Persuasion Techniques in Smishing

Wei Xie
Department of Computer Information Systems
Walker College of Business
Appalachian State University
416 Howard Street
Boone, NC 28608
xiew1@appstate.edu
828.262.8898 (Contact Author)

Sean Melia
MS in Applied Data Analytics
Walker College of Business
Appalachian State University
416 Howard Street
Boone, NC 28608
meliasean29@gmail.com

Victor Zhao
MS in Applied Data Analytics
Walker College of Business
Appalachian State University
416 Howard Street
Boone, NC 28608
zhaovq@appstate.edu

Abstract

At its core, smishing relies on persuasive techniques that exploit human vulnerabilities. Current research on smishing detection and prevention is lacking partly because there is a lack of coded real-time public smishing datasets to advance theory and practice. Following the Persuasion Theory, this study fills the gap by coding 934 smishing messages from two literature-cited datasets to determine the type of persuasion techniques used. In addition to six theory-based techniques, this study identified four additional compelling techniques: threat, ethics, curiosity, and pride. This exploratory study takes mixed method approach: qualitative coding to identify persuasion techniques and statistical analysis for correlations in persuasion techniques.

Keywords: smishing, phishing susceptibility, persuasion theory

Introduction

Smishing is a type of phishing attempt launched by text message to mobile users. The term 'smishing' is derived from two words: SMS (Short Message Service) and phishing. This attack form has become increasingly popular because people are more likely to trust a message that comes in through a messaging app on their phone than a message delivered via Email (Blancaflor et al., 2023). It is also challenging to determine whether a text message is malicious due to its brevity and the small number of features (Blancaflor et al., 2023). Fast-evolving mobile technologies increasingly raise the difficulty of distinguishing phishing from genuine ones (Dhamija et al., 2006). A study pointed out that mobile users are three times more likely than desktop users to fall victim to a web-based phishing attempt (Blancaflor et al., 2023).

Humans remain the weakest link in securing information and systems over time (Heartfield & Loukas, 2018). Scholars highlight the importance of understanding human characteristics to better predict and prevent phishing susceptibility (e.g., Heartfield et al., 2016; Tornblad et al., 2021). Research efforts have focused on personality traits, demographics, emotions, motivations and intentionality, beliefs and attitudes, and experience and knowledge (Tornblad et al., 2021). These scientific efforts reveal significant findings and help us understand phishing susceptibility from various angles. Smishing is a type of phishing through text messages. It is a social engineering method utilizing persuasive communication (Xie & Iyer, 2023). This study argues that individuals fall prey to smishing because persuasion plays a significant role in phishing attacks. The message persuades, deceptively, individuals to divulge personal information, financial details, or login credentials through seemingly legitimate text messages, leading to disastrous security breaches and leaving great economic, reputational, and emotional damage to individuals and businesses (IC3.gov, 2023).

Current research is either devoted to developing countermeasures for phishing emails or investigating the potential of machine learning-based detection systems. Yet, the current knowledge and understanding of how people respond to persuasiveness in smishing are scarce (Williams & Polage, 2019; Ferreira & Teles, 2019). To move smishing detection and prevention research forward, coding real-time public smishing datasets guided by theory is a must (Blancaflor et al., 2023). This study is motivated to fill the gap by coding real smishing messages and asking the main question: what type of persuasion techniques are used in the smishing messages by social engineers? This research seeks to help advance theory and practice.

Persuasion Theory & Literature

This study adopts the theoretical lens of persuasion by Cialdini (1993). He and his team argue that influential techniques use human's tendency to rely on automatic and quick information processing and "mindless" compliance. They identify six standard techniques to generate internal cognitive discomfort, leading to the response to the action-induced stimuli. First, the *Authority* method uses the perception of dominance to convince the audience to accept the beliefs or act on something. *Consistency* encourages the audience to comply by emphasizing dedication to the product, cause, group affiliation, political stands, etc. Persuasion through *Liking* using trust and affinity toward a person, place, object, or experience to induce changes. *Reciprocation* tries to stress a give-and-take relationship and persuade individuals to repay others for benefits received. *Scarcity* preys on people's worries of being left out of something valuable when availability and time are limited. Finally, *Social Proof* relies on peer pressure, a notion that "everyone is doing it." Security researchers have applied the theory to study social engineering in emails and vishing (e.g., Butavicius et al., 2016; Lawson et al., 2020; Jones et al., 2021). Wright et al. (2014) applied the persuasion theory to study phishing emails and expand the definitions to security research. This study conducted persuasive coding following Cialdini (1993) and Wright et al. (2014).

Case Study & Coding Method

In the simplest term, a case is an instance, incident, or unit of a phenomenon and can be anything – a person, organization, cell, action, decision, etc. (Schwandt & Gates, 2018). The critical defining feature of a case study is what is studied or what is a case of. Our empirical case is a smishing message, a contemporary real-life micro situation where there is no control on the part of the researcher and where everything happens by itself (Myers, 2019). We are studying the persuasion techniques used in each smishing SMS.

The case study is interpretive and inductive. It contributes meaningfully and significantly to theory-building, especially on a new topic that is much unknown (Barratt et al., 2011). Corbin and Strauss (2015) recommend a literature review for a sound theoretical basis for coding and building theory. Following the suggestion, we analyzed the raw SMS messages and coded the persuasion techniques deployed in them, according to the persuasion theory, which enables a consistent and systematic approach to studying the content. Additionally, we maintain theoretical sensitivity, opening to what emerges from the data (Strauss & Corbin, 2008). We identified and added possible new persuasion techniques (themes) to expand the existing theory, should there be any compelling evidence (Myers, 2019).

Dataset

In particular, this study collected two mobile message datasets and coded the persuasion techniques utilized in the messages. These two published datasets contain smishing and spam messages, totaling 1385. In 2022, understanding that the absence of representative data can seriously impact the research, Mishra and Soni took the initiative to build a smishing dataset with 638 messages from different internet sources to fill the gap of 'no publicly available smishing dataset.' The second was published by Almeida et al. (2011), which was collected for mobile phone spam and text classification research with 747 spam messages. Spam is unsolicited and sent out in bulk for commercial purposes (advertising) or fraud (perpetrate scams or phishing) by definition (Ferrara, 2019). Technique-wise, spam is social engineering that aims to persuade receivers into doing something, including revealing personal information. It is often generated and sent in massive volumes by botnets, which are networks of infected computers and contain a malicious attempt to gain access to your computer. We deleted some duplicates from the initial total of 1385 and proceeded with 1178 for actual coding.

Coding Process

Our coding process follows a postpositivist approach and is iterative and reflective to ensure the rigor of the results (Corbin & Strauss, 2015). First, we randomized the original 1178 messages to avoid the possible bias developed from coding similar messages clustered together. Second, two researchers coded an initial identical set of 100 messages separately, then met and compared the coding for each message to discuss and reflect on the difference. They then moved on to code the 2nd set of 100 identical messages separately and repeated comparing and discussing. This iteration process continues for all the collected data. Third, after coding the randomized messages, we sort all coded messages so that all similar messages will be clustered together. Doing this allows us to compare differences introduced at different coding times; we then discuss and revise for another round. In the end, we cleaned the redundant messages and ultimately came up with 934 admissible data. Figure 1 shows our coding process.

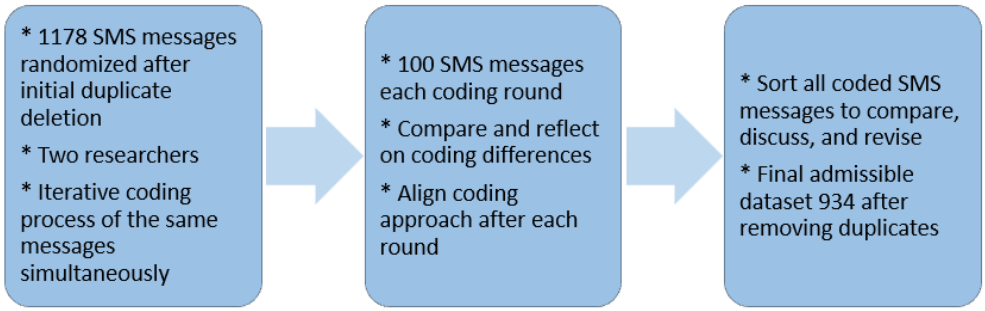

Figure 1: Coding Process

A phisher's goal is to persuade the receiver to believe a falsehood in the message and perform a specific action, such as clicking embedded malicious URLs, calling the fake number, which will lead to social engineers, or texting a reply with personal information. Therefore, in addition to coding the persuasion techniques, we code the messages to see whether there is a response action-induced redirect method, such as URLs, phone numbers for calls or texts, or email addresses. Figure 2 and Figure 3 are the frequency summaries for persuasion techniques and redirect methods in datasets. We will discuss how we code each message in the next Discussion section.

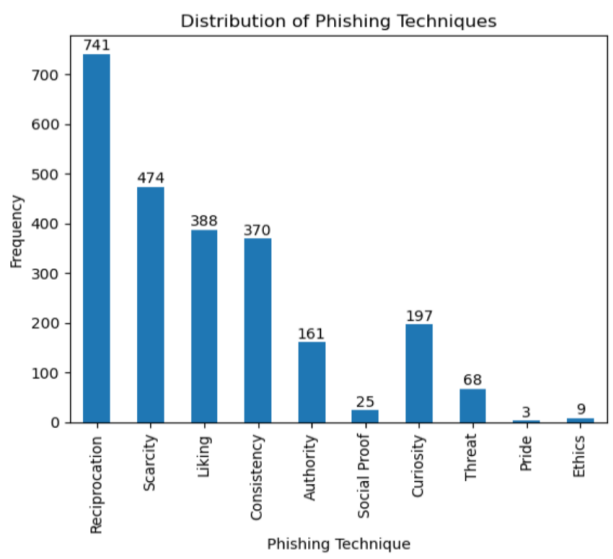

Figure 2: Persuasion Techniques

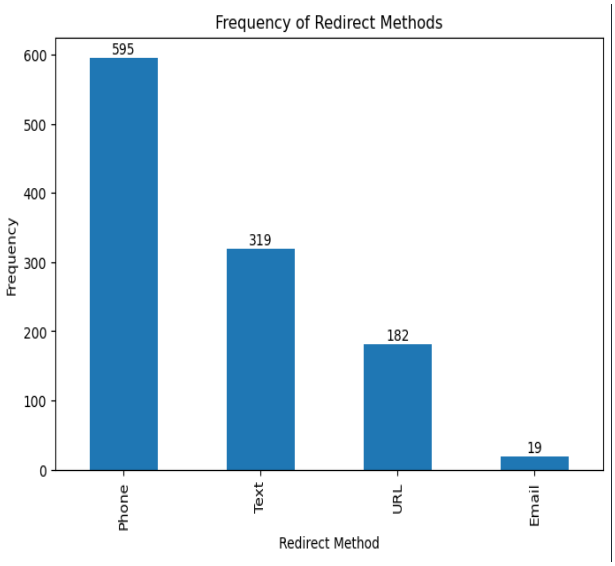

Figure 3: Redirect Methods

Discussions

We treat each message as a micro case and apply Cialdini's (1993) original theoretical definitions for coding guidance. In addition, we refer to Wright et al. (2014) by integrating their extended definitions and samples of persuasion techniques in phishing emails. We also aim to identify new compelling persuasion techniques during the coding process and contribute to expanding the phishing persuasion techniques.

At first glance, smishing might seem like just another text message. It could be a bank notification, a service provider message, or even an alert about a package delivery. However, the cognition generated, or emotions evoked, combined with the familiarity of receiving text messages, could make smishing particularly effective. We discuss each technique in the context of the messages below, including the additional four new techniques identified. You will read actual examples with message ID in parentheses, followed by an analysis.

Micro Case #1 Authority

(#839) 'You have an important customer service announcement from PREMIER. Call FREEPHONE 0800 542 0578 now!'
(#518) 'Your account has been credited with 500 FREE Text Messages. To activate call 08718738034'

Authority persuades the message receivers by using the perception of dominance in position, knowledge, experience, power, etc. It targets humans' belief in obedience to proper authority (Cialdini, 2009; Wright et al., 2014). The messages drop the name of 'PREMIER' (#839) and use assertive language to indicate a position in power or control, e.g., important customer service announcements (#518). *Authority* is not a popular persuasion technique out of the original six, 17% (161 out of 934) messages. However, the security attack is constantly evolving. FTC (2022) published an article to educate the public about the top five text scams. All five used the *Authority* technique, together with the *Consistency*.

Micro Case #2 Consistency

(#229) 'Hi. Customer Loyalty Offer: The NEW Nokia6650 Mobile from ONLY å£10 at TXTAUCTION! Txt word: START to No: 81151 & get yours Now! 4T&Ctxt TC 150p/MTmsg'
(#1051) 'Dear Voucher Holder, To claim this weeks offer, at you PC please go to http://www.e-tlp.co.uk/rewa'
(#513) 'You are now unsubscribed all services. Get tons of sexy babes or hunks straight to your phone! go to http://gotbabes.co.uk. No subscriptions.'

Consistency persuades message receivers to comply by suggesting a prior commitment or a former endorsed opinion and position. It targets humans' tendency to perform consistently (Cialdini, 2009; Wright et al., 2014). These prior commitment suggestions lure receivers to continue participating or maintain the endorsed position. For example, 'loyalty offer' (#229) indicates a long term association with the message sender, 'voucher holder' (#1051) suggests a previous purchase, and 'unsubscribed' implies a previous subscription (#513). *Consistency*, 370 out of 934, 40% of total coded messages, is just 2% below *Liking*. It is gaining publicity in current text scams, together with *Authority* (FTC, 2022).

Micro Case #3 Liking

(#174) 'FreeMsg Why haven't you replied to my text? I'm Randy, sexy, female and live local. Luv to hear from u. Netcollex Ltd 08700621170150p per msg reply Stop to end'
(#246) 'IMPORTANT MESSAGE. This is a final contact attempt. You have important messages waiting out our customer claims dept. Expires 13/4/04. Call 08717507382 NOW!'
(#1014) 'You are a winner you have been specially selected to receive Â£1000 cash or a Â£2000 award. Speak to a live operator to claim call 087123002209am-7pm. Cost 10p'

Liking persuades message receivers to respond by using good wish gestures and words to win the goodwill and friendship of the receivers. It targets humans' preference to say yes to individuals they 'know and like' (Cialdini, 2009; Wright et al., 2014). For example, message #174 strikes a friendly conversation by introducing herself as a 'sexy female living local,' and message #1014 reminds receivers that they are 'specially selected.' It also tries to win the trust through efforts' demonstration. Message #246 uses 'this a final contact attempt' to suggest the sender is putting their efforts into trying to help. Humans are social animals, and feelings of similarity often lead to compliance. *Liking* is the third most common technique, in close tie to *Consistency*, with 388 out of 934, or 42% of total coded messages. Furthermore, *Liking* has become more and more popular in smishing. FTC's (2022) article warns the public that three out of the top five use the *Liking* technique.

Micro Case #4 Reciprocation

(#918) 'Today's Offer! Claim ur Â£150 worth of discount vouchers! Text YES to 85023 now! SavaMob, member offers mobile! T Cs 08717898035. Â£3.00 Sub. 16. Unsub reply X'

Reciprocation persuades message receivers to respond by emphasizing a 'give-and-take' relationship, often with 'uninvited' offers. It targets humans' tendency to repay others' (Cialdini, 2009; Wright et al., 2014). Therefore, most of the time, *Reciprocation* has something 'free' and/or 'valuable' in the offers that are waiting to be claimed, as shown in message #918. It is the most commonly used technique, totaling 741 out of 934, 79% of coded messages.

Micro Case #5 Scarcity

(#865) 'Someone U know has asked our dating service 2 contact you! Cant guess who? CALL 09058095107 NOW all will be revealed. POBox 7, S3XY 150p'
(#683) '500 New Mobiles from 2004, MUST GO! Txt: NOKIA to No: 89545 & collect yours today!From ONLY Â£1 www.4-tc.biz 2optout 087187262701.50gbp/mtmsg18'
(#441) 'URGENT! Your mobile No ********** WON a å£2,000 Bonus Caller Prize on 02/06/03! This is the 2nd attempt to reach YOU! Call 09066362220 ASAP! BOX97N7QP, 150ppm'
(#1001) 'URGENT. Important information for 02 user. Today is your lucky day! 2 find out why, log onto http://www.urawinner.com there is a fantastic surprise awaiting you !'

Scarcity persuades message receivers to comply by preying on people's worries of being left out of something valuable, especially when availability and time are limited. It targets humans' wants for limited resources and opportunities (Cialdini, 2009; Wright et al., 2014). *Scarcity* is the second most common technique (474, 51% of total messages). It is usually used together with *Reciprocation* and has words shouted out in capitalization (e.g., NOW, URGENT, ASAP in message examples) to create a sense of urgency in receivers, hoping to push them to respond and not miss free or valuable offers at a limited time frame.

Micro Case #6 Social Proof

(#380) 'Think ur smart? Win å£200 this week in our weekly quiz, text PLAY to 85222 now!T&Cs WinnersClub PO BOX 84, M26 3UZ. 16+. GBP1.50/week'
(#514) 'You can donate å£2.50 to UNICEF's Asian Tsunami disaster support fund by texting DONATE to 864233. å£2.50 will be added to your next bill'

Social Proof persuades message receivers to react by presenting peer pressure or 'everyone is doing it.' It targets humans' preference for following social norms (Cialdini, 2009; Wright et al., 2014). *Social Proof* usually suggests peers, friends, and mates in the play together. For example, message #380 suggests competition with others while #514 indicates everyone is helping; therefore, you, the receivers, should be part of it too. It is a sparsely used technique in our dataset, with 25 out of 934 (3%) of total messages.

Micro Case #7 Threat

(#549) 'Apple ID: [BUXCX7GBVwWCcOD Final Notification Your Apple 1D is due to expire today. Prevent this by confirming your Apple ID atï¿½http://verifyapple.uk Apple Inc'
(#1068) 'Dear Sir Your Bank card has been blocked because you did not updated yet, If you want to update your ATM card please contact +971586153091 +971523182746.'

Threat appeals to receivers' fear of consequences for something done or not done. It has become more and more popular in smishing. FTC (2022) published an article to educate the public about the top five text scams. Two out of five use threat techniques. For example, message #1068 states that 'Your Bank card has been blocked because you did not updated yet…', clearly threatening the receivers to take action to correct the situation. In a panic, the unsuspecting receivers might call the number, leading them to social engineers who are skilled enough to trick them further into revealing credentials. We identified 68 (7%) messages using the techniques.

Micro Case #8 Curiosity

(#1140) 'You have an important customer service announcement. Calnumber 0800 542 0826 now!'
(#1133) 'A link to your picture has been sent. You can also use http://alto18.co.uk/wave/wave.asp?o=44345'

We have identified that text scammers frequently appeal to human *Curiosity*, the nature of inquisitive thinking, such as exploration, investigation, and learning in humans. Messages using *Curiosity* persuasion often suggest something is waiting to be discovered, for example, something sexual or an important message. *Curiosity* is the most frequently used among the four newly discovered techniques, with 197 (21%) total messages.

Micro Case #9 Ethics

(#23) '25p 4 alfie Moon's Children in need song on ur mob. Tell ur m8s. Txt Tone charity to 8007 for Nokias or Poly charity for polys: zed 08701417012 profit 2 charity.'

Social engineers are fully aware that humans are bound to help others. So, they use *Ethics* to persuade receivers, appealing to our moral compass. This type of message usually suggests assisting others, or it is charity-related. Not very often, we only identified nine (<1%) messages.

Micro Case #10 Pride

(#335) 'Show ur colours! Euro 2004 2-4-1 Offer! Get an England Flag & 3Lions tone on ur phone! Click on the following service message for info!'

Pride appeals to receivers' patriotism and is the least-used technique, with only three (<1%) total. However, we feel it is a valid technique that can evoke a strong feeling in receivers and elicit responses in the right situation. For example, the cited message #335 refers to a Euro Open game. People support their endorsed sports teams!

Table 1 summarizes the original definitions from the two guiding literature, indicators we use to code the messages, and SMS examples. Table 2 provides the four additional persuasion techniques, our definitions and indicators, and SMS examples.

Persuasion Techniques	Definition (Cialdini, 2009)	Definition (Wright et al., 2014)	Our coding guiding indicators in the messages	SMS Examples
Authority	People's tendency to believe that obedience to proper authority is right and disobedience is wrong (Cialdini 2009, pp. 180–181).	persuade/encourage the text message receiver to act on the suggestions in the message by using the perception of dominance (e.g., in position, knowledge, experience, power)	dropping a name, and using a title; using an assertive tone in the message	'your account has been credited...' (#839), 'important messages from claim department...' (#518)
Consistency	Once people make a commitment, they will feel personal and interpersonal pressure to perform consistently with that commitment" (Cialdini 2009, p. 52)	persuade/encourage the text message receiver to comply to the suggestions in the message by emphasizing prior commitment (e.g., behavior, belief), or a former endorsed opinion and position.	suggesting an existing membership and commitment to purchase, product, services, cause, group affiliation, political stands, etc.	'dear voucher holder...to stop texts' (#1051), 'unsubscribed' (#513), 'Customer Loyalty Offer...' (#229) that suggest prior commitment; or, message to encourage continuous participation
Liking	People prefer to say yes to individuals they 'know and like' (Cialdini 2009, p. 142), and compliance practitioners use factors including physical attractiveness, perceived similarities, praise, and association with favorable events/outcomes to increase the chance of compliance.	persuade/encourage the text message receiver to act on the suggestions in the message by using goodwill, trust, and friendship (e.g., emotions, feelings) toward a person, place, object, or experience.	using good wish gestures and words or showing efforts to stimulate liking; flirtation, appearance, and demeanor to evoke good feelings	'sexy female live local…' (#174), 'this is a final contact attempt...' (#246), 'you have been specially selected...' (#1014)
Reciprocation	People has tendency to 'try to repay, in kind, what another person has provided us' (Cialdini 2009, p. 19)	persuade/encourage the text message receiver to act on the suggestions in the message by stressing a give-and-take relationship. Many times the 'uninvited' offers.	indicating something 'free' and 'valuable' have been offered, waiting to be claimed	raffle prices such as 'Today's Offer!' (#918)
Scarcity	People tend to derive scarcity from their personal values; 'opportunities seem more valuable to us when they are less available' (Cialdini 2009, p. 228).	persuade/encourage the text message receiver to comply the suggestions in the message by preying on people's worries of being left out of something valuable when availability and time are limited.	indicating something is limited in time, quantity, etc.	using the words 'NOW', 'ONLY', 'ASAP', 'URGENT', etc. (#865, #683, #441, #1001)
Social Proof	People 'view a behavior as correct in a given situation to the degree that we see others performing it' (Cialdini 2009, p. 99).	persuade/encourage the text message receiver to comply the suggestions in the message by relying on the notion of peer pressure of "everyone is doing it".	suggesting 'peers, friends, mates'	message to encourage participation through suggestions of peer competition (#380), or everyone is helping (#514)

Table 1: Coding Summary of Persuasion Theory Techniques

Persuasion Techniques	Definition (Cialdini, 2009)	Our coding guiding indicators in the messages	SMS Examples
Threat	appeal to receivers' fear of consequences for something done or not done.	indicating charges been made to credit card, or unusual activities happened	'your Apple 1D is due to expire today…' (#549), 'your bank card has been blocked…' (#1068)
Curiosity	appeal to receivers' quality of inquisitive thinking such as exploration, investigation, and learning	suggesting something is waiting or sexual	'you have an important customer service announcement…' (#1140), 'a link to your picture has been sent…' (#1133)
Ethics	appeal to receivers' moral compass	suggesting help others and/or charity-related	'Children in need song…' (#23)
Pride	appeal to receivers' patriotism	suggesting nationality and support to sports team	'show ur colours! Get an England Flag' (#335)

Table 2: Coding Summary of New Persuasion Techniques

Conclusion & Future Research

This study is our initial step in studying persuasion techniques in smishing to fill the gap of no publicly available coded smishing dataset. We collected two publicly published SMS smishing and spam datasets (Mishra & Soni, 2022; Almeida et al., 2011) and coded 934 messages of the persuasion techniques deployed in each message by following the persuasion theory (Cialdini, 1993). We identified and added four new persuasion techniques: threat, curiosity, ethics, and pride, in addition to the original six techniques. The study found that multiple persuasion techniques and action-induced redirect methods are used simultaneously. The limitation of this study ties into the data sets and sample sizes. Future research should

code and study more sample datasets, considering the forever evolving security terrain. Furthermore, future research could use the coded dataset to advance smishing studies in theory and practice, applying different methodologies. For example, the AI study could use the coded dataset to train machine learning (ML) models to distinguish messages between phishing and legitimate classes, to build a persuasive taxonomy, to apply explainable AI (XAI) to ensure transparency and build trust, and to use generative AI algorithms create detection/prevention and training programs (e.g., Ferreira & Teles, 2019). Psychometric studies can build models to understand individuals' sensitivity to the different persuasion techniques and to manipulate and examine persuasion techniques and the variations in effect. Psychophysiological studies can uncover various physiological and neural correlates of the cognitive and emotional responses elicited by persuasion techniques.

References

Almeida, T. A., Hidalgo, J. M. G., & Yamakami, A. (2011, September). Contributions to the study of SMS spam filtering: new collection and results. In *Proceedings of the 11th ACM symposium on Document engineering* (pp. 259-262).

Barratt, M., Choi, T. Y., & Li, M. (2011). Qualitative case studies in operations management: Trends, research outcomes, and future research implications. *Journal of operations management*, *29*(4), 329-342.

Blancaflor, E., Romero, M. A., Nacu, I., & Golosinda, D. R. (2023, May). A Case Study on Smishing: An Assessment of Threats Against Mobile Devices. In *Proceedings of the 2023 9th International Conference on Computer Technology Applications* (pp. 172-178).

Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2016). Breaching the human firewall: Social engineering in phishing and spear-phishing emails. arXiv preprint arXiv:1606.00887.

Cialdini, R. B. (2009). *Influence: Science and practice* (Vol. 4, pp. 51-96). Boston: Pearson education.

Cialdini, R. B. (1993). Influence: Science and practice (3rd ed.). New York: HarperCollins.

Corbin, J., & Strauss, A. (2015). Basics of qualitative research: techniques and procedures for developing grounded theory.

Corbin, J., & Strauss, A. (2008). Qualitative research. *Techniques and procedures for developing grounded theory*, *3*.

Dhamija, R., Tygar, J. D., & Hearst, M. 2006. "Why phishing works," In Proceedings of the SIGCHI conference on Human Factors in computing systems, pp. 581-590.

Ferrara, E. (2019). The history of digital spam. *Communications of the ACM*, *62*(8), 82–91. DOI 10.1145/3299768

Ferreira, A., & Teles, S. (2019). "Persuasion: How phishing emails can influence users and bypass security measures," *International Journal of Human-Computer Studies* (125), pp. 19–31.

FTC. (2023). "IYKYK: The top text scams of 2022," https://www.ftc.gov/system/files/ftc_gov/pdf/texts-spotlight-final.pdf, accessed March 31, 2024.

Jones, K. S., Armstrong, M. E., Tornblad, M. K., & Siami Namin, A. (2021). How social engineers use persuasion principles during vishing attacks. Information & Computer Security, 29(2), 314-331.

Heartfield, R., & Loukas, G. (2018). Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. *Computers & Security*, *76*, 101-127.

Heartfield, R., Loukas, G., & Gan, D. 2016. "You are probably not the weakest link: Towards practical prediction of susceptibility to semantic social engineering attacks," *IEEE Access* (4), pp. 6910-6928.

Internet Crime Complaint Center (IC3). internet crime report. (n.d.) https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf, accessed October 05, 2023.

Lawson, P., Pearson, C. J., Crowson, A., & Mayhorn, C. B. (2020). Email phishing and signal detection: How persuasion principles and personality influence response patterns and accuracy. *Applied ergonomics*, *86*, 103084.

McHugh, M. L. (2013). The Chi-square test of independence. *Biochemia Medica*, *23*(2), 143–149.

Mishra, S., & Soni, D. (2022, December). SMS Phishing Dataset for Machine Learning and Pattern Recognition. In *International Conference on Soft Computing and Pattern Recognition* (pp. 597-604). Cham: Springer Nature Switzerland.

Myers, M. D. (2019). Qualitative research in business and management. *Qualitative research in business and management*, 1-364.

Schwandt, T. A. and Gates, E. F. (2018) 'Case study methodology' in Denzin, N. K. and Lincoln, Y. S. (eds.) The Sage handbook of qualitative research. Thousand Oaks, CA: Sage Publications, pp. 341- 358.

Tornblad, M. K., Jones, K. S., Namin, A. S., & Choi, J. 2021. "Characteristics that Predict Phishing Susceptibility: A Review," In Proceedings of the Human Factors and Ergonomics Society Annual Meeting (65:1), pp. 938-942. Sage CA: Los Angeles, CA: SAGE Publications.

Williams, E. J., & Polage, D. 2019. "How persuasive is phishing email? The role of authentic design, influence and current events in email judgements," *Behaviour & Information Technology* (38:2), pp. 184–197.

Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., & Marett, K. 2014. Influence Techniques in Phishing Attacks: An Examination of Vulnerability and Resistance. *Information Systems Research* (25:2), pp. 385–400.

Xie, W. & Iyer, L. (2023). "Phishing Susceptibility – a Cognitive Dissonance Persuasion View." AIS eLibrary, In: Proceedings of the Twenty-ninth Americas Conference on Information Systems (AMCIS). Panama City, Panama.