What Drives SMiShing Susceptibility? A U.S. Interview Study of How and Why Mobile Phone Users Judge Text Messages to be Real or Fake

Sarah Tabassum, Cori Faklaris, and Heather Richter Lipford,
University of North Carolina at Charlotte

https://www.usenix.org/conference/soups2024/presentation/tabassum-sarah

This paper is included in the Proceedings of the Twentieth Symposium on Usable Privacy and Security.

August 12–13, 2024 • Philadelphia, PA, USA

978-1-939133-42-7

Open access to the Proceedings of the Twentieth Symposium on Usable Privacy and Security is sponsored by USENIX.

What Drives SMiShing Susceptibility? A U.S. Interview Study of How and Why Mobile Phone Users Judge Text Messages to be Real or Fake

Sarah Tabassum
University of North Carolina at Charlotte

Cori Faklaris
University of North Carolina at Charlotte

Heather Richter Lipford
University of North Carolina at Charlotte

Abstract

In today's digital world, SMS phishing, also known as SMiShing, poses a serious threat to mobile users. However, it is unclear whether existing research on phishing can be applied to SMiShing. Our study aims to fill this gap by conducting interviews with 29 mobile phone users in a major southeastern U.S. city. We collected data on participants' experiences with suspicious SMS, understanding the cues they pay attention to, how they verify and report such messages, and the role of prior training in distinguishing real messages from scams. We also collected data on how specific details and context make a legitimate SMS seem genuine. Our findings indicate that participants focus more on the content, format, and links in SMS rather than the sender's short code, phone number, or email address. We suggest design changes to enhance user awareness and resilience against SMS phishing. This research provides practical knowledge to mitigate cyber threats linked to SMiShing. To the best of our knowledge, this is the first interview study on SMiShing susceptibility.

1 Introduction

With the continuous global surge in mobile phone adoption, as of January 2024, approximately two-thirds of the world's population, totaling 5.44 billion people, are actively using mobile phones [32]. Integral to every mobile phone is the Short Message Service (SMS) feature, which, according to Keepnet Labs, has become a prevalent medium for phishing attacks, especially since the onset of the COVID-19 pandemic. In 2020, SMS phishing or smishing attacks saw a staggering 328% increase, with 76% of businesses being targeted during that period [37]. The prominence of text message fraud is further underscored by data from the US Federal Trade Commission (FTC) in 2023, where text message fraud ranked among the top three methods employed by scammers, alongside emails and phone calls [5]. The financial implications of these scams were substantial, with a total loss of $10 billion reported in 2023, of which $372 million resulted solely from fraud text messages [5].

Understanding the reasons behind people falling victim to such scams via text messages is crucial. While extensive research exists on email phishing, its email-based cousin [9, 17, 30, 41, 46, 47, 49], the effectiveness of these techniques in SMShing remains unexplored. Both exploit trust and urgency for deception, but SMS communication's unique features such as shorter length, limited information, and immediacy create a distinct playing field [26, 39]. Traditional phishing research findings, built on email analysis and user behavior, may not directly translate to this mobile-based phishing.

Insights from the 2023 Databook by the US Federal Trade Commission are that younger individuals in the US are more susceptible to these fraud SMS scams, reporting their experiences, while older individuals tend to incur higher financial losses [5]. However, little to no published peer-reviewed research explores why people fall victim to SMiShing or the cues they use to identify legitimate and fraudulent SMS. To address this gap, our study begins with asking, *How do individual participants perceive the credibility of SMS messages and make trust decisions?* And, *What individual and design factors seem important?* To answer these inquiries, we employed an interview-based approach with mobile phone users in a major U.S. city, inspired by Jakobsson's work on phishing email cues [30]. We interviewed 29 participants, focusing on their mobile phone usage, experiences with suspicious and fraudulent SMS, cues they look for to distinguish legitimate from fraudulent SMS, effect of cybersecurity training, verification practices, and reporting behavior. During the interviews, participants were also asked to identify fraudulent and legitimate SMS from examples we provided, based on

USENIX Symposium on Usable Privacy and Security (SOUPS) 2024.
August 11–13, 2024, Philadelphia, PA, United States.

specific cues. We employed inductive methods to analyze the interviews.

Our findings revealed that while determining the legitimacy of an SMS, they prioritized cues such as contents with links, misspelled and out-of-context messages as suspicious indicators. For legitimate text messages, they looked for personalized information, a familiar context, known senders, and an official format. Those who had received some cybersecurity training demonstrated better judgment than those without training. Interestingly, most individuals did not report suspicious messages; instead, they tended to ignore them. Our study suggests a need for increased awareness, the implementation of SMS spam filters on iOS similar to Android [36], and an improved user interface for reporting fraudulent messages.

As of our knowledge, this study represents the first qualitative exploration into SMiShing. Our paper contributes the following:

- An enhanced understanding of individuals' real-life experiences with SMS phishing/fraud SMS.
- Insights into the cues that people use to distinguish between legitimate and fraudulent SMS.
- Design suggestions for telecommunication and mobile companies based on user data.

2 Background and Related Work

Phishing, a persistent cybersecurity threat, has undergone significant evolution since its emergence in the mid-'90s [23]. Initially recognized as a serious concern, service providers began responding with intensified efforts, deploying technical, educational, and legal interventions [30]. Despite these countermeasures, the Anti-Phishing Working Group (APWG) reported a staggering 1,286,208 phishing attacks in the second quarter of 2023, with the financial sector being the primary target, accounting for 23.5% of all attacks [10]. A notable evolution in the phishing landscape was the rise of SMS phishing, commonly known as SMiShing [43]. This variant gained prominence as attackers exploit text messages to deceive users [14]. SMiShing typically involves the dissemination of fraudulent links in text messages, leading unsuspecting victims to forms designed to either extract sensitive information or download malicious content [14, 43].

2.1 Phishing Attacks

Phishing is primarily employs fraudulent emails to impersonate legitimate entities and solicit sensitive information from users [11, 13, 28, 30]. This is recognized as one of the most common and extensively studied cyberattacks [1]. These emails often contain malicious links or attachments, redirecting users to fake websites or initiating the download of malware onto their devices [9, 28]. The motives behind phishing attacks vary, ranging from stealing money and identities to credentials or intellectual property.

Efforts to prevent or detect phishing attacks have led to various research approaches. Hong suggests strategies such as "making things invisible," utilizing machine learning on the backend to classify and filter out phishing attempts, developing improved user interfaces, and providing effective training [18, 20]. Numerous studies have explored factors influencing user susceptibility to phishing attacks, including email design, message content, situational context, and user characteristics [9, 16, 19–21, 31, 41, 46].

Among the studies that focused on visual cues for distinguishing legitimate websites/links, it is worth mentioning the research conducted by Alsharnouby et al. and Petelka et al. Alsharnouby et al.'s investigation explored users' ability to identify legitimate websites by capturing their attention [9]. The study found that users could successfully identify only 53% of phishing websites. Moreover, the study revealed that users typically allocate minimal time to inspecting security indicators and mainly focus on the website content during their assessments [9]. The study by Petelka et al. examined the impact of relocating phishing warnings close to suspicious links in emails [41]. Their findings showed that link-focused phishing warnings significantly reduced click-through rates compared to email banner warnings [41].

Sheng et al. explored demographic vulnerability, revealing the heightened susceptibility of young females to phishing attacks [46]. Their findings underscored that women exhibited greater vulnerability than men, and participants aged 18 to 25 were particularly susceptible due to disparities in computer and web expertise. Educational materials were identified as effective in reducing participants' willingness to provide information on fake webpages, with a marginal decrease in users' inclination to click on legitimate links. In 2007, Jakobsson et al. conducted a study on user reactions to various "trust indicators" in both authentic and phishing stimuli, offering insights into what renders phishing emails and web pages authentic. This research not only guided the design of legitimate material to mitigate risks but also examined factors influencing consumers' perception of legitimate content as dubious, with potential implications for online advertising [30].

Motivated by insights derived from studies on phishing, particularly the works of Jakobsson, Sheng and Alsharnouby [9, 30, 46], our study concentrates on SMiShing. The aim is to adapt and expand upon the understanding of user vulnerabilities in the context of SMS phishing attacks.

2.2 SMiShing Attacks

The term SMiShing is derived from the fusion of SMS, which stands for Short Message Service - the technology underpinning text messages - and phishing [2, 43]. The use of SMS for malicious purposes, termed SMiShing, has been documented since the early 2000s [23]. SMiShing constitutes a social engi-

neering attack that leverages deceptive mobile text messages to deceive individuals into downloading malware, disclosing sensitive information, or transferring funds to cybercriminals. This form of cybercrime has gained increasing prevalence and sophistication over the years [4]. In 2022, 76% of organizations in the U.S. encountered SMiShing attacks [23].

Despite the increasing prevalence of SMiShing, there has been limited academic exploration of its vulnerabilities. Some studies focus on characterizing modern SMS phishing attacks, exemplified by Nahapetyan's work [40]. This research utilized public SMS gateways to capture 67,991 phishing messages over a period of 396 days, providing valuable insights into SMS phishing trends and the clustering of phishing operations. Moreover, Jakobsson's insightful article addresses the use of two-factor "inauthentication" and the growing prominence of SMS phishing attacks related to two-factor authentication [29]. In a study by Rahman et al., involving 10,000 participants exposed to various smishing attacks, they found that personalized or spoofed messages heightened the perceived legitimacy and urgency for users to respond [42]. In a recent survey study on SMiShing susceptibility, findings indicated that the younger population was more vulnerable to such attacks [22]. However, little is known about how well the results from phishing studies apply in this new context. Consequently, there is a need for further research to comprehend SMiShing vulnerabilities. Our work seeks to fill this research gap by gaining deeper insights on SMiShing attacks. Through our study, we aim to offer insights into the dynamics of SMiShing attacks and enhance the understanding of user vulnerabilities in this context.

3 Methodology

To understand the participants' thought processes and personal experiences relevant to our research questions, we conducted in-person interviews. This section discusses the recruitment process, participant demographics, details about the interview sessions, and the data analysis process employed in our study.

3.1 Recruitment

In this interview study, we interviewed 29 participants (16 Females, 13 Males). We promoted recruitment through university research announcements, flyers distributed in a major southeastern U.S. city, and advertisements placed on Craigslist, Facebook, and LinkedIn. These recruitment materials were designed to engage individuals who have encountered or are open to discussing fraudulent messages. Prospective participants were required to complete a brief eligibility survey to determine their eligibility for the interview. From the pool of eligible participants, we aimed to achieve diversity in terms of education/job status and gender. The selection process involved evaluating factors such as gender and educational background. Individuals who met the criteria for the final interview were contacted via email and provided with a consent form. Participants who gave their consent for the interview were subsequently provided with information about the interview's available time slots and locations.

3.2 Participants

We have recruited 29 individuals who regularly use mobile phones, are 18 years or older, and reside in the metro area, making them available for in-person interviews. The participants consist of 16 females (55.2%) and 13 males (44.8%), spanning various age groups: 15 in the 18-24 range, 5 in the 25-34 range, 5 in the 35-44 range, 2 in 45-54 range and 2 who are 55 or older. Prior research indicates that the perception of cyber security risks and attention to trust indicators may differ based on age [25, 35]. In this study, we intentionally recruited people from different age groups to explore potential differences in their thought processes [50]. The participants also represent diverse professional backgrounds, including students, full-time employees, part-time employees, unemployed individuals, and self-employed individuals. Their professional backgrounds cover a wide spectrum, including computer science (CS), engineering (Eng.), business/management (BM), biology (Bio.), humanities (Hum.), education (Edu.), and even entertainment (Entr.).

Table 1 provides information about our participants on their age group (Age), gender (Gen.), mobile phone and carrier type (Mobile Set & Carrier), and occupation with the corresponding fields (Occupation). Furthermore, the table categorizes participants based on their professional status, including students ("Stu."), full-time employees ("FTE"), part-time employees ("PTE"), self-employed individuals ("SE"), and those currently unemployed ("U").

All participants utilize smartphones, with a variety of brands such as Samsung (Sam.), iPhone (iPhn.), Motorola (Moto.), Google Pixel (Pxl.), and Wiko Phone (Wiko). Their mobile carriers include AT&T, T-Mobile (T-Mob.), Tracfone (Trac.), H2O, Verizon (Vrzn), and Assurance (Asr.). Among our participants, 58.6% reported using their mobile phones for at least 21 to more than 30 hours in the past week at the time of the interview. During the interviews, participants were requested to bring their mobile phones to facilitate the review of text messages and the capture of screenshots if necessary.

3.3 Interview Sessions

During the interviews our team's researchers met with some participants at local coffee shops and others at the usability lab on campus. At the beginning of each session, the interviewer provided a brief introduction to the study's objectives and then asked for verbal consent to audio record the interview. Upon obtaining consent, the interviewer proceeded to

Table 1: Participant Demographics: Age group, gender, mobile phone and carrier information, and current occupation with corresponding field of study or profession are presented for all study participants

ID	Age	Gen.	Mobile Set & Carrier	Occupation
P1	25-34	M	Sam.(H2O)	Stu.(Civil Eng.)
P2	25-34	M	iPhn.(Vrzn)	Stu.(CS)
P3	55+	M	Moto.(T-Mob.)	FTE(Edu.)
P4	35-44	F	Sam.(AT&T)	SE(BM)
P5	35-44	F	iPhn.(T-Mob.)	FTE(Other)
P6	25-34	M	iPhn(T-Mob.)	Stu.(CS)
P7	25-34	M	Pxl.(AT&T)	Stu.(CS)
P8	18-24	F	Wiko(Asr.)	Stu.(Bio.)
P9	18-24	F	iPhn.(T-Mob.)	Stu.(CS)
P10	18-24	M	iPhn.(AT&T)	PTE(Other)
P11	18-24	F	iPhn.(AT&T)	U
P12	35-44	M	iPhn.(T-Mob.)	FTE.(Eng.)
P13	55+	F	iPhn.(AT&T)	FTE(BM)
P14	18-24	F	iPhn.(Vrzn)	Stu.(BM)
P15	18-24	F	iPhn.(Vrzn)	PTE(Other)
P16	18-24	F	Sam.(Vrzn)	Stu.(Hum.)
P17	18-24	F	iPhn.(Vrzn)	FTE(Edu.)
P18	25-34	M	iPhn(AT&T)	Stu.(BM)
P19	18-24	F	iPhn.(Trac.)	PTE(Other)
P20	45-54	F	iPhn.(Vrzn)	FTE(BM)
P21	45-54	M	iPhn.(Vrzn)	FTE(Edu.)
P22	18-24	M	iPhn.(Vrzn)	Stu.(BM)
P23	35-44	F	Sam.(T-Mob.)	FTE(Edu.)
P24	18-24	M	Sam.(Vrzn)	Stu.(EE)
P25	18-24	F	iPhn.(Vrzn)	Stu.(BM)
P26	18-24	M	Pxl.(AT&T)	Stu.(CS)
P27	35-44	F	Sam.(T-Mob.)	FTE(CS)
P28	18-24	M	iPhn.(Vrzn)	PTE(Entr.)
P29	18-24	F	iPhn.(T-Mob.)	Stu.(CS)

ask questions designed to address our research questions. The initial query focused on the participants' frequency of using texting apps, followed by questions about their mobile phone models and the mobile carriers they used. Subsequently, participants were invited to share their personal experiences with suspicious, fraud, and spam text messages. In this phase, participants were asked if they had any examples on their phones that they could share. Nearly all participants reported having multiple instances of suspicious and irritating messages. They were then asked to elaborate on why they considered those messages suspicious and were requested to share screenshots of the text messages. Next, each participant was presented with three pairs of legitimate and fraudulent text messages, chosen from a total of six pairs. The selection process was pseudo-random, with the interviewer counterbalancing the pairs to ensure each participant was sufficiently exposed to a variety of messages. We instructed them to think-aloud so that we can understand their thought process. The provided examples, all six pairs, were determined through internal discussions with our research team and industry professionals. In the process of choosing SMS pair examples, we took into consideration the findings from the CSN Data Book 2023, which highlighted imposter scams as the #1 category among the top 10 fraud classifications, as reported by the U.S. Federal Trade Commission [5]. These scams involved the impersonation of bank authorities, government officials, and various services, including healthcare, online shopping transactions, and more. In our study, we concentrated on a diverse set of examples related to banks, credit cards, money transfers, online shopping, and package delivery. We included both iOS and Android messaging app interfaces for these scenarios. Out of the six pairs, four involved simulated bank-related text messages. The remaining two pairs represented real-life instances of both fraudulent and legitimate SMS. Figure 1 illustrates the four pairs of simulated bank-related SMS.

Figure 2 displays the remaining two pairs, taken from real-life instances involving credit/debit cards, package delivery, and online orders. Upon completion of the task, participants were asked about the initial aspects they noticed in a text message from an unfamiliar source and the elements that made a text appear suspicious or legitimate to them. We inquired separately about visual elements, icons, symbols, or colors they considered while assessing the credibility of an SMS. Additionally, participants were questioned about their preferred methods of verifying suspicious SMS messages, actions taken upon receiving such texts, any history of reporting such texts, and the outcomes of such reporting. We also explored their prior training in computer or cybersecurity and how it might aid them in efficiently identifying fraudulent SMS messages. Towards the end of the session, participants were asked if they had any expectations or suggestions that could assist them in recognizing malicious SMS more efficiently. Finally, we expressed gratitude to the participants for their valuable time. Additionally, we provided each participant with "Best Practices to Identify Fraudulent Text Messages" and expressed our appreciation by offering a $25 Amazon e-gift card for their participation. Each interview session ranged in duration from 35 to 56 minutes. The Institutional Review Board (IRB) at our university reviewed and approved our study, and we obtained informed consent from participants.

3.4 Data Analysis

As the interview sessions were conducted in person, we obtained participants' consent and recorded the audio for each session as a reference. Subsequently, we employed an automated transcription service to transcribe all recordings. The first author reviewed all transcripts to ensure alignment with the original recordings. Throughout the interview process, we

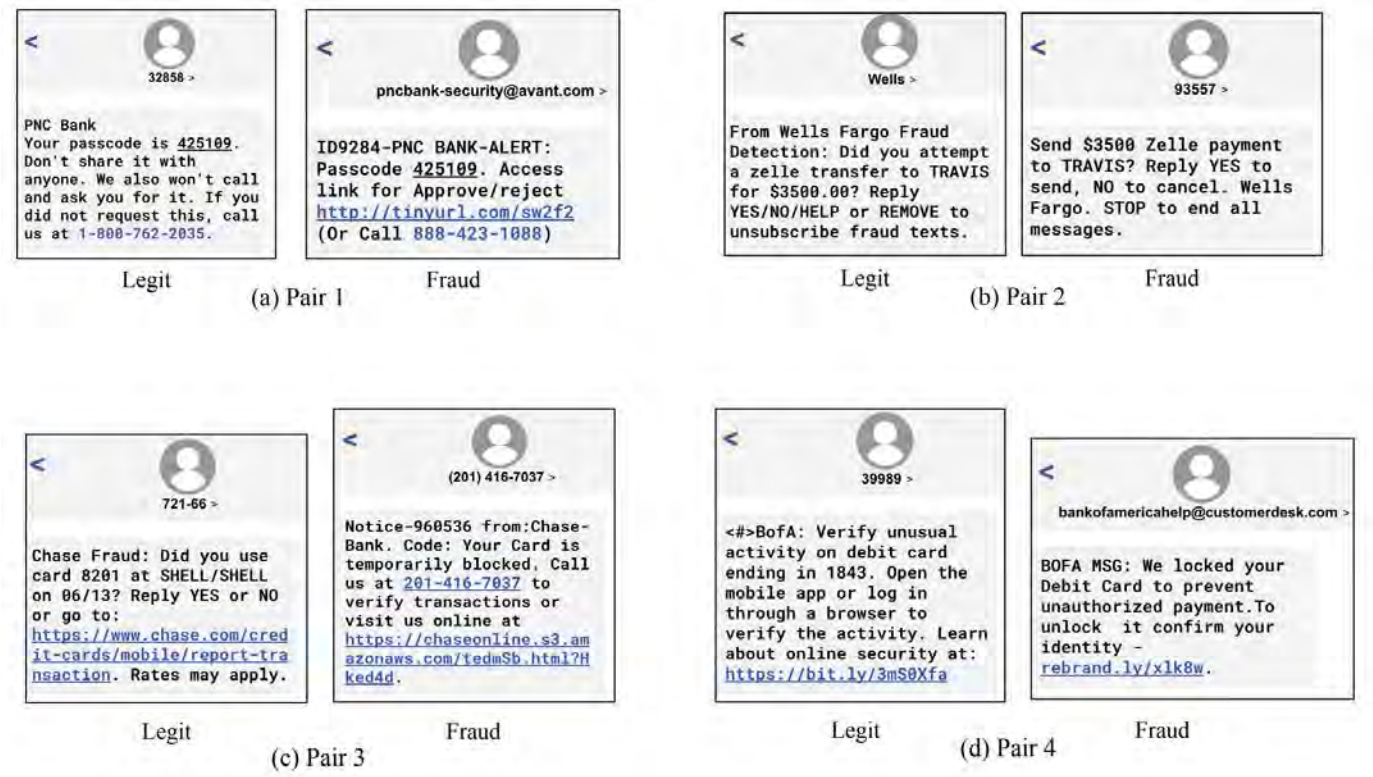

Figure 1: Visual representation of four pairs of simulated legitimate and fraudulent bank-related text messages presented to our participants. These text messages showcase deceptive tactics commonly employed in digital fraud.

systematically applied qualitative coding, enabling us to identify saturation points and adjust the interviews as interesting ideas or themes emerged. We analyzed our interview data using thematic analysis [12] and an inductive method [45], aligning with our research questions. We began by familiarizing ourselves with the data, then performed open coding [33] to segment it based on interview questions. We identified initial codes, explored similarities and differences, merged codes as needed, and organized them into themes, including cues for identifying suspicious and legitimate SMS messages. Research concluded when the codebook was completed, which is included in the appendix. In the coding phase, the first author completed coding for all transcripts. Inductive coding was then conducted across the entire dataset to develop a codebook. Afterward, both the first and second authors jointly reviewed the codes, resolving disagreements through discussion. Although the research team collaborated on code development and evaluation, the first author coded the entire dataset, eliminating the need for inter-rater reliability calculations [38].

4 Results

4.1 Mobile Phones, Carriers and Texting App Usage

Among the participants, 19 individuals (65.5%) were iPhone users with iOS. Android users showed diversity, with 6 participants using Samsung, 2 using Google Pixel, 1 using Wiko phone, and 1 using Motorola. Participants displayed varied choices in mobile carriers, with 11 users for Verizon, 8 users for T-Mobile, and 7 for AT&T. Additionally, there was 1 subscriber each for Assurance, H2O, and Tracfone.

All of our participants shared that they use texting apps on their phones on a daily basis. Participants found these apps very convenient for communicating with friends and family, as well as for planning activities. Many acknowledged regularly receiving suspicious or irritating SMS through these applications. Participants who underwent carrier switches generally reported no noticeable change in the frequency of spam SMS. However, it is noteworthy that one participant (P10) experienced an increase in spam calls and SMS after transitioning from T-Mobile to AT&T.

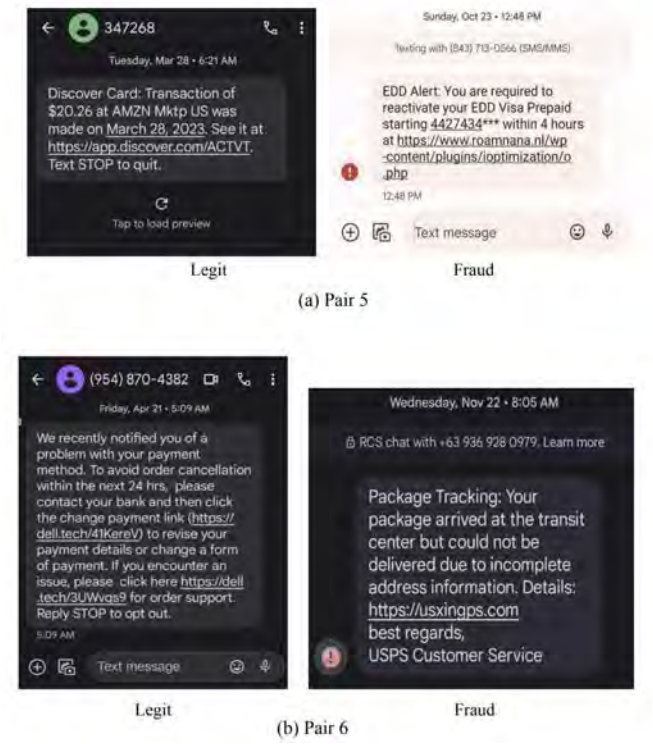

Figure 2: Two pairs of text messages, comprising both legitimate and fraudulent examples, gathered from real-life incidents

4.2 Personal Encounters with SMiShing

To gather insights into our participants' experiences with SMS phishing attacks, we queried, *"Have you ever received fraudulent or suspicious text messages on your phone, especially in the last 3 months?"* In response, all participants reported receiving such messages, with most encountering at least 1 or 2 per month, and some experiencing 3-4 weekly.

Subsequently, we requested participants to share specific examples from their phones. Out of 29 participants, 25 shared SMS examples. Analyzing these messages, we sought to understand the criteria participants used to identify fraudulent SMS and explore any discernible patterns. This investigation revealed varying types of fraud, with certain SMS categories prevailing over others. The following discussion presents the identified SMS types in order of prevalence.

4.2.1 Package Delivery Fraud

Among participants sharing suspicious SMS, 44% (11 out of 25) reported receiving messages purportedly from USPS or UPS. Notably, one participant observed an increased occurrence of such fraudulent SMS around holidays or birthdays. Participant 11(P11) fell for such fraud and clicked on such message under the assumption that it pertained to an awaited package. P11 stated:

"Yeah, so I fell for this because I actually did have a package coming at the time....it depends on the context and when you are expecting some package...This again happened with three days earlier and I also thought that this was legit at first."(P11)

Also, the combination of curiosity, the anticipation of a package, and a lack of awareness about this type of SMiShing attack can serve as motivations for users to click on such links.

4.2.2 Financial Deception

Of the 25 participants, 36% disclosed instances of financial fraud SMS. Primarily, these messages impersonated banks (5 out of 9), focusing on transaction verifications, debit card lock alerts, and similar themes. P25 provided insights:

"I got a transaction alert message...I looked at the email it was sent from and I was like, that doesn't look right....I was still was nervous about it. So I double checked with my bank. I called them.....asked if there was some transaction verification? Because I do bank with Wells Fargo. So I was like I wanted to just double check to make sure."(P25)

Additionally, 2 cases were associated with bill payments, 2 with cryptocurrency offers, and one involving an account block alert. Notably, P16 received MetaMask cryptocurrency wallet alerts, despite not having an account with any crypto wallets.

4.2.3 Fraudulent Business Promotion

Approximately 28% (7 out of 25) received fraudulent business promotion messages. While some promotions were legitimate, participants tended to recall expecting such communications. Vague information, suspicious or unofficial links, and attached images were red flags. P16 shared an example from "K'A'Y" Jewelry, stating:

"Using special characters make it more suspicious....like when they start using characters that are not letters..... I have one in my phone actually that I thought was like, kind of funny. Like pretending to be Kay Jewelers."(P16)

Figure 3 depicts the SMS with three key indicators, as explained by P16 why they believed it was a fraudulent message.

It is worth noting that none of our participants replied to or took any actions in response to unknown business promotions. This is because the distinction between spam and scam is somewhat unclear in their minds; they tend to perceive both as fraudulent activities.

4.2.4 Impersonation Tactics and Deceptive Offers

Around 24% (6 out of 25) received SMS employing impersonation tactics, where the sender pretended to be someone else. Common messages included queries like *"Hi, how are you?"* or *"Can you pick me up at the airport at 6 pm?"* or *"I won't be*

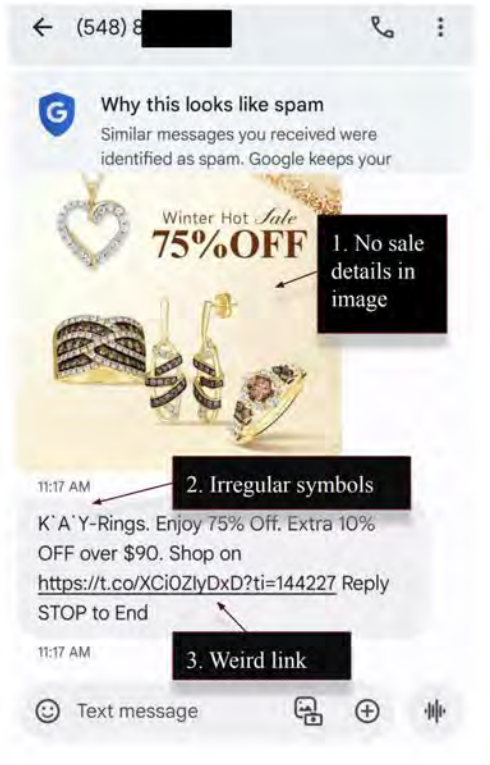

Figure 3: Text message displaying a deceptive business sale offer, highlighting three major suspicious cues identified by Participant 16: absence of detailed sale information in the attached image, irregular symbols used, and a suspicious-looking link

able to go to the winey with you tomorrow". Some participants chose to ignore such messages, while others, exemplified by P2, initially responded, later recognizing the fraudulent nature of the attempt to gather personal information. P2 shared the tendency to respond stems from the belief that the sender might have dialed a wrong number and is genuinely trying to reach someone.

Another participant received a fake job offer but promptly dismissed it due to the exorbitant amount of money promised in the SMS. Additionally, one participant (P18) fell victim to a gift card fraud while expecting a legitimate gift card. Figure 4 shows the SMS related to this incident. P18 shared their experience: *"I noticed that a group of malicious people. They noticed that I'm going to receive the gift cards, okay?.... In the coming few weeks they called me. And they also send me a text message..... And, to be honest, I first I trusted because I think and they are not asking the age and the gift card numbers or pin numbers. Instead, they're asking whether you have received your gift cards or not"*(P18)

Three participants out of 25 reported receiving fraudulent health and car insurance offers. They noted an increase in health insurance scams after having children, while the car

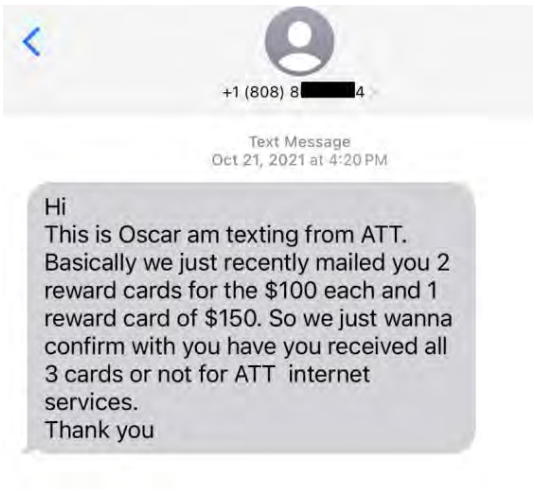

Figure 4: Deceptive SMS impersonating AT&T officials

insurance scams began when they provided their number to auto dealers during a car search.

4.2.5 Political Scams

Regarding political text messages some participants faced confusion distinguishing between legitimate and fraudulent political text messages. Some individuals mistakenly labeled non-harmful messages, specifically related to political campaigns, as fraud or suspicious due to a lack of contextual understanding. Participant P4 exemplified this situation by sharing an SMS, illustrated in Figure 5. P4 shared:
"I think this is a fraud...I don't know who Nikki is, I didn't sign up for that....of course I'm not going to click on the link. Yeah I don't even know the area code "337" and where that number comes from..."(P4)

Moreover, three participants reported receiving political scam SMS. They expressed skepticism about these messages due to irregular lettering and out-of-context content and weird accompanying links.

4.3 Participants' SMS Verification Strategies

We provided three pairs of legit and fraudulent SMS to each participant and requested them to identify them. Our goal was to gain insights into the cues they use when evaluating SMS messages. The comparative chart in Figure 6 shows the participants' capability to differentiate between legitimate and fraudulent SMS within each pair. Specifically, for Pair 2, participants exhibited a tendency to misidentify because they noticed the sentence structure was too informal, and they distrusted SMS messages from shortcodes. Conversely, 3 out of 14 participants incorrectly identified the fraudulent SMS as legitimate. They trusted the 5-digit short code and the instruction to "reply YES to send."

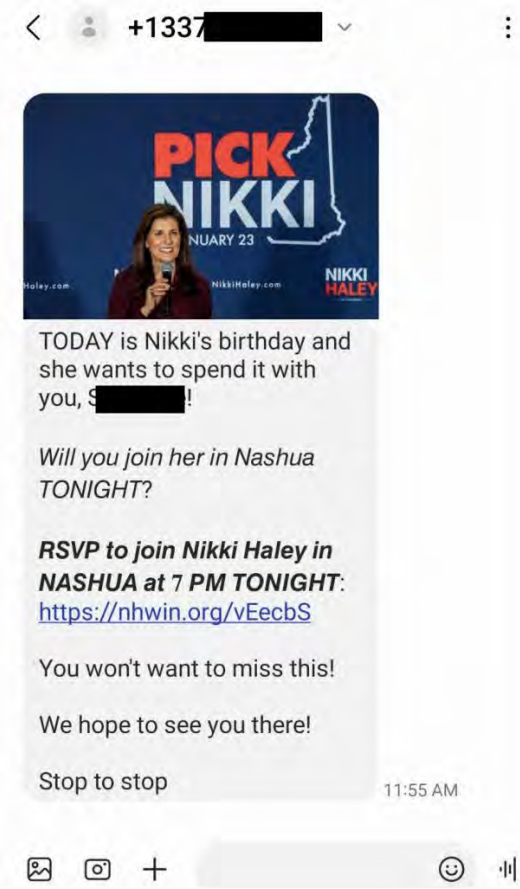

Figure 5: An example of a text message related to a political campaign that raises suspicion due to the absence of contextual understanding and an unfamiliar area code, as reported by P4

In contrast, their performance significantly improved for Pair 4. The legitimate SMS in this pair followed an official format, including personalized information like the last 4 digits of a card, mention of the mobile app, and reliance on the 5-digit short code. On the other hand, the fraudulent SMS came from an email address, raising suspicion. The format and the link appeared unofficial and dubious to the participants. The following sub-sections discuss the specific cues they consider when assessing text messages.

4.3.1 Cues for Suspicious SMS

Here, we elaborate on the cues for suspicious SMS messages as identified by participants, listing them in descending order from the most mentioned to the least:

Suspicious Contents: 28 out of 29 participants (96.5%) emphasized the significance of text message content in their assessments. Specifically, within the content, 17 participants flagged any SMS containing **links** as suspicious.

P21 said: *"...basically any link telling me to click on this immediately makes me suspicious..."*

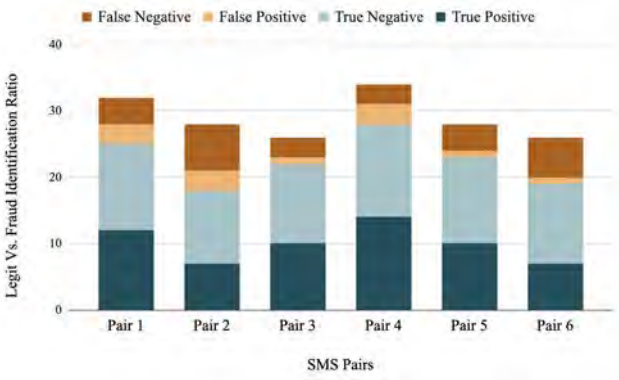

Figure 6: Comparative Bar Chart: Participants' Accuracy in Distinguishing Legitimate and Fraudulent SMS. The chart displays participants' performance, with True Positives indicating correctly identified legitimate messages, True Negatives for correctly identified fraudulent messages, False Positives for incorrectly labeled legitimate messages, and False Negatives for misidentifying legitimate messages as fraudulent.

Among the SMS pairs presented, pairs 1, 3, 4, 5, and 6 contained links. When both legit and fraud SMS messages included links, participants scrutinized the details of the URLs more closely. They tried to be sure whether the domain matched the official domain of the respective company or service. For pair 1, 13 out of 16 participants correctly identified the fraudulent message. They pointed out the presence of "tinyurl" in the link and the lack of security with "http:" at the beginning as red flags. Pairs 4 and 5 were comparatively easy for our participants. Especially, since the fraudulent link in Pair 4 lacked "https:". However, in Pair 6, many participants found it challenging to identify the legitimate SMS, with 6 out of 13 incorrectly labeling the legitimate message as fraudulent due to the inclusion of random letters and multiple links in a single SMS.

15 out of 29 participants indicated that they primarily examine the content first, assessing for the presence of links, correct grammar, or spelling errors. P24 mentioned:

" I usually glance at it and like the first thing I pick out is spelling errors. If things are misspelled that usually it's like a telltale sign. It's something fishy...I generally just ignore ones that include links."(P24) 8 participants expressed suspicion towards SMS related to money, while 2 individuals noted concern with personal inquiries, and 1 with generalized SMS.

Unofficial Format:15 out of 29 (51.7%) participants identified an unofficial format, including wrong spelling and grammar (6/15), the use of irregular special characters (5/15), and SMS containing wrong or weird company names, as suspicious. P17 shared:

"I never click on like the suspicious links or misspelled things.....Or like lower-cases yeah, stuff like that....I look into

the format as well, like, how their constructing the sentence if it doesn't read right stuff like that."(P17)
In Pair 2, a significant reason why 7 out of 14 participants incorrectly identified the legitimate SMS as fraudulent was due to unofficial format of that SMS. P17 added:
"The spelling of 'Zelle' starts with a lower-case 'z'..it's definitely fraud...also the '.00' after the money amount is not normal I think"(P17)
Unknown Sender: While judging an SMS, 18 participants mentioned examining the sender's number, email, or short code. However, it is important to note that they do not automatically categorize unknown senders as fraudulent. Instead, they assess the number in various ways. Of these, 3 participants specifically emphasized checking the area code, expressing reluctance to respond if it fell outside their familiar geographic area. P16 said:
"I'll look at the area code but I'll also obviously look at the content....I don't recognize if it's not from somebody in my area code I usually don't answer it."(P16)
11 out of 29 (37.9%) participants considered any SMS from an unknown sender suspicious, especially if it originated from an international number, according to 2 participants. One participant mentioned mistrust towards SMS sent from email and this made them identify the fraud SMS in Pair 4 correctly. On the other hand, there was a level of skepticism towards short codes as senders, resulting in 2 participants mistakenly labeling the legitimate SMS in Pair 1 as fraudulent.
Out of Context SMS: 6 out of 29 participants deemed any out-of-context SMS suspicious. Out-of-context SMS refers to messages that are unexpected or unrelated to the recipient's recent activities or communications, making them appear unusual and potentially fraudulent.
Immediate Action: 4 out of 29 participants stated that any SMS requesting immediate action would be deemed suspicious by them. P21 said:
"... anything has a time frame telling me that I need to respond within one or two hours makes me suspicious.."(P21)
In Pair 6, three participants noted that the mention of the phrase "next 24 hours" led them to believe it was a fraudulent SMS, although it was actually a legitimate one. On the other hand, in Pair 5, the fraudulent SMS contained the phrase "within 4 hours," aiding participants in identifying it as fraudulent.

4.3.2 Cues for Legitimate SMS

Among the cues that contribute to making text messages more reliable and legitimate for our participants, several factors were highlighted. The top factor was making the SMS more specific with personalized information known only to the subscribed business and not to the general public. Other significant cues included a known context, a familiar sender, and an official format. These factors are discussed in detail below:
Contains Personalized Info: The importance of personalized information in SMS was emphasized by 14 participants. It worked as a key indicator in determining the legitimacy of text messages, especially for Pair 3 and 4. In these pairs, 10 out of 14 and 14 out of 17 participants successfully identified the legitimate message, respectively, attributing their success to the presence of personalized details. Participant 5 shared:
"I will trust the second one as it has the last 4 digits of my card... I think it's hard for scammers to get this information"(P5).
Known Context: Next significant indicator was a known context, as highlighted by 11 participants. They expressed trust in SMS messages they were already expecting. Especially, P12 and P13 mentioned deleting any message on their phone if they do not recognize the sender or the reason for texting. P12 further explained that they ask people to call if necessary but not to send text messages.
Known Sender: Ten participants mentioned that they trust SMS messages from known senders. P16 said:
"I usually trust the numbers that are already saved in my phone... or you know, who gives the name and say like, 'Hi, I am Alex, we met at the college today'... like that... so I can relate."
Official Format: Mentioned by 8 participants, having an official format emerged as another key factor. This played a crucial role in the higher success rate in correctly identifying legitimate SMS in Pair 3 and 4. P7, who saw Pair 4, mentioned noticing the $<\#>$ sign in SMS from Bank of America. P7 said:
"The example with Bank of America, there was a the pound sign at the beginning of the message....I feel like I've seen bank messages that also use symbols in the beginning that could be used the key identifier for legitimacy."(P7)
However, the absence of an official format in the legitimate SMS in Pair 2 and 6 posed challenges for participants. For instance, when evaluating SMS Pair 6, P8 mentioned:
"the text is too long..and it is from some peronal phone number..I do not think it is legit, it's fraud"(P8)
Additionally, participants expressed trust in SMS that require no action, involve no personal inquiries, and exhibit correct spelling and grammar.

4.3.3 Visual Indicators

The majority of our participants did not focus on visual indicators when assessing the credibility of an SMS. On the contrary, they identified excessive use of emojis, excessive exclamation marks or dollar symbols, and messages that were either too long or too short as red flags. Android users mentioned that they would be more suspicious of an SMS if it triggered warning signs from the Android SMS spam filters [36]. In contrast, iPhone users, lacking such warning signs, did not anticipate any indicators for fraudulent SMS.

It was noteworthy to observe that in Pair 5 and 6, despite the fraud SMS displaying warning signs according to the

Google Message Spam Filter, iPhone users overlooked the indicators, whereas all Android users were able to identify them. Additionally, in Pair 6, one participant (P18) placed trust in the fraudulent SMS as legitimate due to the presence of a padlock sign for secured RCS chat [44], as provided by Google. This underscores the need for more efficient and effective design in messaging platforms that align with users' mental models [7, 41].

4.4 Verification Behavior

To understand our participants verification behavior we asked them, *"Where do you turn to for verification when you receive a suspicious text message?"* A majority (72.4%) of participants shared that they would contact the bank or the company mentioned in the SMS for confirmation. To do so, they would either use mobile apps or visit the official website to find the correct contact number and verify the authenticity of the received SMS.

Interestingly, two participants shared a unique approach, stating that they would initially consult their father or elder brother for verification, trusting them as the best option. P15 elaborated, stating,

"Well, I go to my dad first and call him to ask about it. If he says it's legit, then I'll call the company. If both sources confirm its legitimacy, then I will trust it."(P15)

Two participants indicated they rely on their own judgment or analytical skills to verify suspicious SMS. Notably, only one participant (P2) mentioned occasionally using ChatGPT to verify links on suspicious SMS.

P2 explained, *"Sometimes I use websites or ChatGPT. For example, around four months ago, I wanted to purchase tickets from an unfamiliar source, and I was unsure about its legitimacy. I asked ChatGPT, 'Is it legal? Do you have any information about the website?' And it told me, 'Yes, it's legit'."*

Two participants mentioned that they do not engage in any verification process. In contrast, only one participant (P27) employs websites such as SpyDialer [48] to verify unknown caller or sender numbers.

4.5 Reporting Behavior

In order to investigate participants' actions upon receiving suspicious or fraudulent SMS messages and their reporting behavior, we asked them the following questions: *"What do you do when you receive a fraudulent text? Have you ever reported it? How? What were your expectations after reporting? And what actually happened?"*

In response, 55.2% (16/29) of our participants indicated that they generally do not report such messages. Among these, five individuals mentioned simply ignoring the message. Four participants actively delete the messages but refrain from reporting. Additionally, five participants rely on the filtering system on their phones and do not check the spam folder to report such messages. On Android phones, the SMS filter displays a warning sign and provides an explanation for marking a message as spam, as highlighted in green color in Figure 7. However, several participants mentioned that if there was an easier reporting option, as suggested in Figure 7, they would report more.

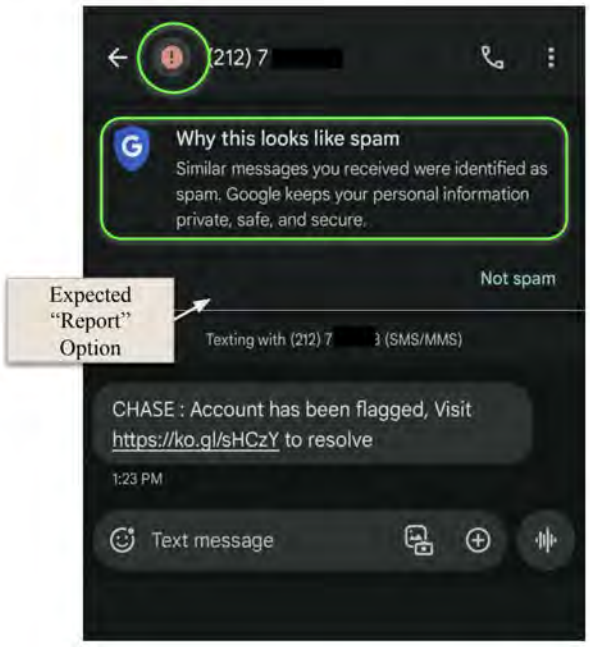

Figure 7: Green-highlighted areas show the warning signs by Android SMS Spam Filters that were appreciated by our participants. Yet, users expressed a desire for more accessible reporting options, as indicated in the image.

Seven out of the 29 participants mentioned that they occasionally report SMS messages, especially if they find them to be alarming, containing sensitive information, or referencing potential financial harm. One participant stated they would only report work-related messages, believing that such reporting could benefit their colleagues.

Six participants shared that they utilize the *"Report Junk"* option on their iPhones when reporting suspicious messages as showed in Figure 8.

iMessage currently lacks spam filters and warning signs, unlike Android. Eight participants suggested that incorporating warning signs, as shown in Figure 8, in suspicious text messages would aid in identification. Interestingly, none of the participants have received any feedback regarding the outcome of their reports. Every participant expressed that they would like to have some feedback or assurance. This feedback would contribute to a sense of confidence and assurance that authorities are actively addressing fraudulent SMS concerns.

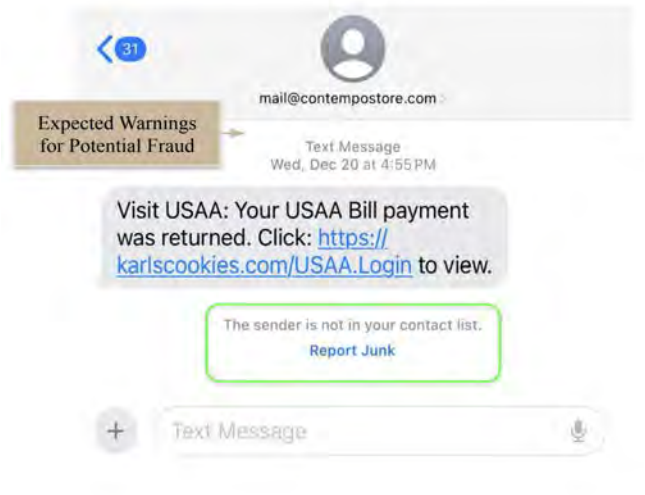

Figure 8: The 'Report Junk' option, highlighted in green on the iMessage interface proved useful for reporting by our participants. Also, they expressed a need for warning signs in the indicated area to better identify potential fraud SMS.

4.6 Effect of Prior Cyber Security Training

Among 29 participants 14 individuals(48.3%) reported not having received any formal training or education related to cybersecurity. While not statistically proven, we observed a trend indicating that participants more susceptible to incorrectly identifying fraudulent and legitimate SMS messages belonged to this group without cybersecurity or awareness training, including P8, P15, and P29 (3 out of 29). Interestingly, those who had some form of training demonstrated better abilities in identifying fraudulent messages. Also, these individuals showed heightened suspicion to legitimate messages, often classifying them as potentially fraudulent due to their added caution. Some participants (P10, P22, P26) mentioned attending seminars on cybersecurity during middle or high school.

Two participant mentioned learning through online awareness posts, while another expressed reliance on their analytical skills, saying that formal training was unnecessary to them. Six participants had a major in computer science and were well aware of cybersecurity. Five received occasional security training at their jobs. One participant had received training on cybersecurity at school. Additionally, two participants learned about cybersecurity from their fathers working in the IT industry. They did quite well in identifying the legit and fraud SMS. They expressed that more structured training would enhance their ability to identify patterns in fraudulent SMS.

5 Discussion

5.1 Key Insights

To reduce susceptibility to SMiShing, it is crucial to understand the cues that make SMS messages appear more legitimate or suspicious. Our study explores these cues and investigates the considerations users take into account when making judgments. We found that the presence of URLs or links, unofficial format, immediate action cues are some of the key factors that people find suspicious which aligns with previous SMiShing related studies [15]. Moreover, participants in our study placed significant importance on context when assessing SMS messages. Before evaluating the content or authority of the message, they considered whether they were expecting the text message. Goel et al. noted that exploiting this context as a human weakness is applicable to SMS phishing as well [24]. Furthermore, participants consistently emphasized the significance of personalized information within the content, highlighting its impact on their judgment of the message's legitimacy.

Another significant factor is the participants' frequent confusion between spam and scam text messages [34]. Many businesses use text messages for promotions, but inconsistencies in numbers and formats often lead people to consider these messages as scams. This observation resonates with the idea of implementing improved designs and educational initiatives to facilitate users in distinguishing between legitimate and fraudulent messages [6, 27].

Moreover, participants stressed the importance of enhanced filtering mechanisms on iPhones to identify and block fraudulent SMS. This recommendation aligns with the growing need for adaptive and advanced security features in mobile devices to proactively detect and prevent SMiShing attacks. Our study also shows that participants often have difficulties reporting incidents because they are not familiar with the "7726" reporting service [3] and feel the need for a more accessible reporting option. This emphasizes the importance of making reporting processes simpler to ensure fast and efficient reporting of fraudulent SMS.

While our study did not identify specific patterns related to mobile carrier, background, or job influencing susceptibility to SMS phishing, we found that younger participants aged 18 to 24, especially those without prior cybersecurity training, were more vulnerable. This aligns with a recent survey by Faklaris et al. on US demographics [22]. Interestingly, some younger participants in our study excelled in identifying fraud vs. legit SMS, mentioning prior cybersecurity training. Additionally, older individuals exhibited greater caution when receiving SMS, often due to security training at work. These findings underscore the potential impact of educational initiatives in enhancing users' ability to identify and mitigate SMS phishing threats.

Our study not only contributes valuable insights into the

nuances of SMS phishing but also advocates for addressing aspects such as improved filtering mechanisms, accessible reporting options, and comprehensive training programs. These are essential to fortifying users against evolving SMiShing threats in the digital landscape.

5.2 Finding Alignment: Comparing SMiShing and Email Phishing

Our study reveals significant parallels between SMiShing and email phishing, particularly in how users assess the legitimacy of messages. Participants placed considerable importance on context when evaluating SMS messages, aligning with findings from prior research on email phishing [8, 24, 30].

Moreover, our study participants consistently highlighted the significance of personalized information within the content of SMS messages, a factor similarly emphasized in email phishing [30, 41]. However, unlike email phishing, where users can hover over links to verify their legitimacy , this action is not feasible on mobile devices. This difference underscores the sophistication of SMiShing attacks, as perpetrators tailor messages to appear genuine by incorporating recipient-specific details and an official-looking format.

Participants also indicated that security symbols, such as padlock icons or indications of secured SMS, are trust indicators. This finding aligns with Jakobsson (2007), who noted the importance of such symbols in establishing perceived safety in email communication [30]. Similarly, users in our study found it helpful to have warning signs on Android phones for potential fraud in SMS, just like those used in email systems. This supports findings from research on email phishing [41].

However, there are notable differences between SMiShing and email phishing. For instance, SMS messages typically do not feature logos or third-party endorsements, which are recognizable brand logos or verifications from credible third parties, commonly used to signify legitimacy in email phishing [30]. This absence of visual and endorsement cues in SMS requires users to rely more heavily on other indicators such as context, content personalization, and security symbols.

These insights indicate that while there are significant overlaps in how users perceive and respond to SMiShing and email phishing, the unique constraints and characteristics of SMS messaging necessitate different strategies for identifying and mitigating these threats. Our findings emphasize the need for tailored approaches to enhance user awareness and defenses against SMiShing.

6 Limitations

We conducted interviews with 29 participants in a major southeastern U.S. city, providing valuable insights into the cues they consider when evaluating the legitimacy of text messages and enhancing our understanding of their experiences with SMiShing. The participants, diverse in age and profession, may not fully represent other locations, particularly rural or underdeveloped areas where awareness levels differ, potentially introducing bias. We used a variety of SMS visual styles: Pairs 1-4 mimicked the iMessage UI, while Pairs 5-6 presented real Android examples. This diversity revealed that Android users recognized warnings more effectively due to familiarity with red indicators, though the visual dissimilarity between pairs is a noted limitation. The selection process was pseudo-random and counterbalanced to ensure exposure to different pairs, but not all participants saw each visual style. Additionally, focusing on financial SMiShing examples may not encompass the full range of SMiShing attacks, suggesting future research should include a broader spectrum. The recruitment text aimed to engage individuals familiar with or open to discussing fraud messages, which may have introduced bias. Future studies should consider a wider variety of SMiShing categories and acknowledge the possibility of emerging SMiShing patterns.

7 Conclusion

Our study sheds light on the pressing issue of SMS phishing (SMiShing) and its significant impact on individuals. Through exploring real-life experiences, we gained nuanced insights into susceptibility factors, with participants highlighting cues crucial for distinguishing between legitimate and fraudulent SMS - emphasizing personalized information, known senders, and official formats. Furthermore, our study contributes valuable recommendations for telecom and mobile companies to enhance security measures. By proposing design suggestions informed by user feedback, we aim to empower these entities to better protect their users from falling victim to SMS phishing scams. As the first qualitative exploration into SMiShing, our research advances the understanding of this cybersecurity challenge. The findings underscore the need for proactive measures and heightened awareness to mitigate the risks associated with fraudulent SMS. In an era where digital communication plays a pivotal role, safeguarding users against SMS phishing is imperative for fostering a secure and trustworthy mobile communication environment.

Acknowledgments

We extend our heartfelt gratitude to our industry collaborators for their invaluable assistance in the design and execution of this research. We also acknowledge the funding provided by the Center for Cybersecurity Analytics and Automation (established with NSF award #1822150), for this study.

References

[1] 2023 data breach investigations report. Retrieved: February 11, 2024 from https://www.verizon.com/business/resources/reports/dbir/.

[2] Recognizing bank account fraud: Bank of america. Retrieved: February 10, 2024 from https://www.bankofamerica.com/security-center/faq/sharing-information/.

[3] How to recognize and report spam text messages, Jun 2022. Retrieved: February 10, 2024 from https://consumer.ftc.gov/articles/how-recognize-and-report-spam-text-messages.

[4] Threat report 2023: State of the phish, Aug 2023. Retrieved: February 10, 2024 from https://www.proofpoint.com/us/resources/threat-reports/state-of-phish.

[5] Consumer sentinel network data book 2023, Feb 2024. Retrieved: February 11, 2024 from https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2023.

[6] Elham Al Qahtani, Yousra Javed, Sarah Tabassum, Lipsarani Sahoo, and Mohamed Shehab. Managing access to confidential documents: A case study of an email security tool. *Future Internet*, 15(11):356, Oct 2023.

[7] Auwal Shehu Ali and Zarul Fitri Zaaba. Mental models review for security and privacy policy: An approach. In *2021 International Conference on Information Technology (ICIT)*, pages 905–909. IEEE, 2021.

[8] Zainab Alkhalil, Chaminda Hewage, Liqaa Nawaf, and Imtiaz Khan. Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, 3:563060, 2021.

[9] Mohamed Alsharnouby, Furkan Alaca, and Sonia Chiasson. Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, 82:69–82, 2015.

[10] APWG. Phishing activity trends report, 2nd quarter 2023, Nov 2023.

[11] Mark Blythe, Helen Petrie, and John A Clark. F for fake: four studies on how we fall for phish. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 3469–3478, 2011.

[12] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2):77–101, 2006.

[13] Chuck Brooks. Cybersecurity trends statistics for 2023; what you need to know, Sep 2023. Retrieved: February 10, 2024 from https://www.forbes.com.

[14] Emily Cahill. Phishing, smishing and vishing: What's the difference?, Jul 2023. Retrieved: February 12, 2024 from https://www.experian.com/blogs/ask-experian/phishing-smishing-vishing/.

[15] Max Clasen, Fudong Li, and David Williams. Friend or foe: An investigation into recipient identification of sms-based phishing. In *Human Aspects of Information Security and Assurance: 15th IFIP WG 11.12 International Symposium, HAISA 2021, Virtual Event, July 7–9, 2021, Proceedings 15*, pages 148–163. Springer, 2021.

[16] Shelby R Curtis, Prashanth Rajivan, Daniel N Jones, and Cleotilde Gonzalez. Phishing attempts among the dark triad: Patterns of attack and vulnerability. *Computers in Human Behavior*, 87:174–182, 2018.

[17] Rachna Dhamija, J Doug Tygar, and Marti Hearst. Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*, pages 581–590, 2006.

[18] Xun Dong, John A Clark, and Jeremy L Jacob. User behaviour based phishing websites detection. In *2008 International Multiconference on Computer Science and Information Technology*, pages 783–790. IEEE, 2008.

[19] Julie S Downs, Mandy Holbrook, and Lorrie Faith Cranor. Behavioral response to phishing risk. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit*, pages 37–44, 2007.

[20] Julie S Downs, Mandy B Holbrook, and Lorrie Faith Cranor. Decision strategies and susceptibility to phishing. In *Proceedings of the second symposium on Usable privacy and security*, pages 79–90, 2006.

[21] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 1065–1074, 2008.

[22] Cori Faklaris, Heather Richter Lipford, and Sarah Tabassum. Preliminary results from a us demographic analysis of smish susceptibility. *arXiv preprint arXiv:2309.06322*, 2023.

[23] Paul Gillin. The history of phishing, Jan 2021. Retrieved: February 11, 2024 from https://www.verizon.com/business/resources/articles/s/the-history-of-phishing.

[24] Sanjay Goel, Kevin Williams, and Ersin Dincelli. Got phished? internet security and human vulnerability. *Journal of the Association for Information Systems*, 18(1):2, 2017.

[25] Yasmeen Hanif and Harjinder Singh Lallie. Security factors on the intention to use mobile banking applications in the uk older generation (55+). a mixed-method study using modified utaut and mtam-with perceived cyber security, risk, and trust. *Technology in Society*, 67:101693, 2021.

[26] Dermot Harnett and W. Stuart Jones. Smishing vs. phishing: Understanding the differences: Proofpoint us, May 2023. Retrieved: February 12, 2024 from https://www.proofpoint.com/us/blog/email-and-cloud-threats/smishing-vs-phishing-understanding-differences.

[27] Cormac Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 workshop on New security paradigms workshop*, pages 133–144, 2009.

[28] Jason Hong. The state of phishing attacks. *Communications of the ACM*, 55(1):74–81, 2012.

[29] Markus Jakobsson. Two-factor inauthentication–the rise in sms phishing attacks. *Computer Fraud & Security*, 2018(6):6–8, 2018.

[30] Markus Jakobsson, Alex Tsow, Ankur Shah, Eli Blevis, and Youn-Kyung Lim. What instills trust? a qualitative study of phishing. In *Financial Cryptography and Data Security: 11th International Conference, FC 2007, and 1st International Workshop on Usable Security, USEC 2007, Scarborough, Trinidad and Tobago, February 12-16, 2007. Revised Selected Papers 11*, pages 356–361. Springer, 2007.

[31] Mohammad S Jalali, Maike Bruckes, Daniel Westmattelmann, and Gerhard Schewe. Why employees (still) click on phishing links: investigation in hospitals. *Journal of medical Internet research*, 22(1):e16775, 2020.

[32] Simon Kemp. Digital 2023: Global overview report - datareportal – global digital insights, Feb 2023. Retrieved: February 02, 2024 from https://datareportal.com/reports/digital-2023-global-overview-report.

[33] Shahedul Huq Khandkar. Open coding. *University of Calgary*, 23(2009):2009, 2009.

[34] Alex Kigerl. Spam-based scams. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, pages 877–897, 2020.

[35] Stewart Kowalski and Mikael Goldstein. Consumers' awareness of, attitudes towards and adoption of mobile phone security. In *20th International Symposium on Human Factors in Telecommunication*, pages 20–23, 2006.

[36] Neil Kumaran. New gmail protections for a safer, less spammy inbox, October 2023. Retrieved: February 12, 2024 from https://blog.google/products/gmail/gmail-security-authentication-spam-protection/.

[37] Keepnet Labs. Smishing statistics 2023: The latest trends and numbers in sms phishing, Jan 2024. Retrieved: February 10, 2024 from https://keepnetlabs.com/blog/smishing-statistics-2023-the-latest-trends-and-numbers-in-sms-phishing.

[38] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for cscw and hci practice. *Proceedings of the ACM on human-computer interaction*, 3(CSCW):1–23, 2019.

[39] Tanya McGill and Nik Thompson. Old risks, new challenges: exploring differences in security between home computer and mobile device use. *Behaviour & Information Technology*, 36(11):1111–1124, 2017.

[40] Aleksandr Nahapetyan, Sathvik Prasad, Kevin Childs, Adam Oest, Yeganeh Ladwig, Alexandros Kapravelos, and Bradley Reaves. On sms phishing tactics and infrastructure. In *2024 IEEE Symposium on Security and Privacy (SP)*, pages 169–169. IEEE Computer Society, 2024.

[41] Justin Petelka, Yixin Zou, and Florian Schaub. Put your warning where your link is: Improving and evaluating email phishing warnings. In *Proceedings of the 2019 CHI conference on human factors in computing systems*, pages 1–15, 2019.

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

[43] IBM Research. What is smishing (sms phishing)?, 2023. Retrieved: February 12, 2024 from https://www.ibm.com/topics/smishing.

[44] Drew Rowny. Access the assistant in messages, plus the latest on rcs, Feb. 2019. Retrieved: February 09, 2024 from https://blog.google/products/messages/access-assistant-messages-plus-latest-rcs/.

[45] Johnny Saldaña. The coding manual for qualitative researchers. *The coding manual for qualitative researchers*, pages 1–440, 2021.

[46] Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Faith Cranor, and Julie Downs. Who falls for phish? a demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 373–382, 2010.

[47] Steve Sheng, Bryant Magnien, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd symposium on Usable privacy and security*, pages 88–99, 2007.

[48] Phillip Tracy. How to do a reverse phone number lookup without paying a dime, March 2021. Retrieved: February 11, 2024 from https://www.dailydot.com/debug/reverse-phone-lookup/.

[49] Melanie Volkamer, Karen Renaud, Benjamin Reinheimer, and Alexandra Kunz. User experiences of torpedo: Tooltip-powered phishing email detection. *Computers & Security*, 71:100–113, 2017.

[50] Heather Young, Tony van Vliet, Josine van de Ven, Steven Jol, and Carlijn Broekman. Understanding human factors in cyber security as a dynamic system. In *Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2017 International Conference on Human Factors in Cybersecurity, July 17- 21, 2017, The Westin Bonaventure Hotel, Los Angeles, California, USA 8*, pages 244–254. Springer, 2018.

A Appendix

A.1 Recruitment Script

This section describes the text we used for our recruitment process. This text was adapted for use in email campaigns, flyers, websites, and social media advertisements to recruit participants for the study:

Receive $25 if Selected for Our Research Study on SMiShing!

We are conducting a research study on SMiShing (fraudulent text messages) and are seeking participants to help us gain deeper insights into this issue.

About the Study: Our study aims to understand how individuals perceive and respond to suspicious or fraudulent text messages. SMiShing, or SMS phishing, is a growing cybersecurity threat, and your experiences and opinions can greatly inform our research.

Participant Criteria: We are looking for diverse participants who meet the following criteria:

- Aged 18 or older residing in Charlotte Metro area
- Use a mobile phone
- Can attend an in-person interview and bring their mobile phone

Study Details: The study will be an in-person interview at/near the UNCC campus. We kindly request that you bring your mobile phone to the interview session. You will be asked if you are willing to share any suspicious or fraudulent text messages that you have received on your phone. The interview is expected to last no more than one hour, and upon completion, you will be rewarded with a $25 Amazon e-gift card.

By participating in this study, you will help us develop a deeper understanding of SMiShing, its impact, and how individuals can protect themselves from such threats. Your insights will contribute to improved cybersecurity practices and awareness.

How to Get Involved: If you are interested in participating, please complete a brief eligibility survey to determine your eligibility and provide your contact information.

If you have any questions about the study, please contact Sarah Tabassum or Faculty Advisor, Dr. Cori Faklaris, at stabass2@charlotte.edu or cfaklari@charlotte.edu.

Thank you for your time and help!

A.2 Interview Guide

Greetings and Introduction: At the start of the study, participants will be greeted and introduced to the research topic. [Good Morning/afternoon. Thank you so much for participating in our study. The research topic is centered around identifying and understanding fraudulent text messages. We are doing this study to understand how users can identify fraud text vs. real text. We want to know about your experience and your opinion about such text messages. We will record the audio responses of yours. And for some questions, I will ask you to think aloud. Is that okay with you? Okay, let's get started then.]

Interview: During the interview, the following questions will be asked:

1. How frequently do you use your mobile phone for texting? What about the texting app on your phone?
2. Can you let me know what type of phone you use? For example, Apple, Android?
3. Which company provides your mobile service? [For example, are you with AT&T, Verizon, or Mint?]
4. Have you faced any privacy or security concerns related to your phone?

5. Have you ever received any fraudulent or suspicious text messages? Especially in the last three months? If yes, What was that? [At this point we will ask them if they can show us any such SMS on their phone. If they can, we will ask them to take a screenshot of that suspicious/fraud SMS and share with us.]

6. What did you do about it? Why? What influenced your decision?

7. Now, I will show you some Real and Fraud text messages to you for understanding your perception and decision-making process. [We want to understand the decision-making Process for each text message] For each text message we will tell them, “Describe the process you go through when deciding whether to trust a text message or not”.

8. When you receive a text message from an unfamiliar source, what are the first things you notice or look for?

9. Is there anything specific in a text message that makes you suspicious? For example, Are there any specific words, phrases, and visual elements that trigger suspicion?

10. Is there anything specific in a text message that makes it appear legitimate? For example, Are there any words, phrases, and visual elements that enhance legitimacy?

11. Do you pay attention to symbols or indicators (like a green checkmark, blue icon, or yellow warning sign) when judging the credibility of a text message? If so, please explain how these indicators influence your trust or suspicion

12. Have you received an SMS with such visual cues, and if so, how did they impact your perception of its legitimacy?

13. Are there specific colors, symbols, or icons in an SMS that make you more or less suspicious?

14. Where do you turn to for verification when you receive a suspicious text message? [Specific reasons for your choice and any phone features used for verification will be discussed.]

15. Have you received formal training or education on computer security/ cyber security or text message security? If so, please describe its effectiveness in preparing you to detect and respond to text message fraud, attacks, or spam

16. What do you do when you receive a fraudulent text? Why?

17. Do you report it? How do you report it? Why?

18. What are your expectations after reporting? And what actually happened?
    Now we will ask some questions for feedback:

19. How do you think text message interfaces could be improved to help users identify fraudulent text messages better?

20. Is there anything else you’d like to share on this topic?

[Thank you so much. That’s all I had to share today. We really value your thoughts and involvement. I will stop the recording now.] Additionally, participants will be provided with a document on "Best Practices to Identify Fraudulent Text Messages" for their reference.

A.2.1 Best Practices to Identify Fraudulent Text Messages

- Be Skeptical of Unknown Senders: Avoid clicking on links or responding to messages from unknown or suspicious senders.
- Double-Check the Sender’s Information: Verify the sender’s identity by cross-referencing contact details with official sources.
- Beware of Urgent Requests: Be cautious if the message conveys a sense of urgency, asking for immediate action or personal information.
- Verify Web Addresses (URLs): Scrutinize any links provided in text messages. Confirm the legitimacy of the website before clicking.
- Look for Spelling and Grammar Errors: Fraudulent messages may contain typos, incorrect grammar, or unusual language.
- Avoid Sharing Personal Information: Never share sensitive personal or financial information through text messages.
- Stay Informed about Scams: Keep up-to-date with common text message scams and fraud tactics to recognize red flags.
- Use Official Contact Channels: If you receive a message from a bank, government agency, or service provider, contact them through official channels to verify its authenticity.
- Enable Two-Factor Authentication (2FA): Use 2FA whenever possible to add an extra layer of security to your accounts.
- Report Suspicious Messages: If you receive a fraudulent text message, report it to your mobile carrier and the appropriate authorities.

- Educate and Share Information: Share knowledge about text message scams with family and friends to collectively protect against fraud.
- Verify Prize Winnings: Be cautious of messages claiming you've won a prize or lottery, as these are often scams.
- Trust Your Instincts
- Regularly Update Your Mobile Device

Remember that text message scams can take various forms, so it's essential to stay vigilant and employ these best practices to protect yourself and your personal information.

A.3 Code Book

Main Code	Definition	Sub-codes	Frequency	Sub-sub-codes	Frequency	Examples from Transcripts
Cues: Suspicious	Any anomaly or irregularity within the message that triggers doubt or concern about its legitimacy, indicating potential fraudulent or malicious intent	Suspicious Content	28	Links	17	"The one thing is the content of messages.. for example, if there is a link, I prefer to check the link. Not clicking, just reading the link, or something like that." [P2]
				Money Related SMS	8	"...if it's related to money, that would definitely become more suspicious." [P9]
				Generalized SMS	1	"..when it looks like a very generalized message, like it's being sent to thousands of people, and it's not personalized to me…" [P3]
				Personal Inquiry	2	"When they ask for my personal information, I become more suspicious." [P11]
		Unofficial Format	15	Wrong/Weird Names	4	"I saw there are some weird Google forms and they have some weird company names." [P8]
				Irregular/Special Characters	5	"...obviously like when they start using characters that are not letters. Okay, you know, and decimals that I have one in my phone.." [P16]
				Grammar/Spelling Error	6	" …some of them sometimes are misspelled and have random capitalization that I noticed." [P17]
		Unknown Sender	11	Any Unknown Sender	7	"Generally, if I don't recognize the sender and the message doesn't align with my daily life or the businesses I usually interact with, that makes me a little suspicious." [P5]
				Email	1	"If I receive a text from an email address, that's usually suspicious. I don't expect banks to use emails for text messages." [P25]
				Intl. Number	2	"I become suspicious if it is coming from some crazy international numbers..." [P27]
				5 digit short-code	1	"There are no strict rules or regulations for these numbers, so it's very easy to mask this type of five-digit code.." [P14]
		Out of Context SMS	6	-	-	"Like, I always ask myself, Was I expecting this SMS? Does it relate to my daily life? If not, I become suspicious." [P7]
		Immediate Action	4	-	-	"Yes, like 'call us now.' Okay? When they say immediate action is required, like things that need to be fixed right away.." [P25]

Main Code	Definition	Sub-codes	Frequency	Sub-sub-codes	Frequency	Examples from Transcripts
Cues: Legit	Trustworthy indicators within a text message that instill confidence in the message's authenticity	Contains Personalized Info	14	-	-	"I guess if it's more personal to me, I'm able to recognize it. Like if they mention something we've discussed before, or if they phrase it as if they've had a conversation with me" [P22]
		Known Context	11	-	-	"If it's from a bank or a place I go frequently, I will trust them." [P17]
		Known Sender	10	-	-	"If I've received texts from them before or if I know them, it's easier to trust. Many companies use the same number for messages. For instance, if it's from Amazon to verify my account, I'll have all our previous texts in that conversation. So if it's a company or bank that I've used before, I'd expect their message to come from the same number." [P12]
		Official Format	8	No Personal Info Inquiry	2	"Like, legitimate senders will never ask for your personal information. If I ordered something, they should already know about my info…" [P8]
				No Action Required	1	"Legitimate SMS will not ask for urgent actions like 'your card is blocked, call now,' or 'go to this link now', you know…." [P10]
				Correct Spelling & Grammar	1	"...if it's coming from a legitimate company or bank, I expect them to have proper grammar and no spelling mistakes, which are usually seen in fraudulent SMS" [P28]
				Correct Format	4	"..usually the companies follow some formats. I look for the correct format while judging legit SMS." [P6]

Main Code	Definition	Sub-codes	Frequency	Sub-sub-codes	Frequency	Examples from Transcripts
Initial Hook	The first thing they notice while judging legitimacy of an SMS from unknown source	Caller ID Information	18	Unknown Number	15	"...I always check the sender's number in the first place or where the SMS is coming from…" [P5]
				Area Code	3	"The area code where it's coming from is the first thing I check…It gives me a quick idea if the message is trustworthy or not." [P16]
		Content	15	Format of SMS	9	"Usually, the format of the text first grabs my attention, whether it's official or vague, you know…" [P27]
				Links	3	"...if it has a link, it gets my attention first…I become more suspicious about the text message…" [P9]
				Grammar/Spelling Error	3	"....always the spelling and grammar... the scammers usually have lots of spelling mistakes, I noticed." [P3]
		Context	5	-	-	"Like, I always ask myself, Was I expecting this SMS? Does it relate to my daily life? If not, I become suspicious." [P7]