# Florida International University

# **FIU Digital Commons**

Global Strategic Communications Student Work

12-3-2023

# DOES GEN Z HAVE A PROBLEM WITH CELL PHONE TEXT SCAMS?

Lucia Ferrufino Florida International University, Iferr009@fiu.edu

Follow this and additional works at: https://digitalcommons.fiu.edu/gsc

#### **Recommended Citation**

Ferrufino, Lucia, "DOES GEN Z HAVE A PROBLEM WITH CELL PHONE TEXT SCAMS?" (2023). *Global Strategic Communications Student Work.* 16.

https://digitalcommons.fiu.edu/gsc/16

This work is brought to you for free and open access by FIU Digital Commons. It has been accepted for inclusion in Global Strategic Communications Student Work by an authorized administrator of FIU Digital Commons. For more information, please contact dcc@fiu.edu.

# DOES GEN Z HAVE A PROBLEM WITH CELL PHONE TEXT SCAMS?

By

Lucia Ferrufino

Instructor: Hugo H. Ottolenghi

# A PROFESSIONAL PROJECT PRESENTED TO THE SCHOOL OF COMMUNICATION+JOURNALISM OF FLORIDA INTERNATIONAL UNIVERSITY IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE

FLORIDA INTERNATIONAL UNIVERSITY

[Fall 2023]

# **Table of Contents**

ABSTRACT
INTRODUCTION
LITERATURE REVIEW
Phishing e-mails scams
Desktop and cell phone phishing scam detection
Emotions
Technology usage
METHODS
Participants
Measures
Procedure
RESULTS
DISCUSSION
Limitations
Recommendations
CONCLUSION
REFERENCE
APPENDICES

#### **Abstract**

The study consists of nineteen Gen Z (18-26) surveyed on cell phone text scams for rewards, a problem with their bank account/credit card, or an issue with their package. The three research questions for this study are as follows. First, is there any communication about text phone scams with other people? The second is, who do they talk to: relatives, friends, co-workers, social media, or others? The third question is, are they worried about text scams?

The survey shows that there is communication with the participants in that they have had conversations with people who have been scammed, and the two people who had been scammed informed a co-worker and social media connection. Additionally, fourteen participants had conversations twice or more weekly to once a month, and four participants had no conversations. Furthermore, in Gen Z's level of worry about being scammed by text, ten participants were not worried, while nine ranged from very worried to occasionally worried.

Keywords: Cell phone text scams, Gen Z, rewards, problem with bank account/credit card, issue with a package, communication, level of worry

#### Introduction

Scams have evolved from mail sent to one's home, phone calls to one's landline, and texts to one's cell phone (mobile or smartphone, the terms will be used interchangeably) since most people do not have a landline. Not only has our technology evolved, but so have the scams. In some instances, the words fraud and scam are used interchangeably. They are two separate actions from the legal and the bank perspectives. First, the legal perspective is that fraud is a serious criminal offense classified as felonies, while scams are considered minor offenses classified as misdemeanors (Team, D. C., 2023). Second, the bank's standpoint is that "fraud is the financial theft without your permission or knowledge, while scams are theft of funds with your permission or knowledge" (Team, D. C., 2023).

Furthermore, one of the first technological scams is phishing e-mails. Every day, people did not know of these types of scams until nearly ten years later, even though the practice originated around 1995 (History of Phishing, n.d.). Phishing scams are among the most commonly used methods to request sensitive information (O'Connor et al., 2021, as cited in Grimes et al., 2010). Different types of online scams are referred to as phishing "for your personal and financial information (e.g., your passwords, Social Security Number, bank account information, credit card numbers, or other personal information)" (Information Technology, n.d.).

Moreover, these "messages claim to come from a well-known software company, online payment service, bank, or other reputable institution" (Information Technology, n.d.). So, to fake authenticity, some will use an organization's e-mail address, logo, and other trademarks (Information Technology, n.d.).

Accordingly, consumer advocates say that text is a communication style with more urgency and one we're more inclined to trust since, typically, people only use texts to communicate with someone they know well; therefore, text scams can be even more complex to avoid than those that come via phone call or email (McCormick, 2023). Moreover, an article from the Federal Trade Commission states that "text scams can take a variety of forms and are sometimes referred to as "smishing" – a mashup of SMS ("short message service") and phishing" (Webre, 2020). The Federal Trade Commission, in an article, stated that "over 40% of people who reported a text scam in 2022 said the text impersonated a bank, was about a gift, delivery, a job, or claimed to be Amazon (see Table A1)" (Fletcher, 2023). According to the 2022 BBB Scam Tracker Risk Report, when targeted text messages, people reported losing \$579.00 (n.d.). Furthermore, according to the 2022 BBB Scam Tracker Risk Report, "for the first time since we began publishing the Risk Report in 2016, ages 18-24 reported a higher median dollar loss (\$220.00) than all other age groups (see Table A2)" and the second highest method of contact are cell phones (see Table A3) (n.d.). Additionally, this amount is up from \$170.00 in 2021, a 29.4% increase (2022 BBB Scam Tracker Risk Report, n.d.).

Moreover, "scammers often already have some information about their targets" (Webre, 2020). To steal from the recipient, their goal is always to get more personal or financial information (Webre, 2020). Unfortunately, consequences can be caused by clicking on a link in a scam text (Webre, 2020). "If you do, the scammer will have your login credentials and will try to access multiple accounts you may have using those credentials" (Webre, 2020). Additionally, another scenario of clicking on a link in a text is that if your cell phone OS security is not up-to-date, it could infect your phone with malware (Webre, 2020). Significantly, increased psychological distress, financial burden, and decreased quality of life are associated with falling

victim to financial exploitation (O'Connor et al., 2021, as cited in Burnes et al., 2017; Ganzini et al., 1990).

This paper focuses on the communication of scams via cell phone text (misdemeanors and funds being stolen with your permission or knowledge) for an issue with your package (for example, please click here), a problem (for example, your bank account/credit card is locked, please click here to unlock/call), or for rewards (for example, you won a prize, please click/call). Each scenario requires that the target take action. Therefore, this paper will not discuss love scams, sextortion, jobs, debt-free, or investments, to name a few. The group under study falls under Generation Z (note Gen Z is 11-26 years old and born between 1997 and 2011), but for this study, the age group is young adults 18-26 (born between 1997 and 2005). "They are commonly referred to as the first fully "digitally native generation" (Gorynski et al.; C., 2023).

The following three research questions are being explored in this paper. First, is there any communication about text phone scams with other people? The second is, who do they talk to: relatives, friends, co-workers, posts on social media, or others? The third question is, are they worried about cell phone text scams? Before investigating the questions above, we will discuss articles on phishing e-mails ("Can adults discriminate between fraudulent and legitimate e-mails? Examining the role of age and prior fraud experience"), compare phishing e-mails between desktops and smartphones ("Holding Your Hand on the Danger Button: Observing User Phish Detection Strategies Across Mobile and Desktop"), briefly examine one's emotional state of mind ("Consumer Experiences with Gift Card Payment Scams: Causes, Consequences, and Implications for Consumer Protection"), and discuss the pitfalls of technology for Gen Z ("Digital crime, trauma, and abuse: Internet safety and cyber risks for adolescents and emerging adults int eh 21st century").

#### **Literature Review**

Phishing e-mails scams

The article "Can adults discriminate between fraudulent and legitimate e-mails? Examining the role of age and prior fraud experience" uses fraud and scams. The focus is on adults' accuracy in detecting a "series of e-mails as legitimate or fraudulent with two factors of one's age and prior experience with fraud" (O'Connor et al., 2021). The study's criteria include "experience of sending and receiving e-mails in charge of their finances and no neurological disorders" (O'Connor et al., 2021). The study group comprised "100 young adults 18-26 and 96 older adults 60-90 years" (O'Connor et al., 2021). The 21-day study period consisted of 21 phishing e-mails being sent to the unbeknownst participants, and the click of the link of that e-mail was tracked (O'Connor et al., 2021).

The results for the groups did differ in the strategy, with older adults using a "high suspicion" strategy that led to mislabeling a legitimate e-mail as fraudulent compared to younger adults" (O'Connor et al., 2021). Furthermore, the extent of fraud experience differed across age groups, with prior fraud victims negatively related to e-mail detection performance (O'Connor et al., 2021). Moreover, "the results were a high susceptibility to clicking to phishing scams of 43% of the participants which clicked at least once throughout the survey period; however, older adult female participants were most susceptible to clicking on the fraudulent links" (O'Connor et al., 2021). The classification was 75%, with no accuracy difference between older and younger adults, but both groups used different strategies to categorize (O'Connor et al., 2021). On the other hand, "younger adults were 3.20 times more likely to be non-targets than target non-victims compared to older adults" (O'Connor et al., 2021).

Furthermore, both were "victimized at similar rates after being targeted" (O'Connor et al., 2021). The older victims were more biased than the younger group, who were less accurate (O'Connor et al., 2021). Thus, on the e-mail detection task, being a fraud victim was negatively related to performance (O'Connor et al., 2021). The research suggests that a more diverse group of older adults be studied and that the "use of computer confidence or e-mail experience is used to predict one's performance" for future research (O'Connor et al., 2021). Additionally, "younger adult fraud victims were less accurate at categorizing e-mails than targeted non-victims" (O'Connor et al., 2021). The research concludes that older adults are more willing to categorize e-mails as fraudulent and have more confidence than younger adults (O'Connor et al., 2021).

# Desktop and cell phone phishing scam detection

The article titled "Holding Your Hand on the Danger Button: Observing User Phish Detection Strategies Across Mobile and Desktop" researches "how digital platforms (desktop vs. mobile) influence users' phish detection strategies" (Dixon et al., 2022). Despite developing technical measures to thwart phishing, email attacks significantly cause cybersecurity breaches (Dixon et al., 2022). For companies and individuals, it can result in significant financial and reputational losses from phishing emails, accounting for 75% of successful security breaches worldwide (Dixon et al., 2022). "These descriptive emails aim to lure the recipient into downloading malicious programs or revealing sensitive information to the attacker" (Dixon et al., 2022). The study of a think-aloud protocol on both platforms consisted of twenty-one young adults (18-25 years) who were asked to rate the legitimacy of emails using a live inbox test (Dixon et al., 2022). All participants have self-reported regular internet use with at least one email account using a smartphone and a laptop/desktop computer (Dixon et al., 2022).

Furthermore, young people, in particular, are increasingly using mobile devices to check emails and access the internet, for which phishing threats are experienced across desktop and mobile (smartphone or tablet) platforms, with 95% of internet access now conducted via a mobile device (Dixon et al., 2022). Smartphones are a growing source of cybersecurity vulnerability (Dixon et al., 2022). Unsurprisingly, this increase in mobile activity has been accompanied by a significant increase in malware targeting mobile devices, making smartphones a growing security risk (Dixon et al., 2022). Hence, weak phish detection on mobile platform results suggests a lack of knowledge about crucial defense information (Dixon et al., 2022). Moreover, "we explored how young adult users (the heaviest users of mobile email systems) interact with the different platform interfaces, focusing specifically on how they utilize two key cues which differ in presentation across the platforms: the sender email address and hover-over previews of any web links in the email body" (Dixon et al., 2022).

Therefore, on the desktop participants could act on this knowledge. However, on the mobile, they had difficulty acting on this knowledge due to a lack of direct transfer of procedural knowledge and/or a riskier process required by the mobile interface (Dixon et al., 2022). In the study, it was noted that critical information on a mobile such as the sender's email address, must be manually displayed by the user, a problem exacerbated by the interaction design of the mobile platform; young users generally lack a coherent email classification strategy (Dixon et al., 2022). "A limitation is using Gmail and Android operating system" (Dixon et al., 2022). The lab-based method in the current study can employ a field research approach in further research (Dixon et al., 2022).

Furthermore, the classifications across both platforms (79%) out of a possible total of 16 correct, with the average success rate of participants was 12.6 (SD 2.1) (Dixon et al., 2022). The

mean mobile score is 5.9 (74%, SD 1.2) compared to the higher score of the desktop mean score of 6.7 (84%, SD 1.2) (Dixon et al., 2022). The default of the sender's email address is hidden, and a link preview is unintuitive and risky with the mobile interfaces for which these two critical problems must be addressed (Dixon et al., 2022). "We suggest minor adaptations to mobile email clients to support good cybersecurity habits and identification of phishing emails" (Dixon et al., 2022).

#### **Emotions**

The article titled "Consumer Experiences with Gift Card Payment Scams: Causes, Consequences, and Implications for Consumer Protection" consists of a study on gift card payment scams with 27 participants being interviewed with an age range from 18 to 81 with a mean age of 56 (DeLiema et al., 2023). According to a growing body of research, fraud on consumers has severe financial and emotional consequences (DeLiema et al., 2023). Furthermore, stolen from fraud victims in the U.S. in any given year, researchers estimate \$40 to \$50 billion (USD) (DeLiema et al., 2023, as cited in Deevy et al., 2012). "In addition to financial losses, victims often report guilt, shame, embarrassment, severe emotional distress, trouble sleeping, job loss, divorce, and indebtedness" (DeLiema et al., 2023, as cited in Buchanan & Whitty, 2013; Button et al., 2012; FINRA Investor Education Foundation, 2015).

Furthermore, research suggests that fraud can have equally devastating long-term outcomes, including anxiety, depression, and suicidality, that can severely impair everyday functioning, whereas violent crime victimization is often considered more serious (DeLiema et al., 2023, as cited in Cross, 2018; Deem, 2000; Ganzini et al., 1990). Moreover, decision-making abilities, such as financial judgment research, indicate that acute stress impairs it (DeLiema et al.,

2023). "In an experimental study, Porcelli and Delgado (2009) found that exposure to an acute stressor (submerging a hand in ice water) exacerbated decision-making biases, whereby participants who lost money in a rigged gambling task made riskier subsequent financial decisions under acute stress than those who were not subjected to a stressor" (DeLiema et al., 2023).

Likewise, compared to participants not facing social stress, those who underwent an acute social stressor (giving a speech) made poorer decisions on a subsequent financial task and failed to consider the consequences of increased financial losses demonstrated by Wemm and Wulfert, 2017 (DeLiema et al., 2023). "Another study showed that participants under acute stress had more difficulty paying attention to multiple stimuli at once and excluded peripheral information in favor of the most immediately salient information" (DeLiema et al., 2023, as cited in Mather & Sutherland, 2011). The induction of an acute stress response is the cause of emotional arousal, a tactic frequently used by perpetrators in a fraud context (DeLiema et al., 2023, as cited in Langenderfer & Shimp, 2001; Loewenstein, 1996). Susceptibility is affected by how emotional states induced by threatening or exciting scam messages are highlighted in existing studies (DeLiema et al., 2023, as cited in Norris & Brookes, 2021).

Also, integral emotions are considered directly elicited by scams (DeLiema et al., 2023). "However, a person's emotional state before fraud exposure – "incidental" emotions – might also influence susceptibility, especially if these emotions and physiological states are unpleasant" (DeLiema et al., 2023, as cited in Wyer et al., 2019). In the gift card payment scams, the participants felt blame and shame; more than half of the participants submitted complaints to federal consumer protection agencies, and in 14 cases, the local police were called (DeLiema et al., 2023). Family and friends were empathetic and understanding in all participants except for

one (DeLiema et al., 2023). Participants were more susceptible to unmet financial and emotional needs (DeLiema et al., 2023). "A culture of fraud reporting can be promoted by reducing the stigma of fraud victimization and offering financial and psychological support services to those who have experienced financial crimes" (DeLiema et al., 2023).

### Technology usage

The group under study is 18-26 and the first "digitally native" generation" (Gorynski et al., 2023). The Pew Research Center in 2018 estimated that 95% of American youths have access to a smartphone and 88% to a home computer, with online usage reported at 89% several times per day or almost continuously (Paat et al., 2020 as cited Anderson & Jiang, 2018b).

Furthermore, many youths' most common mode of communication with close friends is texting (Paat et al., 2020). Hence, "younger Americans are more likely than other age groups to embrace digital platforms and to use them regularly" (Paat et al., 2020). Today's youth confront dangerous side effects in the evolution of the digital environment (Paat et al., 2020, as cited in Cosma et al., 2020; Macchiarini et al., 2018). In conclusion, as the use of mobile phone apps continues to grow, digital media are becoming more integrated into the lives of the younger generation (Paat et al., 2020, as cited in Anderson & Jiang, 2018b; Brenner & Smith, 2013).

"Yet with greater use of digital gadgets also comes more significant risks that technological advancement brings" (Paat et al., 2020, as cited in Machimbarrena et al., 2018).

#### Methods

#### **Participants**

The anonymous survey was conducted via Qualtrics. The total number of participants for the survey consisted of 19. The participants' demographics were 63% females and 37% males, with 21% Black or African American and 79% Hispanic or Latin. Furthermore, one person (5%) had some high school but no diploma, three people (16%) had a high school diploma or GED; additionally, three people (16%) had some college but no degree, another three people (16%) had an associate degree and finally nine people (47%) had a bachelor's degree.

#### Measures

The survey consisted of two qualification questions asking if they were between 18 and 26 and if they used a cell phone (see Appendix B). After the qualification questions, they came to part one if they knew anyone who had experienced a cell phone text scam, part two asked about the participants being scammed via a cell phone text, and lastly, nine demographic questions (see Appendix B). This study measured the communication of cell phone text scams by the participants, the amount lost, if reported, the level of being worried, and posted on social media, if any. All the measurements are analyzed via Qualtrics (see Appendix C).

#### Procedure

A twenty-question survey was created via Qualtrics (see Appendix B for details of the questions). The participants were informed that the study was anonymous. The survey link was distributed to my contacts to share with anyone in the age group, and an email was sent out to

everyone in the Global Strategic Communications master program. The survey results can be found in the results section below (also see Appendix C).

#### **Results**

The survey was conducted via Qualtrics, with 37 people taking the survey but consisting of 19 qualifying participants. The first part asked if they knew anyone who fell for a text scam, and the second part was if the participants had fallen for a text scam. The results for part one of the survey are as follows. In response to question one, if the participants knew anyone who fell for a text scam, the results are that ten people (68%) said yes, and 11 people (52%) said no.

Moreover, in the participants' relationships with the person who fell for the scam, six people (60%) were relatives, three people (30%) were a friend, and one person (10%) had a social media connection.

Additionally, the participants indicated that the type of scam the person they knew fell for was missed delivery by two people (20%), bank alert for two people (20%), debit or credit card locked by three people (30%), and other by two people (20%) for Social Security and Google voice. Of the participants who were informed of the text scams, five people (50%) were on the same day, two people (20%) were told the next day, one person (10%) was informed a week later, and two people (20%) did not recall. Furthermore, the amount lost by the person the participants knew varied from \$50.00 to \$100,000.00, with one response writing that it was reported in time, so no amount was lost, and one wrote unknown. The participants indicated that seven (70%) reported it, and three (30%) reported no.

Moving on to the results of part two of the survey, we will discuss the participants' experience with cell phone text scams. Participants said that they receive text scams once a day

by three people (16%), once or twice a week by fifteen people (79%), three to four times a week, or more than by one person (5%). The type of text scams received (the totals do not add up to 100% because respondents were encouraged to choose all that applied) by the participants are missed delivery by 18 people (95%), bank alerts by seven people (37%), debit or credit card locked by four people (21%), winning a prize or sweepstakes ten people (53%) and one person (5%) selected other specifying "people speaking to me as if they texted the wrong number to phish for useful information." Additionally, the participants were asked if the text scam they received was because of a search on their phone on the same subject or something similar. Three people (16%) said yes, and sixteen people (84%) said no.

Furthermore, the participants were also asked about the text scam they recently received; what stood out about it? The response varied between everything being in caps lock with urgent language, similarities to actual notices, bank alert but not the participant's bank, package delivery but nothing ordered by participants, and suspicious link ending in. vip (full details can be seen in Appendix B). Of the 19 participants, two people (11%) have fallen for text scams, and seventeen (89%) have not. Additionally, the type of scam they fell for was missed delivery, bank alert, and debit or credit card lock, one for each scam (the totals do not add up to 100% because respondents were encouraged to choose all that applied). The follow-up was about whom they informed, with one person telling a co-worker and another participant indicating social media connections.

Moreover, the next question was when did they inform someone. One person said the next day, and another said a month or more later. One participant replied \$30.00 for the amount lost, and the other replied no. The second to last question on how often they have conversations with friends or family about scam texts was two participants (11%) twice or more a week, with

twelve people (67%) saying once a month and four people (22%) responding never. The final question is how worried they are about being scammed by a text; two participants (11%) are very worried, one (5%) is worried, six (32%) are occasionally worried, and ten (53%) are never worried.

#### **Discussion**

Various research has been conducted on phishing e-mails, including how to spot scams, causes, consequences, and implications for consumer protection, internet safety, and so much more, as well as ranging in age. Furthermore, research on viewing phishing e-mails on a desktop/laptop and a mobile device (the screen size is smaller, and whatever is being viewed needs to fit the screen) has also been studied. Scams, in general, are a complex issue, with emotions playing a factor. Additionally, Gen Z faces more significant risks, having always known technology. This can be seen in the 2022 BBB Scam Tracker Risk Report, in which a higher median loss of \$220.00 was reported for ages 18-24 than all other age groups.

Scams have been around, and technology has opened the doors to reach more victims. Thus, this research paper has shown that there is communication on cell phone text scams for Gen Z. However, a larger population needs to be researched to provide a more concrete understanding of the type of communication Gen Z is involved in. Questions include whether the communication is solely on social media, with family/friends in the same generation as Gen Z, or various generations. Furthermore, are those who shared their cell phone text scam stories in the same age group as Gen Z or in a different age group? Moreover, for the person who was cell phone text scammed, it was surprising that they informed a co-worker over a friend or family; hence, in future research, one might ask who you told first and why.

On further analysis of surveyed responses, the participants needed to have been asked more about the person who fell for the scam. For example, the person who fell for the scam what generation they are in. This question could have helped understand the type of communication Gen Z is involved in. On the other hand, the social media connection response for the Gen Z who was told about the cell phone text scam and the one who was a victim of a cell phone text scam was not surprising. Moreover, the fact that fourteen participants talked about cell phone text scams with friends or family is promising. Because nine have varying degrees of being worried and ten are never worried, a follow-up question needed to be asked as to why they are worried or not.

Gen Z is growing; thus, every two to three years, they need to be surveyed and interviewed to see the scope of cell phone text scams and maybe any new technology being used. On another note, those sharing my link informed me that some people they knew only spoke Spanish. Hence, a regret for this study is being unable to translate the survey into Spanish due to time constraints. Therefore, the survey and interviews should be conducted in various languages for future studies.

#### Limitations

First, only some people in Gen Z were surveyed due to time constraints. Second, the size of those surveyed (19 participants) is small. Therefore, a more significant number indicative of the population needs to be investigated, including those who are underage. Third, the study only consisted of a survey, but there also needed to be an interview portion. Last, the study only asked about four types of cell phone text scams (an issue with your package, a problem with your bank

account/credit card being locked, or for rewards winning a prize/sweepstakes), and more text scam types must be included.

#### Recommendations

There are too many scams, and everyone cannot know each type. Therefore, more education for all ages must be implemented at home and in schools. Moreover, there needs to be more checks and protection for all transfers. The literature review showed me this is a global issue; therefore, these checks and protections can start with a worldwide definition of fraud and scams everyone is on board for.

Moreover, the current research only consisted of Gen Z 18-26, so those between the ages of 11 and 17 with parental consent should be surveyed. Additionally, conducting a survey and interviewing the participants for future studies is recommended. The interview can be performed via WhatsApp, Teams, or other apps to reach a more diverse population. The interviews can be one-on-one, a group, or both. A question can be: Does communication and reporting a scamming incident help with not falling for a scam in the future? With those interviewed being followed up every two to three years, it might shed light on how commutation can correlate to falling and being a repeated victim of a scam.

#### Conclusion

This paper set out to examine (1) if there is any communication about text phone scams with other people, (2) who does Gen Z talk to: relatives, friends, co-workers, posts on social media, or others, and (3) is Gen Z worried about text scams. Notably, the survey indicates some communication on text scams, with ten participants knowing someone who has fallen for a text

scam and two participants having experienced text scams. Of those ten participants, six were relatives, three were friends, and one was social media connection. Furthermore, out of the ten who knew someone who fell for a cell phone text scam, they were informed of the amount, if any, with only one participant not knowing. Surprisingly, of the two participants who fell for a cell phone text scam, one participant told a co-worker, and another informed a social media connection. It seems that the reply would have been a relative or friend.

Furthermore, the second-to-last question indicates that fourteen participants have a conversation twice or more a week to once a month, and four people do not have any conversation. Therefore, even with the small number of participants, fourteen are conversing. The last question explored in this paper showed that most of the participants, ten, were not worried, and the rest went between very worried and occasionally worried. This indicates that there is almost a 50/50 between those not worried and those varying in being worried. A correlation may exist between the participants conversing about scams and not being worried or vice versa.

In conclusion, there is communication on cell phone text scams for the nineteen participants, with varying information on the amount lost. The level of worry is almost split half and half, with ten not worried compared to nine. Only one of the people in the relationship who fell for the scam had a social media connection, and the one person (could it be the same person) who fell for a scam told a social media connection. So, Gen Z is communicating about cell phone text scams to their co-worker and social media connections with varying degrees of worry among the participants.

#### References

- 2022 BBB SCAM TRACKERSM RISK REPORT. BBB.org. (n.d.). https://www.bbbmarketplacetrust.org/riskreport
- DeLiema, M., Volker, J., & Worley, A. (2023). Consumer experiences with gift card payment scams: Causes, consequences, and implications for Consumer Protection. *Victims & amp; Offenders*, 18(7), 1282–1310. https://doi.org/10.1080/15564886.2023.2244468
- Dixon, M., Nicholson, J., Branley-Bell, D., Briggs, P., & Coventry, L. (2022). Holding your hand on the danger button. *Proceedings of the ACM on Human-Computer Interaction*, 6(MHCI), pp. 1–22. https://doi.org/10.1145/3546730
- Fletcher, E. (2023, June 8). *IYKYK: The top text scams of 2022*. Federal Trade Commission. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/06/iykyk-top-text-scams-2022
- Gorynski, M. (2023, September 1). *Millennials vs. Gen Z: What are the key differences?* Zendesk. https://www.zendesk.com/blog/millennials-vs-gen-z-customer-service-expectations-compare/
- History of phishing. Phishing. (n.d.). https://www.phishing.org/history-of-phishing
- *Information technology*. UMass Amherst. (n.d.). https://www.umass.edu/it/security/phishing-fraudulent-emails-text-messages-phone-calls
- McCormick, E. (2023, April 22). *Gone in seconds: Rising text message scams are draining US bank accounts*. The Guardian. https://www.theguardian.com/money/2023/apr/22/robotexts-scams-bank-accounts
- O'Connor, A. M., Judges, R. A., Lee, K., & Evans, A. D. (2021). Can adults discriminate between fraudulent and legitimate e-mails? Examining the role of age and prior fraud experience. *Journal of Elder Abuse & Elder Reglect*, 33(3), 181–205. https://doi.org/10.1080/08946566.2021.1934767
- Paat, Y.-F., & Markham, C. (2020). Digital Crime, trauma, and abuse: Internet safety and cyber risks for adolescents and emerging adults in the 21st century. *Social Work in Mental Health*, *19*(1), 18–40. https://doi.org/10.1080/15332985.2020.1845281
- Taylor, E. (2023, April 19). *18 demographic survey questions (with examples)*. Full-Service Market Research Company. https://www.driveresearch.com/market-research-company-blog/7-types-of-demographic-questions-to-include-in-a-market-research-survey/

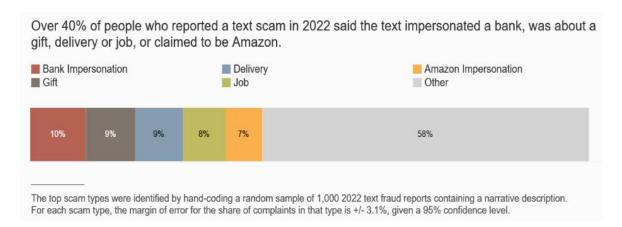
- Team, D. C. (2023, May 9). *Understanding the difference between scams and fraud*. DarkOwl, LLC. https://www.darkowl.com/blog-content/understanding-the-difference-between-scams-and
  - fraud/#:~:text=Financial%20institutions%20differentiate%20the%20two,without%20your%20permission%20or%20knowledge.
- Webre, P. (2020, March 2). *Mobile phone texts: Spam and scams*. Federal Communications Commission. https://www.fcc.gov/news-events/blog/2020/03/02/mobile-phone-texts-spam-and-scams

# **Appendices**

# Appendix A

#### **Tables**

#### Table A1



Data from: Fletcher, E. (2023, June 8). IYKYK: The top text scams of 2022. Federal Trade Commission. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/06/iykyk-top-text-scams-2022

Table A2

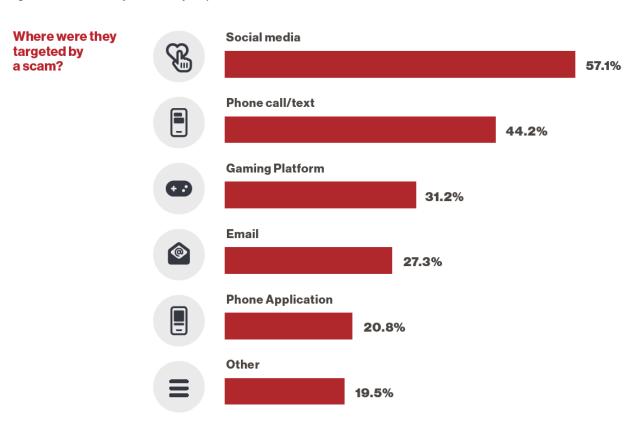
Exposure, susceptibility, and median dollar loss by age (all scam types)



Data from: 2022 BBB SCAM TRACKERSM RISK REPORT. BBB.org. (n.d.).

https://www.bbb.org/scamtracker

**Table A3**Reported method of contact for youth



The totals do not add up to 100% because respondents were encouraged to choose all that applied.

Data from: 2022 BBB SCAM TRACKERSM RISK REPORT. BBB.org. (n.d.).

https://www.bbb.org/scamtracker

# Appendix B

# **Survey questions**

# Qualifications to take the survey

1.	Are you between the ages of 18 and 26? If between 18 and 26, they can continue with		
	the survey.		
	Yes		
	No		
2.	Do you use a cell phone/smartphone? They can only continue the survey if they are		
	cell phone users.		
	Yes		
	No		

# **Survey Questions**

# Part 1

Please find below examples of text scams. You may have received one or more of them in the past several months. After reading them, you will be asked questions about your experiences with scams like these. Your responses will be anonymous.

Missed delivery scam text from FedEx (example below) or other carriers.

Hello Olivia, your FEDEX package with tracking code GB-6412-GH83 is waiting for you to set delivery preferences: <a href="mailto:e3fmr.info/onAyXsVfomA">e3fmr.info/onAyXsVfomA</a>

Below is an example of a fake bank text scam.

FRM:Wells-Fargo . Contact
NOW
SUBJ:ACCT BLOCKED
MSG:PU1C0T.

Text scam claiming that your debit or credit card is locked.

[JP MORGAN ONLINE]: Your debit card has been blocked. Verify your details via link <a href="http://www.http://

Below is an example of you winning a prize or sweepstakes.

USPS LOTTERY WINNER: We are happy to announce that you came 1st in our giveaway! Dont wait up, claim your prize NOW:

1.	Do you know anyone who has fallen for a text scam? If no, then skip to questi
	number 8.
	Yes
	No
2.	The person who fell for the scam, what is your relationship?
	a) Relative
	b) Friend
	c) Co-worker
	d) Social media connection

- 3. For the person who fell for the text scam, what type of scam was it?
  - a) Missed delivery
  - b) Bank alert
  - c) Debit or credit card is locked
  - d) Winning a prize or sweepstakes

e) Other (Specify)

	f) Do not know
4.	When did they tell you about their text scam?  a) Same day  b) Next day  c) A week later  d) Two weeks later  e) A month or more later  f) Do not recall
5.	What was the amount lost?  Blank box to write the amount.
6.	Did they report it (for example, Internet Crime Complaint Center, Consumer Protection Financial Bureau, your bank, etc.)?  Yes  No
7.	If yes, please describe how the financial institution or other entity responded and the outcome.  Blank box to explain.

#### Part 2

As a reminder, below the examples of text scams. Your responses will be anonymous.

Missed delivery scam text from FedEx (example below) or other carriers.

Hello Olivia, your FEDEX package with tracking code GB-6412-GH83 is waiting for you to set delivery preferences: <a href="mailto:e3fmr.info/onAyXsVfomA">e3fmr.info/onAyXsVfomA</a>

Below is an example of a fake bank text scam.

FRM:Wells-Fargo . Contact
NOW
SUBJ:ACCT BLOCKED
MSG:PU1C0T.

Text scam claiming that your debit or credit card is locked.

[JP MORGAN ONLINE]: Your debit card has been blocked. Verify your details via link <a href="http://www.http://

Below is an example of you winning a prize or sweepstakes.

- 8. How often do you receive scam texts on your cell phone?
  - a) Once a day
  - b) Once or twice a week
  - c) Three to four times a week, or more
- 9. What types of text scams did you receive? Select all that apply.
  - a) Missed delivery
  - b) Bank alert
  - c) Debit or credit card is locked
  - d) Winning a prize or sweepstakes
  - e) Other (Specify)
- 10. Did the text scam appear while you were doing a search on your phone on the same subject or something similar?

Yes			
No			
11. Thinking back on the text scam you recently received, what stood out about it?  Empty box to write.			
12. Have you ever fallen for a text scam? Yes			
No			
13. What type of scam did you fall for?			
a) Missed delivery			
b) Bank alert			
c) Debit or credit card is locked			
d) Winning a prize or sweepstakes			
e) Other (Specify)			
14. Whom did you tell about it?			
a) Relative			
b) Friend			
c) Co-worker			
d) Social media connections			
e) No one			

15.	5. When did you tell someone?		
a) Same day			
		Next day	
		A week later	
		Two weeks later	
	e)	A month or more later	
	f)	Never	
16. W		nat was the amount lost?	
	Bla	nnk	
17.	Dio	d you report it (for example, your bank, Internet Crime Complaint Center, Consumer	
Protection Financial Bureau, etc.)?			
	Yes	S	
	No		
18.	If y	ves, please describe how the financial institution or other entity responded and the	
		come.	
	Dic	ank box to explain.	
19.	Но	w often do you have conversations with friends or family about scam texts?	
		a) Twice or more a week	
		b) Once a week	

- c) Once a month
- d) Never
- 20. How worried are you about being scammed by a text?
  - a) Very worried
  - b) Worried
  - c) Occasionally worried
  - d) Never worried

# **Demographic Questions**

# Select one from the dropdown menu.

- 1. Gender: How do you identify?
  - a) Man
  - b) Woman
  - c) Non-binary
  - d) Prefer not to say
- 2. Ethnicity
  - a) Asian
  - b) Black or African-American
  - c) Hispanic or Latino
  - d) Native American or Alaska Native
  - e) Native Hawaiian or Pacific Islander

			34
	f)	White	
	g)	Other	
	h)	Prefer not to say	
3.	What	is your highest education?	
	a)	Some high school, no diploma	
	b)	High school diploma or GED	
	c)	Some college, no degree	
	d)	Associate degree	
	e)	Bachelor's degree	
	f)	Master's degree	
	g)	Doctorate	
	h)	Prefer not to say	
4.	Emplo	yment status	
	a)	Employed full-time	
	b)	Employed part-time	
	c)	Student and employed part-time	
	d)	Student and employed full-time	
	e)	Full-time student	
	f)	Disabled	

h) Prefer not to say

g) Unemployed

	b)	Married or domestic partnership
	c)	Widowed
	d)	Divorced
	e)	Separated
	f)	Prefer not to say
6.	What i	s your annual household income?
	a)	Under \$29,999
	b)	\$30,000 to \$49,999
	c)	\$50,000 to \$74,999
	d)	\$75,000 to \$99,999
	e)	\$100,000 to \$149,999
	f)	\$150,000 or more
7.	What 1	anguages do you speak fluently (select all that apply)?
	a)	English
	b)	Spanish
	c)	Italian
	d)	German

5. Marital status

e) French

a) Single, never married

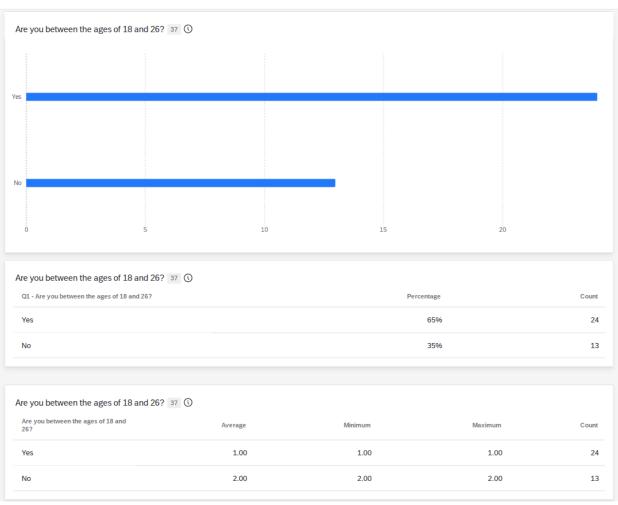
- f) Russian
- g) Mandarin
- h) Other
- i) Prefer not to say

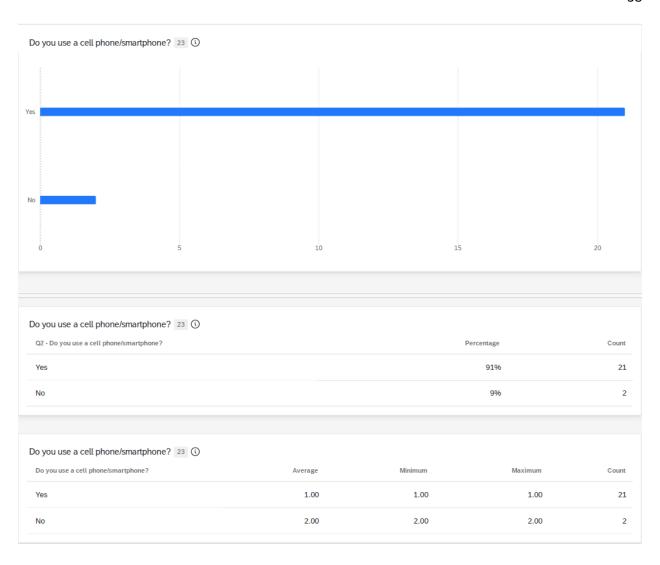
Thank you for taking the time to complete this survey. I genuinely value the information you have provided. I am incredibly grateful for your valuable time and honest information.

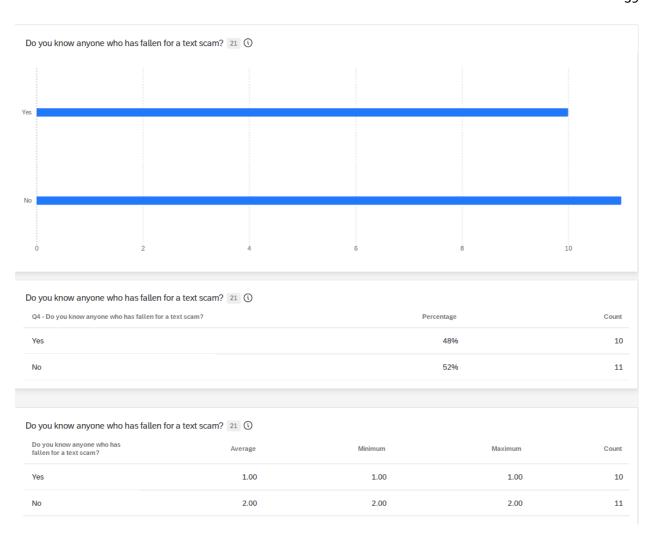
## Appendix C

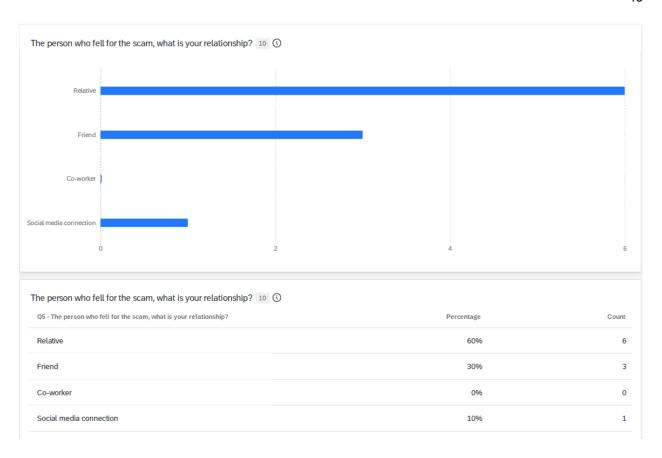
## **Survey results**

Responses: 37

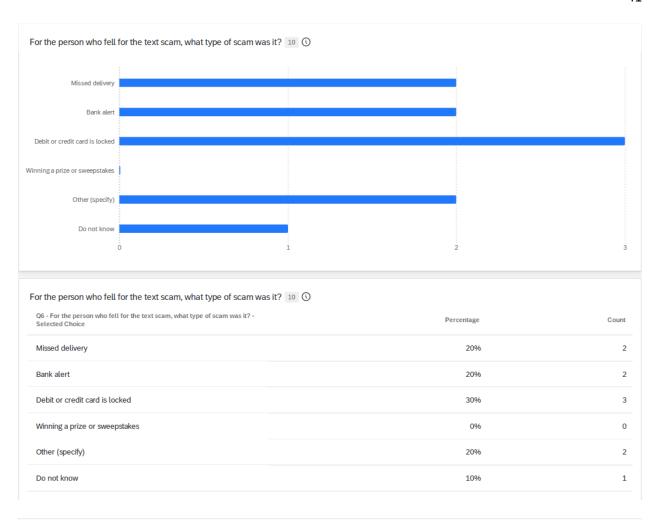




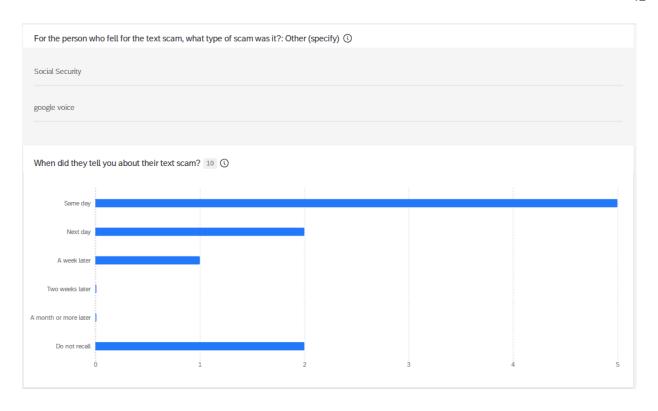




ne person who fell for the scam, what is your rela	ationship? 10 ()			
The person who fell for the scam, what is your relationship?	Average	Minimum	Maximum	Coun
Relative	1.00	1.00	1.00	
Friend	2.00	2.00	2.00	
Co-worker	-	-	-	
Social media connection	4.00	4.00	4.00	



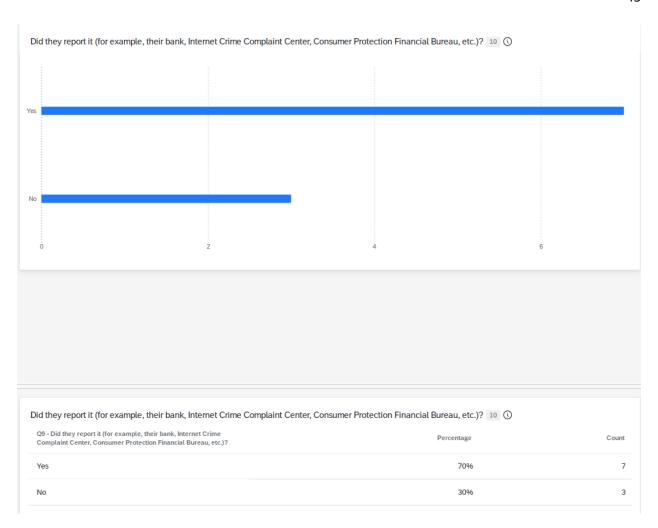
r the person who fell for the text scam, what t	ype of scam was it? 10 (			
or the person who fell for the text scam, what type of scam was it?	Average	Minimum	Maximum	Coun
Missed delivery	1.00	1.00	1.00	
ank alert	2.00	2.00	2.00	
Debit or credit card is locked	3.00	3.00	3.00	
Vinning a prize or sweepstakes	-	-	-	
Other (specify)	5.00	5.00	5.00	
o not know	6.00	6.00	6.00	



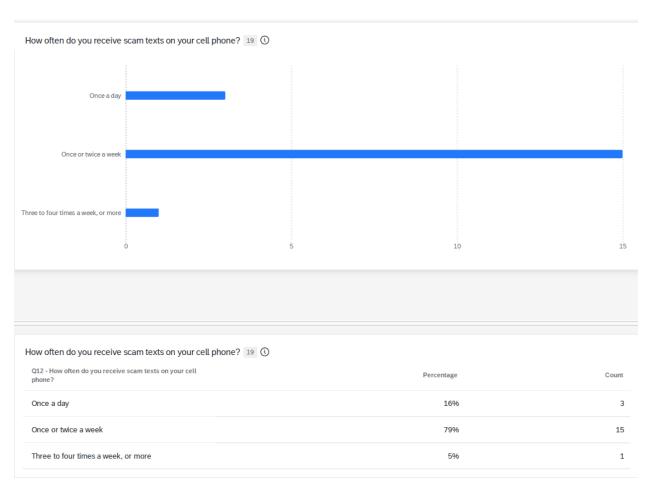
## DOES GEN Z HAVE A PROBLEM WITH CELL PHONE TEXT SCAMS?

Q7 - When did they tell you about their text so	am?	Per	centage	Cou
Same day			50%	
Next day			20%	
A week later			10%	
Two weeks later			0%	
A month or more later			0%	
Do not recall			20%	
	scam? 10 ①			
When did they tell you about heir text scam?	Average	Minimum	Maximum	Cot
When did they tell you about their text scam? Same day	Average			Cot
When did they tell you about their text scam?  Same day  Next day	Average	1.00	1.00	Cod
When did they tell you about their text scam?  Same day  Next day  A week later	1.00 2.00	1.00 2.00	1.00 2.00	Cod
then did they tell you about their text When did they tell you about their text scam?  Same day  Next day  A week later  Two weeks later  A month or more later	1.00 2.00 3.00	1.00 2.00 3.00	1.00 2.00 3.00	Со
When did they tell you about their text scam?  Same day  Next day  A week later  Two weeks later	1.00 2.00 3.00	1.00 2.00 3.00	1.00 2.00 3.00	Со

What was the amount lost? (Blank box to write amount.)
800
400
N/A, they reported it in time to not lose money
0
300.00
0
I don't know
100,000
2000
50

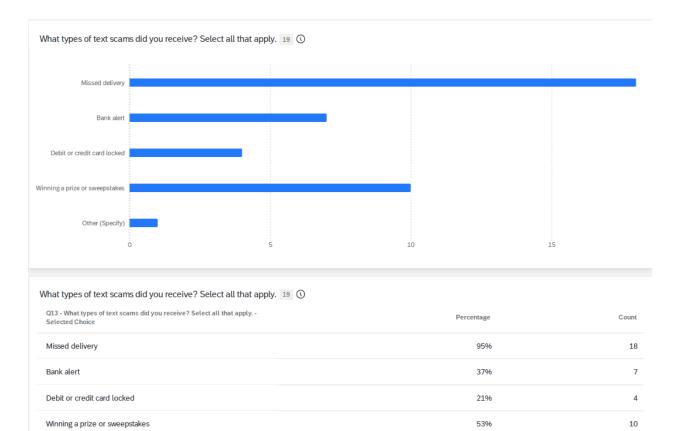


Did they report it (for example, their bank, Internet Crime Complaint Cente	Average	Minimum	Maximum	Coun
Yes	1.00	1.00	1.00	
No	2.00	2.00	2.00	
yes, please describe how the financial institution	or other entity respond and the outo	come. (Blank box for you to write.)		
ey were able to get a refund after investigating				
ocial Security Administration				
laced temporary money until confirming scam.				
deleted the message				
o not remember				



ow often do you receive scam texts on	your cell phone? 19 🛈			
How often do you receive scam texts on your cell phone?	Average	Minimum	Maximum	Count
Once a day	1.00	1.00	1.00	3
Once or twice a week	2.00	2.00	2.00	15
Three to four times a week, or more	3.00	3.00	3.00	1

1

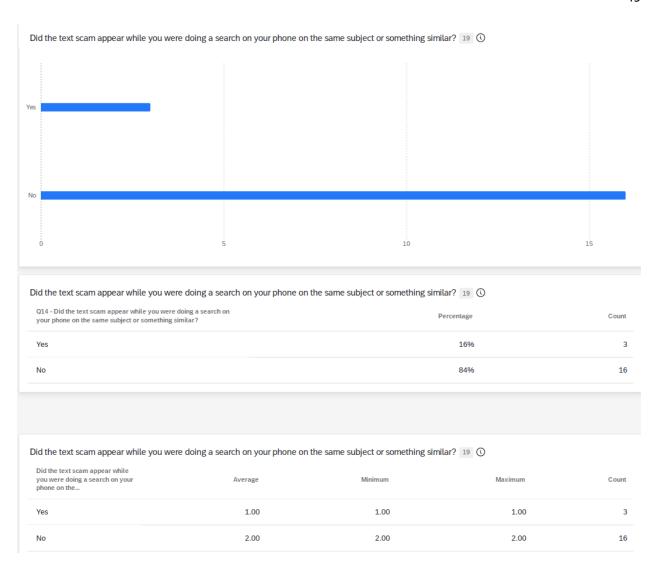


5%

What types of text scams did you receive? Select all that apply.: Other (Specify)

Other (Specify)

People speaking to me as if they texted the wrong number in order to phish for useful information.



What types of text scams did you receive? Select all that apply.: Other (Specify)
They used a lot of caps lock. They use urgent language.
How desperate people are to try and steal money from other people who are struggling financially. It's like, welcome to my bank account that only has \$5 dollars in it. Congrats. You just played yourself. LOL.
How similar it looked to the real notices
I've received many scam texts. I don't ever click the links they send or provide personal information
The type of bank. As the bank that is sent is not the bank i use for my finances.
I can spot a scam text because i am always aware of changes in orders i place and changes to my bank.
They stand out to me because I know I haven't made any orders and it's weird that I would be getting a one off message with typos and weird text placement.
That I hadn't order any packages
It said that I have a UPS order but I didn't have any.
The suspicious link. It ended with xip
Money statement
it would say my package from ups is stuck in the warehouse when i never ordered a package.

