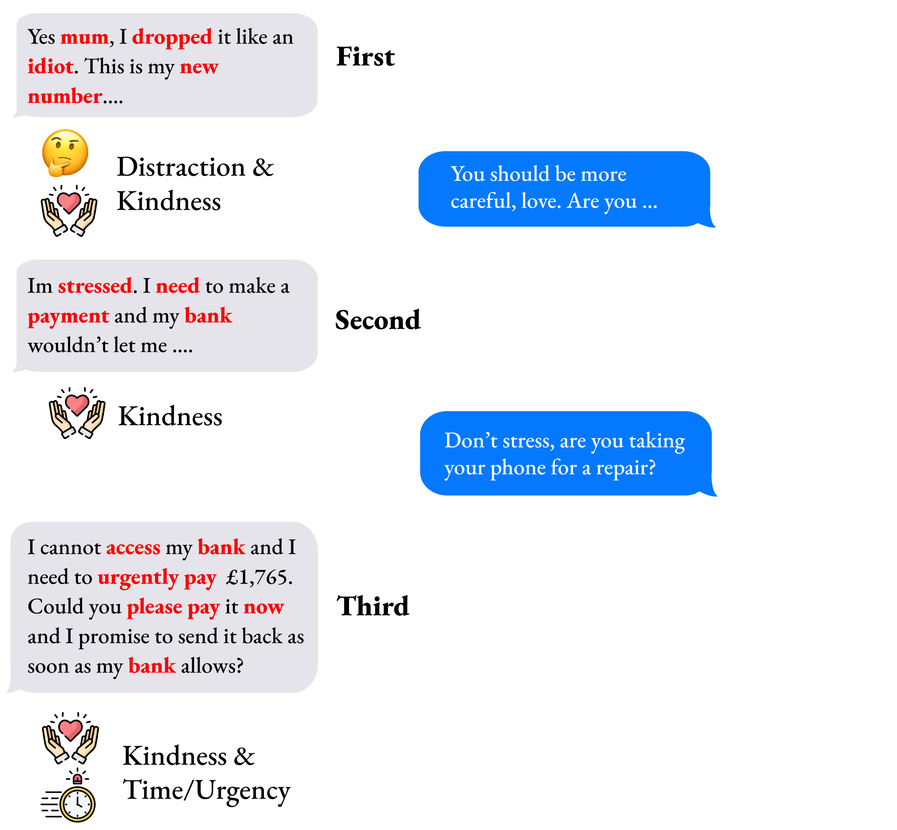

Figure 2: Identification of lures from the first three scammers’ responses.

Mobile Network Operators (MNOs)

Scammers prefer mobile network operators that SIM boxes/banks support. MNO1 is the most abused.

Mobile Network Operators	Type	SMS Originating	SMS Scammer	SMS Continuing	Online Messaging Originating	Online Messaging 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 1: Original mobile network operator distribution of originating sender ID mobile numbers, scammer mobile numbers, and continuing mobile numbers over SMS and online messaging platforms.

Amounts Requested

EMIs have only 8 requests above £2,500 compared to 29 requests above £2,500 into high street banks.

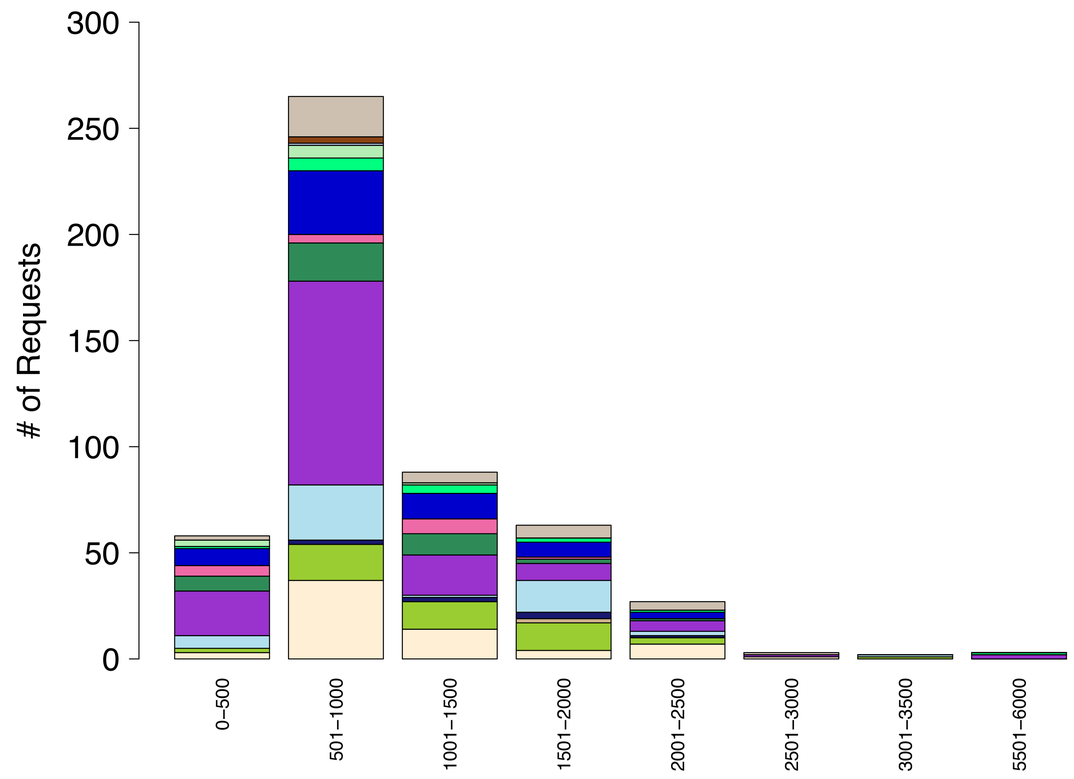

Figure 3: Distribution of amounts (£) scammers request into electronic money institutions (EMIs) per transaction. The different colors represent the different institutions.

Recommendations

The telecom regulators should mandate the mobile network operators to implement privacy-preserving Know Your Customer (KYC) checks before issuing pay-as-you-go (PAYG) mobile numbers.

Scammers abuse SIM boxes/banks to broadcast scam messages and communicate with the victims. GSM support should be disabled by default.

Financial institutions should enhance their fraud detection and prevention mechanisms and collaborate with mobile network operators to find connections to block scammers.

Check out our accepted paper at USENIX Security 2025 – >

sharad.agarwal@ucl.ac.uk
https://sharad1126.github.io