What Are Brands Telling You About Smishing? A Cross-Industry Evaluation of Customer Guidance

Dev Vikesh Doshi
California State University San Marcos
doshi002@csusm.edu

Mehjabeen Tasnim
California State University San Marcos
tasni001@csusm.edu

Fernando Landeros
California State University San Marcos
lande029@csusm.edu

Chinthagumpala Muni Venkatesh
California State University San Marcos
muniv005@csusm.edu

Daniel Timko
Emerging Threats Lab / Smishtank.com
danielttimko@gmail.com

Muhammad Lutfor Rahman
California State University San Marcos
mlrahman@csusm.edu

***Abstract*—Phishing attacks through text, also known as smishing, are a prevalent type of social engineering tactic in which attackers impersonate brands to deceive victims into providing personal information and/or money. While smishing awareness and cyber education are a key method by which organizations communicate this awareness, the guidance itself varies widely. In this paper, we investigate the state of practice of how 149 well-known brands across 25 categories educate their customers about smishing and what smishing prevention and reporting advice they provide. After conducting a comprehensive content analysis of the brands, we identified significant gaps in the smishing-related information provided: only 46% of the 149 brands mentioned the definition of smishing, less than 1% had a video tutorial on smishing, and only 50% of brands provided instructions on how to report. Our study highlights variation in terminology, prevention advice, and reporting mechanisms across industries, with some brands recommending potentially ineffective strategies such as ”ignoring suspicious messages.” These findings establish a baseline for understanding the current state of industry smishing awareness advice and provide specific areas where standardization improvements are needed. From our evaluation, we provide recommendations for brands on how to offer streamlined education to their respective customers on smishing for better awareness and protection against increasing smishing attacks.**

I. Introduction

With the increased reliance on mobile devices over the past decade, there has been a dramatic rise in adversaries posing as reputable companies or representatives, and in customers falling victim to them [52]. Yet public awareness of the threat has lagged behind; fewer than 35% of the North American population is aware of what smishing is [19]. In 2024, the FTC estimated that text message scams, including smishing, resulted in $470 million in financial losses [33], a figure that is projected to continue growing [53]. Additionally, recent reports indicate that scammers are increasingly diversifying their targets, impersonating a wider range of organizations [5].

While phishing has been extensively studied in both academic and industry publications, smishing has received comparatively less attention, despite its growing prevalence [49]. The unique threats that smishing poses can be seen in their delivery method, and in how users interact with messages on mobile devices [37], [66]. As shown in Figure 1, taken from Smishtank [58], [59], [64], fake and real SMS from a brand can appear almost identical. With small changes to the URL (such as “uspw” instead of “usps”) or by using a phone number instead of a short code, users who lack technical knowledge or awareness of smishing are often tricked into believing the messages come from legitimate brands.

Given these clear risks to end users, many companies have publicly share anti-smishing awareness advice [4], [10], [14], [26], [54], [56]. These efforts aim to mitigate the risk of falling prey to attackers. While most advice is geared towards employees rather than customers in order to prevent data breaches [16], [43], brands also release information for their end users, which can help avoid reputational damage and indirect costs such as customer support and loss of business [11]. This customer-facing advice takes many forms, including videos, text, and multimedia instruction on how to spot an attack, as well as what to do when you identify an attack. With each company taking their own unique approach, the need arises to investigate the nature of the anti-smishing information given by brands and the tools they offer to end users to protect themselves from fraud [40]. This advice forms a key aspect of cybersecurity education. By examining how this advice is communicated and where it may fall short, we can identify areas where brands can better protect end users and their trust in the brand.

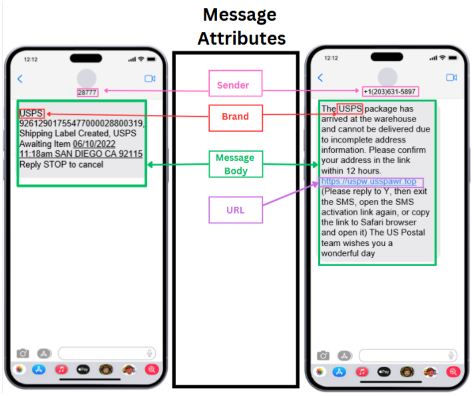
Cybersecurity education is widely recognized as key to preventing cybersecurity attacks, and brands can play a crucial role in this educational process [3], [32], [51]. Given their direct customer relationships and the trust they command, brands have a unique opportunity, and responsibility, to offer accurate anti-smishing guidance, particularly in light of the potential consequences of failing to address such attacks [29].

Symposium on Usable Security and Privacy (USEC) 2026
27 February 2026, San Diego, CA, USA
ISBN 978-1-970672-07-7
https://dx.doi.org/10.14722/usec.2026.23067
www.ndss-symposium.org, https://www.usablesecurity.net/USEC/

For example, according to a 2019 U.S. consumer survey commissioned by the brand-protection firm Incopro, 52% of respondents reported losing trust in a brand after unintentionally purchasing a counterfeit good online [27]. Moreover, a brand-trust survey by Mimecast found that 57% of respondents stated they would stop spending money with their favorite brand if they fell victim to a phishing attack impersonating that brand [38].

As primary targets of smishing attacks, brands are well-positioned to educate customers using their platform to provide tailored, trustworthy guidance. To understand the current state of industry practice for smishing awareness and advice, we conducted the first systematic content analysis of anti-smishing advice from major corporations, examining common themes, use of supplementary information, and post-incident guidance approaches. This foundational study aims to document what information and guidance brands currently provide, establishing a baseline for understanding industry practices. Our research questions are:

1) **RQ1:** How do brands define smishing and the methods to identify smishing attacks?
2) **RQ2:** What percentage of brands provide additional information such as external links, videos, or examples?
3) **RQ3:** What instructions do brands provide to prevent smishing, report a smish attempt, and what steps to take after becoming a victim of smishing?



USPS 92612901755477000028800319, Shipping Label Created, USPS Awaiting Item 06/10/2022 11:18am SAN DIEGO CA 92115 Reply STOP to cancel

The USPS package has arrived at the warehouse and cannot be delivered due to incomplete address information. Please confirm your address in the link within 12 hours. https://uspw.usspawr.top (Please reply to Y, then exit the SMS, open the SMS activation link again, or copy the link to Safari browser and open it) The US Postal team wishes you a wonderful day

Fig. 1: Screenshot of real (left) and fake (right) SMS of the same brand

To answer these research questions, we identified 149 popular brands from Smishtank [58], [59], [64] and Phishtank [63] and collected data from the websites of those 149 brands. We then performed a qualitative analysis of the advice offered by brands to educate their end users. We found that less than 50% of the brands mentioned smishing on their websites. Only 35% of the brands provided smishing examples, and less than 1% of the brands had video tutorials on smishing for their users. Brands defined smishing as an act of deception involving malicious links. To prevent their users from falling victim to a smishing attack, brands advised their users to trust their instincts and block the smishing contact.

Based on these findings, we recommended that brands standardize smishing definitions for better understanding. We also recommend mentioning simplified reporting methods and including government and carrier resources so users do not have to navigate each brand's specific reporting process. Another recommendation is for brands to invest in modern multimedia to educate their users about smishing attacks.

II. Related Works

Smishing Related Studies While smishing research remains limited, recent studies have shed light on user susceptibility to these SMS phishing attacks. Timko et al. found that US users, on average, achieved 65.60% accuracy in identifying fake SMSes compared to 44.6% for real messages [57]. Worryingly, response rates to smishing messages exceeded 15%, especially when senders posed as known brands or organizations. Given that the number of people falling for cyber attacks is increasing [28], new methods are constantly being implemented with the goal of reducing that number. For example, Sheng et al. [55] experimented with an online game that provided anti-phishing training to users. Toll scams, which often begin with SMS phishing, have also emerged as a threat. Recent work [41] analyzed thousands of scam domains, revealing registrar abuse, obscure TLD use, and coordinated registration bursts.

User Behavior Beyond detection accuracy, user behavior plays a crucial role in smishing success. Blancaflor et al. identified a "curiosity trap," where users tend to open suspicious messages to verify legitimacy, inadvertently exposing themselves to malicious content [9]. This behavior contributes to the 4.17% success rate of smishing campaigns. The blurring line between real and fake messages further worsens the issue, as users ignore 50% of genuine messages due to perceived smishing [45]. According to a study conducted by Neupane et al., users subconsciously process and identify aspects of real and fake links differently [44]. Similarly, Tabassum et al. explored factors that drive smishing susceptibility, examining how and why users judge a SMS message to be real or fake. These studies highlight the importance of message design and user education in differentiating between legitimate and fraudulent communications. Furthermore, a past study found that while many users do not recognize the term smishing, they are aware of the risk that comes with being a victim of an SMS attack [22]. Despite this, Downs et al. explained in their study that users have a hard time linking this awareness to their susceptibility to an attack [20]. These findings underscore the critical importance of clear, accessible organizational communication about smishing threats.

Research conducted by Karakasiliotis et al. concluded that cyber attacks have both psychological and technological dimensions [30]. Li et al. identified trust building as a crucial step for a phishing attack to succeed [36]. Alarmingly, Camp et al. found that many users trust their computer systems to the extent that they underestimate risks, which could explain why many users click on visually deceptive links [13]. A study by Cho et al. explored how various personality traits impact a user's willingness to trust someone [15]. They found that users with high levels of anxiety, i.e., neuroticism, were less likely to trust what they were sent and, in turn, were more likely to consider the associated risks. Attackers employ various techniques to deceive users, making it difficult to distinguish genuine messages from fraudulent ones. Drake et al. described a technological method for this by masking a URL address to appear as if it is sourced from a reputable website [21]. Another deception technique is emotional manipulation. Goel et al. [25] demonstrated that emotional manipulation can influence users' decision-making by eliciting feelings of fear and anticipation, proving emotions to be an effective way of getting someone to click on a harmful link. This extensive body of research highlights significant user behavioral vulnerabilities to smishing attacks. While previous studies have thoroughly demonstrated what makes users vulnerable to smishing attacks, there is limited understanding of what information organizations currently provide to customers about these threats. Our study systematically documents current organizational practices by presenting an evaluation of smishing education content and guidance that brands currently offer to help users recognize and avoid the behavioral manipulation tactics employed in smishing attacks.

How Brands Provide User Cyber Education With the escalation of smishing in recent years, the number of scammers impersonating reputable and trustworthy brands to deceive users is also increasing [47]. These kinds of attacks, where scammers pretend to be well-known brands, are becoming very common, and these scammers are becoming more advanced day by day. A report by the Federal Trade Commission noted an 85% increase in brand impersonation between October 2020 and September 2021, which resulted in losses of USD 2 billion [23]. Additionally, a report highlighted that eight in ten organizations (i.e., 80%) experienced at least one successful email-based phishing attack in 2022, which further emphasizes the critical need for enhanced cybersecurity education and awareness [47].

Cybersecurity education has become an essential tool in response to these threats, reducing user susceptibility to smishing. Education directed at improving user detection takes a wide variety of forms, and targeted training programs have been developed to help vulnerable populations. A study by Lastdrager et al. found that targeted training towards children and teens significantly improved their detection accuracy through training [34]. In a different approach, Wang et al. [61] found that cybersecurity education which employed evidence-based AI explanations for message detection was able to improve user detection of smishing across all age groups, with the greatest improvement in older adults. Effective cybersecurity education has the potential to equip users with the necessary knowledge and skills to detect and avoid cyber threats. Many research studies emphasize the significance of adopting effective, learning-based approaches to cybersecurity training. Bada et al. mention that educational efforts should go beyond merely providing information; they should be targeted, actionable, and practical, offering clear steps that users can implement immediately [7]. Additionally, Bhaskar et al. state that showing the aftermath of real breaches and highlighting how vulnerable organizations are to cyber threats is the best possible way to spread cybersecurity awareness [8].

In addition to traditional methods, brands have started adopting more user-centric cybersecurity education techniques, which include interactive models and game-based learning platforms. A study by Williams et al. demonstrated that a game-based approach in cybersecurity education effectively engages and inspires non-cyber students [65]. Similarly, research by Khan et al. highlighted the benefits of game-based learning platforms in enhancing cybersecurity education [31]. Organizations like Google have implemented free phishing quizzes to assess and improve user awareness [48].

Despite all the efforts, there is a significant gap in understanding how different brands educate their users about cybersecurity, especially smishing. Our research study aims to fill this gap by conducting an extensive content analysis study of 149 brands. We examine whether brands spread awareness about smishing, what awareness they provide, and how they want their users to approach smishing attacks based on their unique brand strategies. By systematically cataloging current approaches, we seek to establish a baseline understanding of industry practices and identify the range of strategies currently employed. We also aim to document common patterns and approaches found across different organizations' smishing education materials. Through this analysis, we aim to map the current landscape of organizational anti-smishing communications and identify gaps where industry practice could be strengthened or standardized.

III. Methodology

This study analyzes anti-smishing cybersecurity advice provided by 149 U.S. brands that are highly represented in public phishing and smishing datasets. To assess both the content and comprehensiveness of corporate guidance, we employed a mixed-methods approach combining systematic content collection, qualitative coding analysis to identify thematic patterns in advice, and quantitative frequency analysis to measure the prevalence of educational elements that can help prepare users for smishing attacks.

We collected data across eight categories addressing the full lifecycle of user engagement. Five categories captured text content for qualitative analysis of the advice and guidance regarding smishing, while three used binary coding for quantitative analysis to measure the presence of smishing-related resources. For each brand, we systematically searched official websites for smishing-related guidance. We performed qualitative analysis using open coding techniques in ATLAS.ti, with AI-assisted initial coding followed by rigorous manual validation and iterative refinement.

The methodology includes brand selection from Smishtank and Phishtank databases based on frequency of impersonation reports, systematic data collection from official brand websites, and codebook development through hybrid AI-assisted and manual coding processes.

Categories	Description
Definition of smishing	The company's definition of smishing, including definitions of phishing via text message or SMS.
How to identify smishing	Details commonly found in smishing messages.
Is there a video tutorial provided?	If a video tutorial on smishing is provided.
Are there examples of smishing provided?	If explicit examples of what a smishing message might look like are provided.
Are there any external links provided?	If external links are mentioned for further help or guidelines.
Steps on how to report fraud	Instructions on how to report a suspicious text message.
Steps to take after becoming a victim	Instructions for smishing victims to mitigate damages.
Smishing prevention advice	Advice on preventing customers from becoming victims of smishing.

TABLE I: Description of categories

Category	Count
Technology & Software	25
Retail & E-commerce	23
Finance & Banking	23
Telecommunications	7
Social Media	6
Automotive & Ground Travel	6
Cybersecurity & VPN	6
Food & Beverages	5
Gaming	5
Payment Services	5
Logistics & Delivery	4
Health & Pharmaceuticals	4
Insurance	4
Housing & Utilities	4
Entertainment/Streaming	4
Dating Platform	3
Air Travel	3
Government	3
News & Information	2
Finance & Investments	2
Cryptocurrency	2
Education	1
Non-Profit & Advocacy	1
Food Delivery	1

TABLE II: Distribution of the brands

A. Brand selection

We selected brands from phishtank.com [63] and smishtank.com [58], [59], [64]. Both of these websites are known for reporting phishing and smishing attempts, respectively. We identified the most reported brands on these two websites and only selected the brands that are popular in the United States region. Choosing frequently reported brands allows us to cover the brands that are commonly impersonated. Their popularity was determined by the number of phishing reports linked to each brand.

We selected a total of 149 distinct brands to have a diverse and healthy range of data. The brands selected were from a wide range of categories, including but not limited to Technology & Software, Retail & E-commerce, Social Media, and Food and Delivery (mentioned in detail in *Table II*). Choosing from a diverse range ensured that we analyzed brands across different sectors. The full list of all brands chosen for each category can be found in the appendix.

B. Data collection

For the data collection process, we included eight distinct categories designed to answer our three research questions. The categories included:

1) Definition of smishing (**RQ1**)
2) How to identify smishing (**RQ1**)
3) Are there video tutorials provided? (**RQ2**)
4) Are there examples of smishing provided? (**RQ2**)
5) Are there any external links provided? (**RQ2**)
6) Steps on how to report fraud (**RQ3**)
7) Steps to take after becoming a victim (**RQ3**)
8) Smishing prevention advice (**RQ3**)

The choice of coding topics reflects major challenges across the full lifecycle of user engagement with smishing threats. That being, what is smishing, how you identify it, how to mitigate it, how to report it, and what to do if you have fallen victim. Researchers have made strong cases for the importance of each of these topics [35], [42], [50]. Additionally, these choices closely align with categories of focus by CISA [18].

These categories (described more in *Table I*) ensured that we collected enough information to correctly analyze and answer our research questions in a structured manner. Each of the categories covered a distinct aspect of this study. For example, "Steps to take after becoming a victim" and "Steps on how to report fraud instructions" were designed to answer **RQ3** (What instructions do brands provide to prevent smishing, report a smish attempt, and what steps to take after becoming a victim of smishing?).

We analyzed the websites of each of the 149 brands thoroughly. This included visiting the website of each brand, and searching for the smishing and smishing-related terms to find any help or guidelines provided. The search terms included smishing, scam or spam texts, SMS fraud, and SMS phishing. We also used Google site-specific searches with these phrases (e.g., 'site:brandX.com smishing') to identify smishing-related pages within each brand's domain. If the brand's website did not have a search feature, we manually reviewed the FAQ, Help, and About pages of the brand to look for smishing guidelines. If we did find any information or guidelines related to smishing, we copied it into our dataset.

We maintained an Excel sheet to track and store our data. We had one column for each of the above-mentioned eight categories and additional columns for the brand name, link to the website where the information was provided, and category of the company. Each set of information found on a brand's website was mapped to its respective column. For the categories, "examples of smishing," "video tutorials provided," and "external links included," we recorded binary values ('Yes' or 'None') to enable quantitative analysis of prevalence across brands. For the remaining five categories, we collected the full text of the category content from brand websites for subsequent qualitative coding analysis.

C. Codebook Development

After the data collection, we moved on to data analysis. We conducted qualitative analysis using open coding techniques [24]. We used ATLAS.ti for initial coding and dataset organization [62], leveraging its integration of fine-tuned OpenAI models [6] to generate preliminary codes. While automated coding differs from traditional open coding methods, Computer-Assisted Qualitative Data Analysis Software (CAQDAS) tools are used in qualitative research, particularly when combined with human validation [2], [39]. We used AI-generated codes as a starting point and then performed a thorough manual review, refining the codes through team discussions. This hybrid approach ensured the rigor and reliability of our analysis.

Using the CAQDAS tools, the lead researcher coded all data to create the primary codebook, which was then manually reviewed by two additional coders. The lead researcher worked with the additional coders, who reviewed the codebook and coded data to discuss emerging themes and refine the codes. Discrepancies identified during review were resolved through collaborative discussion, ensuring alignment in interpretations and reducing potential bias. This iterative process continued, allowing for adjustments to the coding scheme as new insights emerged, until distinct and well-defined themes were established that effectively addressed each research question. The full codebook is provided in the appendix section.

IV. Results

A. Answering RQ1

1) Smishing Definitions: The study identified several themes regarding smishing techniques and their characteristics. Deceptive messaging emerged as a prominent strategy, with brands frequently highlighting messages that impersonated brands or persons to appear legitimate. As one brand mentioned,

> *"One way phishers try to gain this information is by posing as a reliable company or person in emails, texts or direct messages. They will send some form of communication asking for verification, information updates, financial updates or even just try to get you to navigate to a provided link. (Yahoo)"*

This aligns with the theme of requesting personal information and embedding malicious links, with such tactics designed to manipulate users' trust and urgency.

Another recurring theme was the creation of urgency, with messages instructing users to "act immediately" or risk consequences. For example, a brand shared,

> "*Creating a sense of urgency to pressure the recipient into taking immediate action. (ExxonMobil)"*

Smishing was also recognized as a type of social engineering attack, often involving short URLs or trustworthy entities to obfuscate the malicious intent. Brands described these tactics as a manipulative approach to electronic fraud activity, emphasizing the psychological tricks used to extract information or provoke action. One brand summarized this succinctly, stating,

> "*Smishing is a form of social engineering attack where attackers use SMS (Short Message Service) or text messages to trick individuals into divulging sensitive information, clicking on malicious links, or taking other malicious actions. (Berkshire Hathaway)"*

Some brands also refer to smishing as SMS phishing, as phishing is a more widely known term, as stated by one of the brands,

> "*Smishing, or SMS phishing, is a phishing technique. (NordVPN)"*

A brand also defined smishing as a technique to install malware through malicious links and then further extract a person's personal information. For example,

> "*often similar to texts you might receive from legitimate businesses. If you click the fake link, you might be asked for personal information or get malware installed on your phone that can extract information automatically. (Navy Federal Credit Union)*"

Another theme that we observed was defining smishing as an SMS that used fear as a strategy to trap a victim. This tactic would make the participants more vulnerable to falling into the smish trap. As mentioned by a brand,

> "*Urgent or Threatening Language: Smishing messages often create a sense of urgency or contain threats to prompt immediate action. (IBM)"*

Adding to this, a brand also defined smishing as a text message that creates a sense of urgency, preventing the victim from taking the time to make an informed decision. For example, a brand wrote,

> "*Smishing messages often create a sense of urgency or include threats to prompt immediate action. (Amazon)"*

Out of the 149 brands that we analyzed, we found that only 46% of brands defined smishing. Each of the 69 brands that defined smishing had similar definitions as described in the above themes. However, it is important to note that more than 50% of brands did not even mention what smishing is. This is a significant concern, as there have been instances where smishing attempts have been made by attackers pretending to be the brand. When users visit the websites of brands that do not mention smishing, they have no idea about smishing.

2) How to Identify Smishing: The study highlighted some critical themes on how scammers operate during a smishing attack and the signs of identifying them. The most recurring theme was asking for personal information. Most brands warned users that requests for sensitive data such as credit card numbers, bank account details, PINs, CVV codes, one-time passwords, or even full names can be a clear indication of smishing.

Another significant theme was the sense of urgency in the smishing text. Scammers use these tactics to pressure victims into acting quickly, giving them less time to contemplate their actions. These urgent requests are usually to log in, send money, or confirm account details. As one brand explained,

> *"Urgent or Alarming Content: Smishing messages often convey urgency or alarm to prompt immediate action (Coco Cola)."*

Unexpected links or attachments from senders were also seen as a common theme in this study. If the text contains unusually lengthy links or unexpected attachments, that is a big red flag. As one brand noted,

> *"Phishing emails may include attachments claiming to be a 1099 tax document or other important files (Robinhood)."*

These links in the SMS sometimes mismatch with the official service provider's email. Even though the links are usually lengthy, it does not mean short URLs are secure. Often, scammers shorten URLs to mislead people. To combat this, brands recommend hovering over any link to preview the URL without clicking, as highlighted in the advice:

> *"If the message includes a link, hover over it (without clicking) to preview the URL. Verify that the URL is legitimate and related to the claimed sender (Walmart)."*

Misspelled websites or email addresses in the SMS are another big red flag. Communications from any legitimate company are well-written and error-free. Misspellings, poor grammar, inconsistent fonts, or odd markings are clear indicators of smishing attempts. As one brand highlighted,

> *"Lack of proper grammar and punctuation, many of these scams originate from foreign countries(Consumer Cellular)"*

Trusting the user's instincts is also a major theme found in the study. If a message seems even slightly suspicious, the user should stop engaging and think before taking any further steps. As one brand emphasized,

> *"If something feels off or too good to be true, it might be a smishing attempt (Walmart)."*

Scammers often lure victims with claims of winning large sums of money, sponsored lotteries, fake prize notifications, gift cards, or promotions. These tempting offers are made to attract people, as mentioned,

> *"Scammers may also contact you with attractive offers for free stock or other enticing deals to lure you in (Robinhood)."*

Requests to download apps, install software, or be directed to third-party websites are additional indicators of smishing. Scammers attempt to gain access by provoking victims to install malware on their systems. Therefore, any request to download a third-party app or involve a different party for any kind of activity is highly suspicious and a clear sign of smishing, as a brand mentioned,

> *"Hulu will not direct you to an unfamiliar third party for support. We will never direct you to install third-party software in order to troubleshoot (Hulu)."*

Requesting funds for various activities is another common scamming tactic. Scammers ask for payments, claiming they will apply for a job, pay insurance or delivery fees, or provide administrative fees for grant funds. Usually, they include a third party to fulfill the payment, making it an obvious scam.

Brands have mentioned that scammers try to pretend to be a brand that most people trust. They often impersonate well-known service providers like Instagram, claiming to be from their security team to extract account information. They manipulate the links to make them look like the authentic service provider's email address or phone number, so victims get confused. For example,

> *"The sender's email or phone doesn't match the name of the company that it claims to be from (Apple)."*

Scammers also use emotional manipulation techniques. As one brand mentioned,

> *"Emotional appeals—attempts to lean on a personal connection, either new or preexisting, can be a way to get you to stop thinking rationally and leave you vulnerable (Discover)."*

They sometimes behave overly friendly but make persistent requests. On the other hand, they may impose threats to instill fear in victims, leading them to take immediate but wrong actions and fall for the scam. One brand noted,

> *"Alarming threats of drastic consequences involving financial and legal issues if there is not an immediate response (Consumer Cellular)."*

Out of the 149 brands analyzed, 57% (85 brands) did not provide any instructions on how to identify smishing attempts. Only 43% (64 brands) offered guidance, leaving a significant portion of users without the necessary resources to recognize and avoid these scams. This gap in support is significant given that we these are popular brands that have already been targeted. This absence of smishing-specific educational resources not only makes users more vulnerable, but also highlights the importance of providing a standardized guidelines to avoid confusion between end-users. Without a consistent standard approach to educational resources, users are left to distinguish their legitimate messaging from the spoofed version on their own, raising the risk of exploitation.

RQ1 Summary: Different brands have their own ways of defining smishing. The spectrum of definitions ranges from smishing being an act of deception to impersonating a brand or person to SMS involving short links. For providing guidelines to identify smishing attacks, some brands mentioned noticing technical details like checking the link address, sender's details, and if the SMS contains any attachments, whereas other brands mentioned trusting personal capabilities such as following emotional appeal.

B. Answering RQ2

1) Video Tutorial: We also analyzed how many brands provided a video tutorial on smishing. Videos can depict a better scenario of what a smish message looks like, what a malicious link looks like, and what red flags to look for while examining an SMS. Moreover, these video tutorials can also walk through the process of identifying a smish, correctly reporting and blocking the sender, and the steps to take after becoming a victim. Videos offer a multimodal learning experience by integrating text, audio, and visual elements, which can enhance engagement and is preferred by some users when compared to text-only content [1], [60].

We found that only 1 out of the 149 brands we explored provided a video tutorial on smishing. This indicates a lack of interactive videos and examples mentioned by the brands on their websites. This also highlights and encourages scammers to use different tools and leverage the lack of awareness to scam more potential victims. Exploring modern multimedia tools and providing cybersecurity awareness in an interactive way could strongly portray the brand's commitment to the safety of its customers, as even suggested by Bada et al. [7].

2) Smishing examples: We explored how many brands provide a smishing example on their website. Smishing examples can explain a smish in a digital way compared to text content. These examples would help customers understand what a smish looks like and depict scenarios used by attackers. Seeing examples would also help potential victims understand the specific scenarios of urgency or fear a smish could create. For example, a bank could have smish examples of fake scenarios like payment failures or fraudulent transactions.

Only 35% of the 149 brands we explored mentioned a smishing example or screenshot. This indicates a significant gap in educating customers about the specific smishing scenarios of the respective brands. It also highlights the brands' failure to utilize modern multimedia options to better explain a cyber attack rather than just writing text. Providing examples and screenshots can greatly aid user understanding of smishing scenarios and potential attacks specific to each brand.

3) External Links: Out of the 149 brands we explored, 47 brands provided external links as additional resources for their users. These external links vary from personal websites of the respective brands to links from sources such as law enforcement agencies. However, less than 50% of the brands provided an external link reference, the brands provided some valuable extra information on smishing for the user.

These links provided users with further guidance and support in case they did not have enough knowledge about the aftermath of the smishing. Some brands (for example, Instagram) direct the users to their official support page which has tips about keeping your account safe. Some brands direct to blogs or posts posted by cybersecurity organizations on how to protect user privacy online. By providing these links, brands not only educate and prepare their user to be safe from scammers but also give them useful resources to equip them with proper tools in case the users need further help to report the smishing.

RQ2 summary: We observed less than 50% of the brands provided additional and interactive information such as external links, video tutorials, and smishing examples. However, the brands that did not provide any additional information, listed valuable insights and helpful resources for their user. For example, a few brands provided screenshots of previously reported smishing scams for the user to have a better understanding. Some brands even provided links to government helplines for best reporting practices and official guidelines to follow concerning smishing. Overall, a small proportion of brands provided additional information but those who did provide had mentioned important and true resources.

C. Answering RQ3

1) Reporting Instructions: The study identified several key themes regarding instructions for reporting fraud. Reporting to the respective brand was the most emphasized approach, with brands frequently noting how this step ensures that responsible brands are informed promptly. This also ensures, that the smish attempt is correctly reported and the required steps are taken to avoid a future scam. Furthermore, this suggests that respective brands have different ways to block and report the sender as per the type of brand, so it is best to refer to and apply the methods defined by the respective brand. As one brand mentioned,

> "*If you see something that you believe is a scam, avoid responding or interacting with it and report it to Instagram immediately. (Instagram)*"

Another significant theme was the role of government authorities and specialized agencies. Brands often mentioned forwarding fraudulent messages to entities like the FTC, FBI, or the cybercrime division, with one brand sharing,

> "*Consider filing a report with the Federal Trade Commission and/or state attorney general's consumer protection office, or the FBI. (Costco)*"

Additionally, using designated numbers like 7726 was highlighted as a quick and effective way to alert service providers about spam or phishing attempts.

The inclusion of specific details in reports also emerged as a key theme. Brands described how providing timestamps, screenshots, and scam details added credibility and clarity to their reports. For instance, one brand mentioned,

> "*Text message: Screenshot the message and include the number that contacted you Phone call: Include the phone number from the call and share as much detail as possible (Robinhood)*"

This approach aligns with the importance of utilizing online reporting platforms and official channels to streamline the reporting process.

Finally, brands noted preventive measures such as marking fraudulent messages as spam and deleting them. One brand summarized this sentiment, stating,

> "*Report spam in Google Messages When you report a conversation as spam, you also block the sender and move the message to your "Spam & blocked" folder. (Google)"*

Some brands even mentioned educating others about the scam and spreading awareness so people are notified and alerted. As one brand stated

> "*Alert Your Contacts: If the fraudulent instructions involve requests to your contacts or associates, inform them about the potential scam. This helps prevent the spread of the scam to others. (Walmart)"*

Out of the 149 brands that we analyzed, we found that only 50% of the brands provided steps on how to report a smishing scam. The other 50% are popular brands that have no instructions defined on how to report a smish attempt. This also supports the fact that lack of reporting which further creates a lack of awareness is one of the common reasons for smishing scammers to survive and scam more and more victims [46].

2) Steps After Becoming a Victim: The study highlighted some core themes on what to do after becoming a victim of a smishing attempt. Almost all the brands ask the user to call or inform them immediately if the users think they have been scammed. If any bank information was shared with the scammer or there was a financial loss of any kind, brands highly suggest contacting the bank immediately and getting help from them. Some brands also ask the victims to report the scam and forward the message to the mobile carriers. As one brand stated,

> *"If possible, forward the smishing message to your mobile service provider, as they may use it to improve their security. (IBM)"*

Brands also encourage the victims to report the scams to appropriate law enforcement agencies. Filing a complaint to the Federal Trade Commission (FTC) is the most common law enforcement agency that was brought up by those brands. Some other agencies that were mentioned are the Internet Crime Complaint Center, the state Attorney General's office, local cyber-crime unit. local or state police agencies. In the case of any identity theft, one brand suggested filing an affidavit at www.identitytheft.com.

Another significant theme was to change their password to a stronger one and incorporate uniqueness for any accounts that were compromised and then log out from all devices. Brands also recommend to not use the compromised device if possible just to be cautious about any malware. One brand mentioned,

> *"Stop using the device. In fact, don't even use the affected device (laptop, phone) to change your passwords. It may be infected with malware that will collect your new passwords, leaving you no better off than before (Synchrony)."*

Regular monitoring of the accounts is also one of the crucial themes found in the study. The accounts that have been compromised before to detect any suspicious activity. Monitoring financial accounts was emphasized for any unrecognized transactions.

After becoming a victim, scanning the device with an anti-virus is necessary to be protected from any possible malware. If any anti-virus is not already installed, brands recommend installing a reliable anti-virus and scanning the infected device with it as soon as possible.

At any point, if there is any other text that seems to be suspicious, do not engage. Brands also say not to click any links that do not look reliable. When interaction has already been established, cease any communication immediately because replying can trigger future smishing attempts as the scammers know the number is active. In that situation, brands ask victims to stop using the device. For example,

> *"Then, disconnect the potentially infected device completely from the internet and cell service, which will help isolate any issues. (Synchrony)"*

For an extra level of security, several brands emphasize enabling two-factor verification whenever possible for accounts. As one brand mentioned,

> *"This adds an extra layer of security by requiring a second form of verification in addition to your password. (Tech Mahindra)"*

Finally, brands noted some general measures such as information from family, friends, and colleagues so scammers cannot harm them. Being calm and collected is important so the situation does not get worse. Blocking those smishing phone numbers is crucial. It was also recommended to learn about cybersecurity and do some research online to be aware of safety in the future.

Out of the 149 brands analyzed, 65.77% (98 brands) did not provide any clear steps for users to follow after becoming a victim of smishing scams. Only 34.23% (51 brands) offered guidance, leaving a majority of users without critical support during such incidents. This underscores a significant gap in victim assistance and highlights the urgent need for brands to prioritize victim-focused measures to address this vulnerability.

3) Smishing Prevention Advice: The study identified a range of strategies for preventing smishing attacks, with an emphasis on user vigilance and proactive security measures. A prominent theme was avoiding interactions with suspicious content, particularly refraining from clicking links or opening attachments, which was frequently cited by participants. As one brand explained,

> "*Don't click a link if you're not sure about it; go directly to the company website instead. (Netflix)"*

Similarly, exercising caution when engaging with SMS and verifying the legitimacy of senders emerged as critical preventive measures, highlighting the need for skepticism.

Another significant theme was the protection of personal information, with brands emphasizing the importance of not sharing sensitive data such as account credentials or financial details. For instance, one brand noted,

> "*Never provide personal or financial information unless you are certain of the identity of the person or business that is contacting you. (Walgreens)*"

Brands also stressed the necessity of verifying sender authenticity multiple times before transferring funds, underscoring a measured and cautious approach to potential threats.

Technical safeguards were another recurring theme. Installing the latest antivirus software, enabling two-factor authentication, and maintaining strong passwords were commonly recommended actions. Brands highlighted the value of such precautions, with one noting,

> "*Make sure your devices and security software are up to date. Consider installing anti-malware software for added security. (Capital One)*"

Additionally, double-checking website URLs and relying only on official apps or platforms for transactions were identified as critical strategies to avoid SMS phishing traps.

Brands also highlighted the importance of proactive measures, such as reporting suspicious messages to brands or marking them as spam to minimize future risks. Educational initiatives like cyber awareness training and staying updated on the latest cybersecurity scams were seen as vital tools for preventing smishing. As one brand stated,

> "*Complete our Cyber Fraud & Secure Online Banking training in the Support & Community Section of J.P. Morgan Access (J.P. Morgan)*"

Finally, brands advocated for vigilance and skepticism when encountering unexpected requests, such as demands for payment for hospital or utility bills. Practices like constant account activity monitoring, recognizing red flags, and trusting instincts were also highlighted as effective deterrents. One brand succinctly captured this sentiment, stating,

> "*Regularly check your account activity for any suspicious transactions and contact us immediately about any suspicious or erroneous wires. (J.P. Morgan)*"

and another brand mentioned,

> "*Be skeptical of unexpected calls, emails, or messages asking for sensitive information. Trust your instincts and take precautions to ensure you're protected. You can stay one step ahead of scammers by always verifying what you're being told—even if it means hanging up or ignoring a message until you're sure. (Navy Federal)*"

Out of the 149 brands that we analyzed, only 69% of the brands provided advice on how to prevent smishing. The brands that provided the content on how to prevent smishing had guidelines related to the above themes. The remaining 31% of the brands had no mention of steps to identify smishing. The customers of these brands unfortunately are not educated about the scenario, even though these were popular brands whose names were part of previously reported smishing scams. This lack of content supports that lack of awareness increases the chances of a victim falling into a smish trap as the victim is not educated enough on smishing prevention.

RQ3 Summary: Even though different brands provide different advice on how to report smishing and steps after becoming a victim, they have a lot in common. The pieces of advice range from trusting user instincts, and blocking the smishing account to reporting smishing to law enforcement agencies. All the brands who provided the advice related to smishing reporting recommend either reporting or taking some level of action in one way or another.

V. Discussion

A. General Discussion

In this study, we analyzed the smishing awareness and prevention education provided by 149 distinct brands. We leveraged encoding techniques and identified relevant themes that most of the brands highlighted. We discovered that a greater percentage of the brands don't mention relevant or sufficient information on smishing, even though there have been smishing attack attempts using the brand's name. Below, we discuss and conclude the findings from each of the categories that we analyzed qualitatively:

Smishing Definitions: Brands differed in how they defined smishing to their customers. They most commonly portrayed smishing as an act of deception involving text messages, a malicious link, and a feeling of fear or urgency. There were also references to technical definitions like a type of social engineering attack, SMS phishing, and spam text. Some of the brands did not even mention the definition for smishing. This inconsistency highlights the need for a standardized, user-friendly definition. Brands should consider adopting definitions from authoritative sources such as CISA, which offer their own definition on smishing [17]. Using federal agency definitions as a foundation promotes consistency across platforms, while still allowing brands to tailor their messaging to the specific threats their users may face.

Prevention Advice: The prevention advice analyzed from different brands implied a mix of user-focused strategies. For example, always being cautious while interacting with an SMS and always verifying the sender and any links before reacting to an SMS. On the contrary, technology-focused strategies like two-factor authentication, constantly tracking account activity, and using firewalls were not emphasized much. While user behavior plays an integral part in a victim falling into a smishing attack [9], technical safeguards are also important to increase resistance against falling for a smish.

Reporting Fraud Instructions: Different brands had different ways of dealing with smishing attack reports. While some brands suggested directly reporting a smishing attempt to the respective brand, others suggested seeking government aid and reporting to anti-phishing organizations or local consumer protection agencies. We observed that not many brands (n=6) mentioned reporting the smish message to 7726, which is an official government helpline for reporting smishing messages. Some brands even mentioned reporting the message to the respective provider. This highlights the need for brands to mention both government resources and the brand's resources (if there are any) for reporting a smish message, to ensure a better and more detailed scrutiny of the smish attempt.

Identifying Smishing: Different indicators were suggested by different brands to identify a smishing attempt. The most common themes included SMS requesting personal information and SMS portraying a sense of urgency, both of which prompt the user to take quick action. Unexpected links from senders, cross-checking with the brand, and trusting personal instincts were also common themes. Additional markers highlighted were grammatical errors, fake offers, and money lending. All these prominent themes indicate that potential victims should always be alert and on their toes. Having cyber and smishing education also plays a significant role in identifying a potential smish message.

Steps to take after becoming a victim: While there were not many brands that included the steps to take after becoming a victim, some did suggest detailed steps. Informing the service provider, reporting to law enforcement, and changing login credentials were the most prominent themes in the qualitative analysis. A few brands also suggested monitoring the account and installing antivirus software to neutralize the attack and prevent any potential loss. Less common themes included blocking scam numbers, remaining calm, and seeking advice from the respective brand. While all of these suggestions are valid, there is a need to define the steps to take after becoming a victim in a more streamlined manner. The steps should cover protecting accounts and given information, appropriately reporting the smishing attack, and measures to take to avoid a potential attack in the future.

B. Recommendations

After conducting a comprehensive qualitative analysis of smishing awareness advice provided by major tech companies and financial institutions, several recommendations emerge to enhance cybersecurity resilience and protect individuals and organizations from smishing attacks:

Standardization of smishing Definitions: Brands primarily defined smishing as a "deceptive message" or "a message impersonating a brand or a person." However, "SMS containing a short URL" or "social engineering attack" wasn't mentioned much. This leads to ambiguity and incomplete education for the brands' customers. There is a need for greater standardization in cybersecurity and smishing education provided across different brands. While variations tailored to each brand's content are noted, aligning definitions with industry best practices can promote consistency and clarity in anti-smishing efforts. Further, expanding the scope to include critical identifiers like "short URL" would also provide comprehensive exposure to smishing education and common smishing tactics for potential victims.

Simplifying Reporting Methods: Reporting methods like "Report to respective brand" and "Contact FTC" were widely suggested. However, using official channels or reporting to 7726 was not mentioned much. This causes a problem in streamlining a reporting mechanism for the victim, who has to navigate different and complex reporting instructions depending on the brand. This fragmentation aligns with recent calls for improving fraud reporting infrastructure, as Button et al. [12] identified inadequate reporting and intelligence coordination as critical barriers to effective fraud response, particularly for cross-border threats. We suggest that brands should include a more streamlined reporting method and incorporate government and carrier reporting methods for a more efficient reporting process. Another possible solution could be, popular phone companies (like Apple and Google) or network providers (like AT&T and Verizon) could inform the respective brand whenever their users report a smishing attempt to them.

Improve Smishing Identification and Prevention Education: Identification methods such as "SMS creates a sense of urgency" and "SMS contains unexpected links" were widely mentioned across the websites of different brands. However, important details like "shortened URL" or "includes attachments" were not covered. For prevention advice, basic yet vital instructions such as "Don't click any links" and "Always be cautious" were briefly covered across most brand websites. However, we observed that tips like "Check website URL thoroughly" and "Trust instincts" received limited mention.

Based on these findings, we recommend that brands provide more streamlined yet detailed education and content on smishing identification and prevention methods. Prior research also shows that more actionable and practical approach of providing cyber education is recommended [7]. Brands can utilize modern multimedia tools to design interactive educational content for better user understanding. To imply this, even if a game-based approach works better as suggested by Khan et al., brands should invest the resources to create this particular awareness [31]. Streamlining these aspects would help potential victims be cautious and detect smishing in its early stages. This would further assist victims in reporting the smish attempt and securing their personal information.

Provide examples and video tutorials: Only 35% of the 149 brands that we explored provided smishing examples, and less than 1% provided a video tutorial related to smishing. Examples and visual content could help a potential victim in numerous ways, such as: What does a smish message look like? What does a malicious link look like? What red flags should be looked for when inspecting a text message? How to report a smish message? How is malware installed through a link?

Reading plain text content can be boring for users and presents a greater challenge in maintaining their attention [1]. Instead, we recommend that brands invest in educational videos and interactive content for their users to better understand this type of scam. Interactive content like quizzes and puzzles could greatly attract more users to learn about smishing. Examples of previous smishing attempts would also help users understand scenario-based smishing. For example, in a bank scam, the scenarios would include asking for OTP or bank passwords. This scenario education would help to immediately alert the user when they see a text message with a similar scenario. It would also provide the user with a real-life walkthrough of a smish attempt.

Overall, by implementing these recommendations, brands can strengthen their smishing awareness efforts and effectively mitigate the risks posed by this prevalent form of cybercrime. Brands can increase their defenses against smishing attacks and empower users to recognize and respond to potential risks more effectively.

C. Limitations

Despite our best efforts, this research does have areas for improvement and elaboration. For example, while we feel our collection of meaningful data is solid, there are ways to improve it to reflect further findings. Also, the number of brands in each category is not equally divided. For example, we analyzed 25 Technology & Software brands but only 4 Entertainment/Streaming brands. This also made it difficult to analyze and compare data across different categories. We selected brands that have already been found to be targeted by phishing and smishing attacks from Phishtank and Smishtank. To our surprise, we found that some of these brands did not have a webpage to warn customers about phishing or smishing, which is most concerning. The research team decided to take content from web pages from brands listed on Phishtank and Smishtank. There are possible chances we could have missed a few brands that are popular in smishing scams.

Additionally, we are analyzing content from web pages whose companies are based in the United States. There is an opportunity for other works to analyze corporations on a global scale or a more isolated approach using a different country as the company's base of operations. Companies are often held to different standards depending on which country they operate under, both publicly and legally. Therefore, it is reasonable to inquire whether this affects preventive advice or lack thereof.

Another limitation is the use of publicly available content. These companies may engage in more activities to prevent customers from becoming victims of smishing; however, the research team decided to exclusively analyze content from reputable web pages as it can be difficult to find other such programs by the company.This means the study is limited to the brand awareness reflected on their websites, while companies may have employed other strategies, such as videos, awareness campaigns, or social media outreach to educate customers. Another thing one must acknowledge is that this research is reliant on this public information and does not have access to any private preventative advice that may be taking place. This may manifest itself in the form of internal company communication or training programs, which could be part of a larger effort of combating SMS phishing.

During the encoding process, we came up with the theme 'explicit definition,' and we determined that mentioning that phishing can be done through SMS constituted or was enough to be considered an explicit definition. However, upon closer inspection, it can be argued that this is also a missed opportunity for further analysis. It can be valuable to differentiate and analyze how frequently these web pages actually mention smishing by name rather than passively mentioning it as an avenue through which phishing is done. If we were to repeat this study, this change would certainly be employed.

VI. Conclusion

Smishing attacks are rising over time. Brands are taking initiatives to provide awareness advice to their customers to reduce these attacks. In our study, we analyzed advice from 149 various brands that are most likely to be targeted by smishers and revealed several themes or strategies. We found that less than 50% of brands mentioned smishing on their website and less than 1% had a video tutorial. Smishing attacks are increasing exponentially day by day, and the lack of smishing awareness is one of the major reasons victims fall for a smish attack. Thus, we recommend that brands educate their customers in an interactive and streamlined manner about smishing so there is enough awareness among potential victims to combat it.

References

[1] Jemal Abawajy. User preference of cyber security awareness delivery methods. *Behaviour & information technology*, 33(3):237–248, 2014.

[2] Rabab Abumalloh, Mahmud Alrahhal, Nahla El-Haggar, Albandari Alsumayt, Zeyad Alfawaer, and Sumayh Aljameel. Exploring individuals' experiences with security attacks: a text mining and qualitative study. *Emerging Science Journal*, 8(1), 2024.

[3] Hanaa Alghamdi. Can phishing education enable users to recognize phishing attacks? 2017.

[4] Amazon. Avoiding payment scams. www.amazon.com/gp/help/customer/display.html?nodeId=G3KGTPA8B42CKBJ4. Access Date: 11/2/2024.

[5] Anti-Phishing Working Group. Phishing activity trends report: 1st quarter 2025. Technical report, APWG, April 2025. Accessed: 2025-07-28.

[6] ATLAS.ti. Why atlas.ti? https://atlasti.com/why-atlas-ti, 2023.

[7] Maria Bada, Angela M. Sasse, and Jason R. C. Nurse. Cyber security awareness campaigns: Why do they fail to change behaviour? https://arxiv.org/abs/1901.02672, 2019.

[8] Ranjit Bhaskar. Better cybersecurity awareness through research. *ISACA Journal*, 2022(3), 2022. Available at: https://www.isaca.org/resources/isaca-journal/issues/2022/volume-3/better-cybersecurity-awareness-through-research.

[9] Eric B Blancaflor, Adrian B Alfonso, KN Banganay, G Dela Cruz, K Fernandez, and S Santos. Let's go phishing: A phishing awareness campaign using smishing, email phishing, and social media phishing tools. 2021.

[10] AppRiver blog post. https://appriver.com/blog/201408fake-jp-morgan-secure-emails. Access Date: 11/2/2024.

[11] Indranil Bose and Alvin Chung Man Leung. Do phishing alerts impact global corporations? a firm value analysis. *Decision Support Systems*, 64:67–78, 2014.

[12] Mark Button, Branislav Hock, Joon Bae Suh, and Chol Soo Koh. Policing cross-border fraud 'above and below the surface': Mapping actions and developing a more effective global response. *Crime, Law and Social Change*, 83(1):5, 2025.

[13] L. Jean Camp. Mental models of privacy and security. IEEE, 2009. Available at: https://ieeexplore.ieee.org/document/5247001.

[14] Viasat Help Center. https://help.viasat.com/s/article/How-to-avoid-phishing-attacks-and-other-online-scams. Access Date: 11/2/2024.

[15] Jin-Hee Cho, Hasan Cam, and Alessandro Oltramari. Effect of personality traits on trust and risk to phishing vulnerability: Modeling and analysis. IEEE, 2016.

[16] CISA. Teach employees to avoid phishing. https://www.cisa.gov/secure-our-world/teach-employees-avoid-phishing.

[17] CISA. Technical information paper-tip-10-105-01 cyber threats to mobile devices. https://www.cisa.gov/sites/default/files/publications/TIP10-105-01.pdf.

[18] CISA. Avoiding social engineering and phishing attacks. https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks, Feb 2021.

[19] Safety Detectives. What is smishing (sms phishing)? - facts & how to stop it. https://www.safetydetectives.com/blog/what-is-smishing-sms-phishing-facts/, 2022.

[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] E. Christine Drake, J. Jonathan Oliver, and J. Eugene Koontz. Anatomy of a phishing email. MailFrontier, 2004. https://www.ceas.cc/papers-2004/slides/114.pdf.

[22] Morgan Edwards, Thomas Morris, Jing Chen, and Jeremiah Still. Smishing attack vector: Surveying end-user behavior, experience, and knowledge. SageJounrals, 2023. https://journals.sagepub.com/doi/10.1177/21695067231192193?icid=int.sj-full-text.similar-articles.9.

[23] Federal Trade Commission. Ftc launches rulemaking to combat sharp spike in impersonation fraud. https://www.ftc.gov/news-events/news/press-releases/2021/12/ftc-launches-rulemaking-combat-sharp-spike-impersonation-fraud, December 2021.

[24] Uwe Flick. The sage handbook of qualitative data analysis. 2013.

[25] 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.

[26] Walmart Inc. https://corporate.walmart.com/privacy-security/fraud-alerts. Access Date: 11/2/2024.

[27] Incorpo. One in four u.s. consumers have been conned into purchasing counterfeit goods in past 12 months according to incopro survey. https://www.prweb.com/releases/one-in-four-u-s-consumers-have-been-conned-into-purchasing-counterfeit-goods-in-past-12-months-according-to-incopro-survey-895741585.html, 2019. Accessed: 2025-01-30.

[28] itpro. Smishing attacks increased 700% in first six months of 2021. https://www.itpro.com/security/scams/360873/smishing-attacks-increase-700-percent-2021, 2021. [Accessed Jul 24, 2022].

[29] Daniel Jampen, Gürkan Gür, Thomas Sutter, and Bernhard Tellenbach. Don't click: towards an effective anti-phishing training. a comparative literature review. *Human-centric Computing and Information Sciences*, 10(1):33, 2020.

[30] A Karakasiliotis, Steven Furnell, and Maria Papadaki. Assesing end-user awareness of social engineering and phishing. Network Research Group, 2006. https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1011&context=isw.

[31] Manzoor Ahmed Khan, Adel Merabet, Shamma Alkaabi, and Hesham El Sayed. Game-based learning platform to enhance cybersecurity education. *Education and Information Technologies*, 27(5):5153–5177, 2022.

[32] Eunkyung Kweon, Hansol Lee, Sangmi Chai, and Kyeongwon Yoo. The utility of information security training and education on cybersecurity incidents: An empirical evidence. *Information Systems Frontiers*, 23:361–373, 2021.

[33] Keepnet Labs. Smishing statistics 2023: The latest trends and numbers in sms phishing, 2023.

[34] Elmer Lastdrager, Inés Carvajal Gallardo, Pieter Hartel, and Marianne Junger. How effective is anti-phishing training for children? In *Thirteenth symposium on usable privacy and security (soups 2017)*, pages 229–239, 2017.

[35] Elmer EH Lastdrager. Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science*, 3:1–10, 2014.

[36] Tong Li, Chuanyong Song, and Qinyu Pang. Defending against social engineering attacks: A security pattern-based analysis framework. The Institution of Engineering and Technology, 2023. https://doi.org/10.1049/ise2.12125.

[37] Tanjim Mahmud, Md Alif Hossen Prince, Md Hasan Ali, Mohammad Shahadat Hossain, and Karl Andersson. Enhancing cybersecurity: Hybrid deep learning approaches to smishing attack detection. *Systems*, 12(11):490, 2024.

[38] Mimecast. Brand trust: One cyberattack is enough to lose consumer trust and custom. https://mysecuritymarketplace.com/reports/brand-trust-one-cyberattack-is-enough-to-lose-consumer-trust-and-custom/, 2021. Accessed: 2025-12-5.

[39] Ani Munirah Mohamad, Felicia Yong Yan Yan, Nurhazman Abdul Aziz, and Shuhairy Norhisham. Inductive-deductive reasoning in qualitative analysis using atlas. ti: Trending cybersecurity twitter data analytics. In *2022 3rd International Conference for Emerging Technology (INCET)*, pages 1–5. IEEE, 2022.

[40] Mattia Mossano, Kami Vaniea, Lukas Aldag, Reyhan Düzgün, Peter Mayer, and Melanie Volkamer. Analysis of publicly available anti-phishing webpages: contradicting information, lack of concrete advice and very narrow attack vector. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 130–139. IEEE, 2020.

[41] Morium Akter Munny, Mahbub Alam, Sonjoy Kumar Paul, Daniel Timko, Muhammad Lutfor Rahman, and Nitesh Saxena. Infrastructure patterns in toll scam domains: A comprehensive analysis of cybercriminal registration and hosting strategies. *arXiv preprint arXiv:2510.14198*, 2025.

[42] Bilal Naqvi, Kseniia Perova, Ali Farooq, Imran Makhdoom, Shola Oyedeji, and Jari Porras. Mitigation strategies against the phishing attacks: A systematic literature review. *Computers & Security*, 132:103387, 2023.

[43] NCSC. Phishing attacks: defending your organisation. https://www.ncsc.gov.uk/guidance/phishing, February 2024.

[44] Ajaya Neupane, Md Lutfor Rahman, Nitesh Saxena, and Leanne Hirshfield. A multi-modal neuro-physiological study of phishing detection and malware warnings. In *Proc. of the 22nd ACM SIGSAC Conf. on Computer and Communications Security*, pages 479–491, 2015.

[45] James Nicholson, Yousra Javed, Matt Dixon, Lynne Coventry, Opeyemi Dele Ajayi, and Philip Anderson. Investigating teenagers' ability to detect phishing messages. pages 140–149, 2020.

[46] Social Engineering Org. www.social-engineer.org/newsletter/understanding-smishing/.com. Access Date: 11/15/2024.

[47] Proofpoint. Proofpoint's 2023 state of the phish report: Threat actors double down on emerging and evolving tactics. https://www.proofpoint.com/us/newsroom/press-releases/proofpoints-2023-state-phish-report-threat-actors-double-down-emerging-and-0, 2023. Accessed: 2024-11-18.

[48] Google quiz website. https://phishingquiz.withgoogle.com/?hl=en. Access Date: 10/10/2024.

[49] 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.

[50] 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*, CODASPY '23, page 49–60, New York, NY, USA, 2023. Association for Computing Machinery. https://doi.org/10.1145/3577923.3583640.

[51] Benjamin Reinheimer, Lukas Aldag, Peter Mayer, Mattia Mossano, Reyhan Duezguen, Bettina Lofthouse, Tatiana Von Landesberger, and Melanie Volkamer. An investigation of phishing awareness and education over time: When and how to best remind users. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, pages 259–284, 2020.

[52] Kroll report. www.kroll.com/en/insights/publications/cyber/monitor/vishing-smishing-attacks. Access Date: 11/22/2024.

[53] RoboKiller. Robokiller 2023 mid-year phone scam report. https://www.robokiller.com/robokiller-2023-mid-year-phone-scam-report, 2023.

[54] Verizon Account Security. https://www.verizon.com/about/account-security/smishing-and-spam-text-messages. Access Date: 11/2/2024.

[55] 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.

[56] Toyota Support. https://www.toyota.com/support/privacy-notice/. Access Date: 11/2/2024.

[57] Daniel Timko, Daniel Hernandez Castillo, and Muhammad Lutfor Rahman. Understanding influences on sms phishing detection: User behavior, demographics, and message attributes. In *Symposium on Usable Security and Privacy (USEC)*, 2025.

[58] Daniel Timko and Muhammad Lutfor Rahman. Commercial anti-smishing tools and their comparative effectiveness against modern threats. In *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pages 1–12, 2023.

[59] Daniel Timko and Muhammad Lutfor Rahman. Smishing dataset i: Phishing sms dataset from smishtank. com. In *Proceedings of the*

Fourteenth ACM Conference on Data and Application Security and Privacy, pages 289–294, 2024.

[60] Melanie Volkamer, Karen Renaud, Benjamin Reinheimer, Philipp Rack, Marco Ghiglieri, Peter Mayer, Alexandra Kunz, and Nina Gerber. Developing and evaluating a five minute phishing awareness video. In *Trust, Privacy and Security in Digital Business: 15th International Conference, TrustBus 2018, Regensburg, Germany, September 5–6, 2018, Proceedings 15*, pages 119–134. Springer, 2018.

[61] Yizhu Wang, Haoyu Zhai, Chenkai Wang, Qingying Hao, Nick A Cohen, Roopa Foulger, Jonathan A Handler, and Gang Wang. Can you walk me through it? explainable {SMS} phishing detection using {LLM-based} agents. In *Twenty-First Symposium on Usable Privacy and Security (SOUPS 2025)*, pages 37–56, 2025.

[62] Atlasti website. www.atlasti.com. Access Date: 11/14/2024.

[63] Phish Tank website. www.phishtank.com. Access Date: 4/22/2024.

[64] Smishtank website. www.smishtank.com. Access Date: 4/22/2024.

[65] Lowri Williams, Eirini Anthi, Yulia Cherdantseva, and Amir Javed. Leveraging gamification and game-based learning in cybersecurity education: Engaging and inspiring non-cyber students. *Journal of The Colloquium for Information Systems Security Education*, 11(1):1–8, 2024.

[66] Ezer Osei Yeboah-Boateng and Priscilla Mateko Amanor. Phishing, smishing & vishing: an assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences*, 5(4):297–307, 2014.

Appendix

VII. Qualitative Codes

- Prevention Advice (46)
  Don't click any links or open any attachments (85), Always be cautious when interacting with SMS (81), Always check and verify the legitimacy of the sender's number, sms text and link included (80), Don't share any personal information (73), Do not respond to unverified senders or act quickly (36), Stay thoroughly informed about the latest cybersecurity scams (32), Only send money/pay after verifying the sender authenticity at least twice (28), Contact the company directly to verify any suspicious text (26), Don't share account related information (25), Install latest version of antivirus software (24), Avoid phone calls from unknown or suspicious callers (23), Always double check gift card transactions (21), Only use official website/app to perform or verify any action (20), Maintain two-factor authentication and use strong passwords (17), Report any suspicious message to the respective brand (17), Check website URL and information thoroughly before entering any information (14), Check grammar of the SMS (12), Block and delete suspicious texts for avoiding future smishing attempts (8), Set alerts (8), Sender Verification (7), Suspicious Messages (7), Cyber Awareness Training (6), Avoid Text Messages (6), Mark suspicious messages as spam (5), Vigilance (4), Unexpected debt collection (3), Unexpected Hospital bills (3), Skepticism (3), Utility bills (3), Avoid Installing Programs (2), Constantly track your account activity (2), Company sends SMS from only Specific Phone Numbers (1), Fake Deals (1), Firewalls (1), Ignore and Delete (1), Information Gathering (1), Log-in credentials protection (1), Lookout for impersonal greetings (1), Not asking to delete app (1), Enroll to Paperless Statements (1), Public Computer Avoidance (1), Red Flags (1), Seek Advice (1), Sensitive Information (1), Session Security Restrictions (1), Trust Instincts (1),
- Smishing Definitions (20)
  Sending deceptive message(23), SMS requesting personal information (18), Impersonates a brand or person (14), Sending malicious links over SMS (12), SMS Phishing (10), Electronic fraud activity (9), SMS creating urgency (9), Phishing (8), Sending fake information over SMS (8), A type of cyberattack (6), Asking to take immediate action (3), Asks to install malware (3), Type of social engineering attack (3), Manipulate (2), Scammers (2), Threats (2), Trickery (2), Trustworthy entity (2), Short URL (1), Text Phishing (1)
- Report Fraud Instructions (24)
  Report the SMS to the respective brand (68), Contact FTC (14), Contact government authorities (13), Forward to Anti-Phishing Organizations (13), Consumer Protection Agencies (8), Online Reporting Platforms (7), Report to cyber crime division (6), Report to provider (6), Forward SMS to 7726 (5), FBI (4), Internet Crime Complaint Center (4), Report as Spam (3), Share Screenshot (3), IRS (2), Local Law Enforcement (2), Specific Information Required (2), Consumer Sentinel Network database (1), Delete Message (1), Include all scam details (1), Official Channels (1), Platform Support (1), Preventing Spread (1), Screenshot Submission (1), Timestamp (1)
- How to Identify Smishing (24)
  Ask for personal information(36), A sense of urgency(26), Unexpected links from sender(24), Trust your instincts(21), Misspellings or grammatical errors(17), Fake offers or promotions(15), Mimic trustworthy brands(13), Ask for funds(10), Cross checking with the brand(10), Include attachments (8), Unknown sender information (7), Impose threats(6), Mismatched links (6), Include third party(5), Fake delivery notifications(3), Ask to download an app or software (2), Provides phone number (2), Sender information hidden (2), Caution exercise (1), Directs to another website (1), Shortened URL(1),Emotional Appeal (1), Subtle differences with original brand(1), Variation of email domains(1),
- Steps to Take After Becoming Victim (21)
  Inform and forward the relevant details to service provider(39), Report Law Enforcement (25), Change password and log out from devices (23),Account monitoring(22), Use anti-virus in the affected device (15), Do not engage(13), Check for identity theft (10), Inform Fraud Detection(10), Report to mobile carrier(10), Exercise caution for any future phishing (9), Educate yourself and other about cybersecurity(9), Take quick actions (8), Stop interaction if already engaged(8), Enable Two factor Verification(7), Inform friends and family(4), Learn from the provider website on how to secure account(4), Update email security(2), Provide written request to provider if necessary(2),Be calm(1), Block scam numbers (1), Research about phishing(1)

VIII. Brands

- Technology & Software (25): *Adobe, Dropbox, ibm, accenture , Tech Mahindra, Cognizant , Intel, Accurint, Apple, Outlook, Microsoft, Google, Dynata, Verasight, Glide, HP, Eventbrite, Qualtrics, Samsung, Indeed, Intuit, Lenovo, Netsuite, Rackspace, Salesforce*
- Retail & E-commerce (23): *Target, Shopify, Ebay, Craigslist, Costco, BestBuy, Kohl's, JCPenny, Macy's, Amazon , walmart, walmart, American Greetings, Home Depot, Lowe's, Sam's Club, Best Buy, TJ Maxx, Kohl's, Gap Inc, Temu, Reebok, Rakuten*
- Finance & Banking (23): *Visa, American Express, CitiBank, Wells Fargo, Capital One, Discover, USBank, Synchrony, Navy Federal, J.P. Morgan, Bank of America, Chase Bank, ABSA Bank, Alliance Bank, Bank of the West, Barclays, Regions Bank, Navy Federal Credit Union, Deutsche Bank, US Bank, PNC Bank, Santander, Robinhood*
- Telecommunications (7): *MetroPCS, Xfinity, Consumer Cellular, Viasaat, Verizon, AT&T, Xfinity*
- Social Media (6): *Instagram, TikTok, Reddit, Whatsapp, X, Snapchat*
- Automotive & Ground Travel (6): *Toyota, Uber, Lyft, Ford, Tesla, FasTrak*
- Cybersecurity & VPN (6): *NordVPN, Malwarebytes, Hut Six, Cofense, Palo Alto Network, Duo Security*
- Food & Beverages (5): *Coca Cola , Pepsi, Burger King, McDonald's, Domino's*
- Gaming (5): *Arenanet, Blizzard Entertainment, GameStop, Steam, Zynga*
- Payment Services (5): *Paypal, Stripe, Venmo, Square, Western Union*
- Logistics & Delivery (4): *UPS, FedEx, DHL, USPS*
- Health & Pharmaceuticals (4): *CVS, Walgreens, Aetna, Walgreens*
- Insurance (4): *Allstate, StateFarm, USAA, Geico*
- Housing & Utilities (4): *SDGE, Shell, ExxonMobil, Chevron*
- Entertainment/Streaming (4): *Netflix, Youtube, Disney, Hulu*
- Dating Platform (3): *Coffee Meets Bagel , Bumble, Hinge*
- Air Travel (3): *Delta Airlines, Virgin Airlines, American Airlines*
- Government (3): *IRS, Electronic Benefit Transfer, Employee Development Department*
- News & Information (2): *Yahoo, WHO*
- Finance & Investments (2): *Berkshire Hathaway, Blackrock*
- Cryptocurrency (2): *CoinBase, Binance*
- Education (1): *CSU Northridge*
- Non-Profit & Advocacy (1): *Vote.org*
- Food Delivery (1): *GrubHub*