

University of Central Florida

STARS

Graduate Thesis and Dissertation 2023-2024

2023

Navigating with Sharks: How the Marketing Practices Help to Create Successful Phishing Emails

Erica Castilho

University of Central Florida



Part of the [Experimental Analysis of Behavior Commons](#), [Marketing Commons](#), [Social Media Commons](#), and the [Technology and Innovation Commons](#)

Find similar works at: <https://stars.library.ucf.edu/etd2023>

University of Central Florida Libraries <http://library.ucf.edu>

This Doctoral Dissertation (Open Access) is brought to you for free and open access by STARS. It has been accepted for inclusion in Graduate Thesis and Dissertation 2023-2024 by an authorized administrator of STARS. For more information, please contact STARS@ucf.edu.

STARS Citation

Castilho, Erica, "Navigating with Sharks: How the Marketing Practices Help to Create Successful Phishing Emails" (2023). *Graduate Thesis and Dissertation 2023-2024*. 254.

<https://stars.library.ucf.edu/etd2023/254>

NAVIGATING WITH SHARKS: HOW THE MARKETING PRACTICES HELP TO CREATE SUCCESSFUL PHISHING EMAILS

by

ERICA LEITE DE CASTILHO GRÃO

MSc Information Technology, 2012

BSc Information Systems Technology, 2006

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in the Department of Industrial Engineering and Management Systems
in the College of Engineering and Computer Science
at the University of Central Florida
Orlando, Florida

Fall

2023

Major Professor: Ben D. Sawyer

© 2023 Erica Leite de Castilho Grao

ABSTRACT

A phishing email is a crime where a scammer sends an email to get sensitive data. Everyday phishing email attacks impact billions of people worldwide. Preparing users to better identify phishing and avoid risky engagement with it is essential to combat this threat. We consider that as phishing emails and email marketing aim to target email clicks, scammers can use marketing practices in phishing emails to achieve their goals. However, the security research community doesn't explore deeply the similarities between phishing and email marketing. This study presents a distinctive framework known as the Phishing Engagement Marketing Optimization (PEMO). The primary objective of PEMO is to provide practices commonly used in email marketing to be applied to phishing simulations. This work presents the methodology to apply PEMO to phishing simulations and a hypothetical scenario to help understanding. We also determined which PEMO practices have a significant effect on phishing email engagement. To address the research problem, we ran an experiment with 400 participants to evaluate how they engage with 100 emails, where 92 were original emails and 8 were phishing emails. We also collected information about the motive of the decision-making behavior. Results showed that lower-risk participants, classified here as non-offenders, were not able to recognize phishing which applied Usability and Influence or Persuasion and Usability practices. In addition, higher-risk participants, classified here as offenders, increased replied and forwarded engagements with phishing which applied Persuasion practices. This work can help information security specialists better prepare users to avoid risky engagements with phishing attacks that apply marketing practices by designing phishing simulations that leverage those same practices.

Index Terms — phishing email, phishing decision-making, user behavior.

My passion for education made me the first in my family to pursue a Doctorate. I am proud to be part of the minority that represents less than 1% of Latin American women with a higher degree in the STEM area living in the U.S. I am proud to be recognized by the U.S. government as a professional of exceptional ability in computer management. I am even prouder to start my Ph.D. program while raising a 4-month-old baby and a preschooler in unprecedented times of the COVID-19 pandemic. I dedicate this work to my kids, Lucas and Bruno, hoping that my thirst for knowledge inspires them to study and go beyond where I get.

I also dedicate this work to my parents, Cleone and Zurlene, who taught me the importance of hard work, education, and the passion to share my knowledge and inspire others. In addition, I dedicate this work to my husband, Junior Grão, who has been my base, giving support when I require it: ears when I want to vent my tiredness, hands when I need to rise, strength and credibility when I think I couldn't continue.

ACKNOWLEDGMENTS

I want to thank my advisor, Dr. Ben D. Sawyer, for being an outstanding leader and helping me establish my path for graduation and my future career. I am incredibly grateful for his methods to oversee my desires before I could understand them. I also thank Dr. Matthew Canham for helping me dive into my research's psychological aspects and for driving me deeper into the cybersecurity industry. I thank NIST (National Institute of Standards and Technology) for funding part of this research and Knowbe4 for making available some free licenses for UCF use. In addition, the committee members that helped me to improve some aspects, directed my study and donated their time to my evaluation. Moreover, I thank Dr. Dave Miller for the peer review.

TABLE OF CONTENTS

ACKNOWLEDGMENTS.....	v
TABLE OF CONTENTS	vi
LIST OF FIGURES	viii
LIST OF TABLES	xi
LIST OF ABBREVIATIONS	xii
CHAPTER 1: INTRODUCTION	1
CHAPTER 2: BACKGROUND	4
Persuasion (P)	4
Usability (U)	7
Influence (I)	10
Key points	11
CHAPTER 3: THE PHISHING ENGAGEMENT MARKETING OPTIMIZATION (PEMO)	
FRAMEWORK	12
PEMO description	12
Application and Expectations	16
Key points	20
CHAPTER 4: METHODOLOGY	21
Participants	21
Methods and tools	22
Procedure	23
Analysis technique	28

Keypoints	32
CHAPTER 5: RESULTS AND DISCUSSION	34
Participants information	34
Results	36
Discussion	49
Keypoints	53
CHAPTER 6: CONCLUSIONS	55
APPENDIX A: PHISHING EMAIL IMAGES	59
Microsoft	60
Employee bonus list	68
APPENDIX B: IRB DOCUMENTS	76
APPENDIX C: CITI TRAINING COMPLETION CERTIFICATE	78
APPENDIX D: AUTHORIZATION FOR USE OF WEBQUAL 4.0	80
APPENDIX E: SPSS CONFIGURATION FOR MANCOVA	83
APPENDIX F: SPSS MANOVA RESULTS	93
APPENDIX G: PUBLICATIONS	96
REFERENCES	98

LIST OF FIGURES

Figure 1: PEMO introduces the use of practices (Persuasion, Usability, and Influence) commonly used by marketing specialists and identified to be used in the phishing context to impact the level of engagement with emails. The engagement is classified according to the risk of decisions. 13

Figure 2: Six steps to apply PEMO in phishing email simulations..... 17

Figure 3: This research aims to measure how each of the PEMO conditions on the left impacts the level of engagement with phishing emails on the right..... 19

Figure 4: Example of questions for each phase of the research, starting on pre-survey, going to experiment, and finishing on post-survey. 25

Figure 5: Relationship between variables included in the MANCOVA analysis..... 29

Figure 6: Classification of participants in offenders and non-offenders according to the number of clicked, replied or forwarded engagement levels..... 30

Figure 7: Participants per gender 34

Figure 8: Participants per race identification..... 35

Figure 9: Participants per age group 35

Figure 10: Participants per level of risk 36

Figure 11: Whisker Plot for Marked as phishing engagement level including P, U, PU, and OPE conditions. Covariates appearing in the model are evaluated at the following values: AGE_GROUP = .94, GENDER = .55, DURATION = 1741.06. Error bars: +/- 2 SE..... 40

Figure 12: Whisker Plot for Marked as phishing engagement level including I, PI, UI, and PUI conditions. The UI condition is highlighted because it had the most negative impact in marked as phishing. Covariates appearing in the model are evaluated at the following values: AGE_GROUP = .94, GENDER = .55, DURATION = 1741.06. Error bars: +/- 2 SE..... 40

Figure 13: Rates for each engagement level achieved in the OPE and UI conditions, according to non-offenders. The marked as phishing engagement is highlighted because it showed statistical significance in the previous analysis. 41

Figure 14: Rates for each engagement level achieved in the Original Phishing Email (OPE) and Usability + Influence(UI) conditions, according to offenders. The marked as phishing engagement is highlighted because it showed statistical significance in the previous analysis 42

Figure 15: Whisker Plot for [Deleted, Ignored or Marked as Spam] engagement levels including P, U, PU and OPE conditions. Covariates appearing in the model are evaluated at the following values: AGE_GROUP = .94, GENDER = .55, DURATION = 1741.06. Error bars: +/- 2 SE..... 44

Figure 16: Whisker Plot for [Deleted, Ignored, or Marked as Spam] engagement levels including I, PI, UI, and PUI conditions. The UI condition is highlighted because it had the most negative impact in marked as phishing. Covariates appearing in the model are evaluated at the following values: AGE_GROUP = .94, GENDER = .55, DURATION = 1741.06. Error bars: +/- 2 SE..... 44

Figure 17: Rates for each engagement level achieved in the OPE and PU conditions, for non-offenders. The deleted, ignored, or marked as spam engagement is highlighted because it showed statistical significance in the previous analysis. 45

Figure 18: Rates for each engagement level achieved in the OPE and PU conditions, for offenders. The deleted, ignored, or marked as spam engagement is highlighted because it showed statistical significance in the previous analysis. 45

Figure 19: Whisker Plot for [Clicked] engagement level including P condition. Highlighted is the P condition. Covariates appearing in the model are evaluated at the following values: AGE_GROUP = .94, GENDER = .55, DURATION = 1741.06. Error bars: +/- 2 SE..... 47

Figure 20: Whisker Plot for [Replied or Forwarded] engagement level including P condition. Highlighted is the P condition. Covariates appearing in the model are evaluated at the following values: AGE_GROUP = .94, GENDER = .55, DURATION = 1741.06. Error bars: +/- 2 SE..... 47

Figure 21: Rates for engagement level achieved in the Original Phishing Email (OPE) and Persuasion (P), according to non-offenders. 48

Figure 22: Rates for engagement level achieved in the Original Phishing Email (OPE) and Persuasion (P), according to offenders. 48

LIST OF TABLES

Table 1: Summary of the six rules of persuasion based on (Cialdini, 1993).....	5
Table 2: Summary of the techniques used in the Liking principle, based on Cialdini's book (Cialdini, 1993).....	7
Table 3: PEMO's Rules for the Persuasion Practice	14
Table 4: PEMO's Rules for the Usability Practice	15
Table 5: PEMO's Rules for the Influence Practice	16
Table 6: List of phishing emails sent to 8 groups (A-H) with a total of 64 variations. It includes the 7 PEMO conditions (P, U, I, PU, PI, UI, PUI) and the Original Phishing Email (OPE). Each group received a different variation of each email context. Each person received all PEMO conditions. Email context was counterbalanced around each participant group.	27
Table 7: Plan of emails to provide a stimulus similar to the real world. The table presents the email type, the number of emails, and the source of the emails.	27
Table 8: Univariate Tests for Persuasion + Usability + Influence (PUI). The significant effects are highlighted in gray.....	37
Table 9: Univariate Tests for Persuasion (P). The significant effects are highlighted in gray.	37
Table 10: Univariate Tests for Usability (U). The significant effects are highlighted in gray.	38
Table 11: Engagement rate for each PEMO condition. Highlighted are the statistically significant effects for each engagement level.....	39

LIST OF ABBREVIATIONS

- I - Influence
- OPE - Original Phishing Email
- P - Persuasion
- PI – Persuasion + Influence
- PU – Persuasion + Usability
- PUI – Persuasion + Usability + Influence
- PEMO - Phishing Engagement Marketing Optimization
- U - Usability
- UI – Usability + Influence

CHAPTER 1: INTRODUCTION

Phishing attacks, a crime where a scammer contacts a person and tries to get sensitive data, are a top cyber security threat to organizations and individuals (Sjouwerman, 2020). Indeed, organizations constantly suffer security attacks caused by individuals within the company who repeatedly fall victim to phishing emails (Canham et al., 2019), a type of phishing attack executed by email. Even though successful attacks have been reduced over the years, the amount of capital lost by companies to prevent or deal with this issue has increased after COVID-19 (Morgan, 2020). Recently, the Interpol agency has reported that criminals are taking advantage of increased security vulnerabilities caused by the working-from-home model to steal data, generate profit, and cause disorder in people's lives. For example, from January to April 2020, phishing emails corresponded to 59% of cyber threats related to COVID-19 (Stock, 2020). Consequently, companies need to control the risk of losing data and capital caused by phishing emails to succeed.

Phishing emails are arguably similar to another form of commercial goal-driven communication, email marketing since both of them target to convince users to engage positively with emails. As an example, in a broad context, marketing specialists constantly have to create and test ways to capture leads and transform them into buyers, and so do hackers and scammers who send phishing emails in search of their victims. Indeed, persuasion (Cialdini, 1993; Ibrahim et al., 2014; Walker, 2014), usability (Barnes & Vidgen, 2002; Gunelius, 2018; Ibrahim et al., 2014), and influence (Kahneman & Tversky, 1979; Brown & Fiorella, 2013; Farook & Abeysekara, 2016) are practices very commonly used by marketing specialists and identified to be used in the phishing context (Akbar, 2014; Jayatilaka et al., 2021; Parsons et al., 2019; P. Lawson et al., 2019; P. Lawson et al., 2020; Steves et al., 2020; Tanvir, 2020; Tolsdorf & Lo Iacono, 2020; Wright et al., 2014; Zielinska et al., 2016; Williams

et al., 2018; Williams & Polage, 2019). However, could marketing practices such as those cited before be used by hackers and scammers to be successful in their endeavors?

Although phishers regularly use marketing practices (Stojnic et al., 2021), the application of these practices in the phishing context needs further investigation by researchers, for example, the investigation of the use of Influence loss-based emails (Valecha et al., 2022). Indeed, researchers have not yet amply studied the application of the combination of several different marketing practices at the same time in one phishing email. As an example, researchers previously investigated the individual application of persuasion, usability, and influence in the phishing context, but not in combination. Research on this specific topic is necessary to learn more about the factors that impact phishing email engagement levels, and the type of actions that users do when dealing with phishing emails. Our proposed research aims to answer the gap in understanding the application of marketing practices in phishing emails to help identify the factors that increase the level of risk when in contact with phishing emails. Understanding these factors is essential for the improvement of phishing simulation campaigns executed in organizations by Information Security (InfoSec) departments.

To address our goal of understanding the application of marketing practices in phishing emails, we created the Phishing Engagement Marketing Optimization (PEMO) Framework. PEMO was designed with the three practices commonly used in marketing and phishing, known as persuasion, usability, and influence. PEMO contributes with a guide with rules of marketing practices to be applied in the process of creation of emails during phishing simulations. This work presents the methodology to apply PEMO to phishing simulations and a hypothetical scenario to help understanding. We also evaluated which marketing-derived practices from PEMO impacted the engagement level when applied to phishing emails. Specifically, we determined which PEMO practices had a significant effect on phishing email engagement levels. To address the research problem, we ran an experiment with 400

participants. We used an online survey to investigate how the participants engaged with a hundred emails, where eight were phishing emails. We also collected information about the motive of the decision-making behavior.

Consistent with some authors (Downs et al., 2007; Pattinson et al., 2012), we believe that understanding why people fall for phishing attacks is relevant for professionals to face cybersecurity challenges. Therefore, this paper helps information security specialists better prepare users to avoid risky engagements with phishing attacks using marketing practices by designing phishing simulations that leverage those same practices.

The remaining sections are organized as follows. 'Chapter 2: Background' summarizes and discusses the literature about the three practices commonly used in marketing and phishing. Then, 'Chapter 3: The Phishing Engagement Marketing Optimization (PEMO) Framework' introduces the new framework and presents a guide with PEMO's best practices to impact phishing email engagement level. Following, 'Chapter 4: Methodology' presents the methodology and criteria used for selecting subjects and data synthesis. Then, 'Chapter 5: Results and Discussion' summarizes the results we found and provides analysis and discussion. Finally, 'Chapter 6: Conclusions' introduces the final closure of this work.

CHAPTER 2: BACKGROUND

This chapter summarizes and discusses the literature about the three practices commonly used in marketing and phishing which are persuasion (10.1), usability (10.2), and influence (10.3). Each section explains the concept of the practice and discusses previous research on its application in marketing and the phishing email contexts. Finally, the section 'Key points' summarizes this chapter's most important findings (10.4).

Persuasion (P)

Persuasion (P) is a practice commonly used by marketing specialists to manipulate people's emotions to make a favorable decision, and which details can be found in Dr. Robert Cialdini's work (Cialdini, 1993). Some authors affirm that it is possible to induce someone to decide according to others' desires through persuasion: by manipulating their thoughts and feelings and, through it, their actions (Cooper, 2021). Even though persuasion might seem to be a manipulative and unethical behavior, professionals in marketing use it to convince others to decide to buy products and services. For example, a research (Ibrahim et al., 2014) introduced the persuasive visual design applied to websites, which helps marketers increase sales.

Persuasion uses words and technical arguments to change someone's behavior by first obtaining approval and trust, and then using a gradual work of conviction (Cooper, 2021). A seminal article on persuasion principles (Cialdini, 1993) summarizes the rules of persuasion: authority, consistency, liking, reciprocation, scarcity, and social proof.

Table 1 introduces an explanation of these rules. Each rule provides principles and techniques that can help manipulate people's decisions and be applied in different moments of contact between the interlocutor and the receiver.

Table 1: Summary of the six rules of persuasion based on (Cialdini, 1993).

Rule name	Summary
Authority	People trust others in positions of authority in some occupation or expertise.
Consistency	People try to justify their decisions as consistent with previous commitments.
Liking	People respond to requests made by those they like, even if they don't know this person. But they identify politeness and a "likable" personality.
Reciprocation	People feel obligated to repay favors to others, even if the favor was not previously asked by the individual.
Scarcity	People see value in rare things and feel motivated to obtain them quickly.
Social proof	People want to feel integrated into the community and trust in things that others are doing.

Scammers also use persuasion to succeed in phishing email attacks (Akbar, 2014). The use of persuasion is so disseminated in phishing emails that some tools analyze the use of rules of persuasion to decide about email blocking (Li et al., 2020; Nishikawa et al., 2020). In addition, some studies investigated the principles most used in phishing emails. A study (Akbar, 2014) that reported the use of rules of persuasion in phishing emails revealed that the authority principle was used for 96.1% of phishing emails analyzed, while the scarcity principle was used for 41.1%. These numbers are supported by other research (P. A. Lawson et al., 2019; Tanvir, 2020) that stated that the four principles most used in phishing emails are commitment/ consistency, liking, authority, and scarcity, while the authority principle is the most explored in volume. Furthermore, one study (Zielinska et al., 2016) that examined a dataset of 887 emails sent between 2010 and 2015 found that the persuasion principles of commitment and consistency, as well as scarcity, increased during that time, while the principles of reciprocation and social proof decreased over the same period.

Overall, researchers investigated the principles that create more susceptibility to phishing emails. Indeed, one research (Wright et al., 2014) demonstrated the effectiveness of using rules of persuasion in phishing emails compared to emails that don't apply the principles. Users have a high level of trust in emails utilizing the liking principle (P. Lawson

et al., 2020; P. A. Lawson et al., 2019), social proof, and reciprocity (Tanvir, 2020). On the other hand, emails utilizing principles of authority and scarcity usually cause more suspicion and distrust, resulting in a high tendency to be designated as phishing attacks (P. Lawson et al., 2020; Tanvir, 2020). Not all agree, and some work finds that phishing emails utilizing only the liking persuasion principle are least likely to be detected by the recipient (P. Lawson et al., 2020). Others show that authority and urgency lead to high click rates (Williams et al., 2018). While some studies have shown that scarcity and social proof are not considered as effective as the authority principle, others have shown that users are not susceptible to the authority principle and are, in fact, most susceptible in emails containing social proof and scarcity principles (Parsons et al., 2019). Perhaps users are not broadly susceptible to scarcity but are commonly susceptible to consistency and reciprocity principles. Perhaps reciprocity is the most persuasive principle, while the social proof and scarcity principles were not considered to be persuasive (as in Parsons et al., 2019). Possibly, the topic of the persuasion principles that impact phishing email engagement can benefit from more investigation.

Eventually, some research was developed to verify the correct identification of phishing emails regarding the use of persuasion principles. One study (Tanvir, 2020) surveyed 136 participants and showed a relationship between the common persuasion strategies, the number of phishing cues, and email exposure time. Individuals can better detect phishing emails that use authority and scarcity principles (P. Lawson et al., 2020; Tanvir, 2020).

For the purpose of this research, we will work just with the liking principle, to be consistent with previous studies that stated that the use of the liking principle alone is more persuasive in emails (Lawson et al., 2020). The liking principle of persuasion states that people prefer to say yes to requests of someone that they know and like. Thus, the objective of this principle is to establish a “liking” feeling from the receptor of the message to the provider of the message (Cialdini, 1993). Cialdini described six techniques that can be applied to achieve

the Liking principle. These techniques, described in Table 2, are known as physical attractiveness, similarity, compliments, familiarity, contact and cooperation, and condition and association.

Table 2: Summary of the techniques used in the Liking principle, based on Cialdini's book (Cialdini, 1993)

Technique	Description
Physical attractiveness	Good-looking people have an advantage in social interaction.
Similarity	We like people like us in opinions, personality traits, background, dress, interests, lifestyle, etc.
Compliments	Use of positive estimations from people who want something from us.
Familiarity	We like things that are familiar to us, like names that seem familiar or ethnic groups.
Contact and cooperation	Keep people working for the same goals, with the idea of "pull together" for mutual benefits. It is summed to competitiveness with another group.
Condition and association	People are conditioned to associate the message with the messenger. So, people like others who deliver good news or show success in a similar endeavor they are trying to conquer.

Despite which technique of the Liking principle is applied, persuasion continues to impact trust and cause phishing susceptibility. Along with those lines, usability can be used for the same purpose.

Usability (U)

According to ISO FDIS 9241-210 (ISO, 2009), usability (U) is connected to the proportion of effectiveness, efficiency, and satisfaction that a product, system, or service delivers to a user (Bevan, 2009; Hornbæk, 2006). Some believe that usability cannot be directly measured due to the lack of validity measures, but instead, one can measure aspects of it (Hornbæk, 2006). Human-Computer Interaction (HCI) researchers have been adopting the usability concept stated by ISO to categorize the approaches related to the aspects of usability research as effectiveness, efficiency, and satisfaction (Hornbæk, 2006). According to previous research (Bevan, 1995), there is an interaction between these three aspects, with

satisfaction being based solely on the user and effectiveness and efficiency related to the user and its interaction with the product.

Many researchers have associated usability with 'ease of use' (Flavián et al., 2006; Hornbæk, 2006). However, some authors connect usability and design (Barnes & Vidgen, 2002; Norman, 2004). WebQual4.0 (Barnes & Vidgen, 2002), a method to evaluate the quality of websites, describes usability with the following aspects: ease to learn, clear and understandable, ease to navigate, ease to use, attractive appearance, appropriate design, sense of competence, and positive user experience. Another author who connects usability and design is Donald Norman in his book 'Emotional Design' (Norman, 2004). Norman cited some studies placed in the early 1990s that proved that attractive things work better by connecting usability and aesthetics. Consistent with these authors, we will also consider usability related to ease of use and design in this research.

In their daily routine, email marketing specialists need to include usability in their work to achieve their goals. Hence, email marketing platforms like Mailchimp, for example, provide many email templates with a professional design that highlights the next steps and engagement goals by providing easy-to-use buttons and links. Indeed, these templates are differentiated according to segments like the targeted customer type and email topic. Therefore, the need for web design knowledge is much appreciated for email marketing professionals to include usability in their email marketing templates.

Marketing professionals constantly appeal to usability to impact their consumers in emails, but phishers are starting to get attention to it. Indeed, usability is of high importance in written communication. For example, some authors argue that design is the first thing noticed when opening messages (Gunelius, 2018; Williams & Polage, 2019). Above all, users look for a professional layout, logo, button appearance, and the number of links and banners to help in decisions about email marketing, but also in phishing emails (Gunelius, 2018; Jayatilaka et al., 2021b; Kumar, 2021; Li et al., 2020; Steves et al., 2020; Tolsdorf & Lo

Iacono, 2020; Williams & Polage, 2019). Specifically, in phishing email messages, a study (Williams & Polage, 2019) found that emails with professional design, such as those containing a logo and a copyright statement, are more persuasive, trustworthy, and likely to be responded to than emails without professional designs. Hence, the need to prepare professionals to recognize when phishers use these features commonly used by marketing professionals to influence users.

In this specific research, similar to (Barnes & Vidgen, 2002), we connected usability to the following aspects: ease to learn, clear and understandable, ease to navigate, ease to use, attractive appearance, appropriate design, sense of competence, and positive experience. Our adaptation of these factors to the email context is as follows.

1. Ease to learn: it is easy to understand how to interact with the email.
2. Clear and understandable: the interaction with the email is clear. The user knows what to do next.
3. Ease to navigate: navigation is the process or activity of accurately ascertaining one's position and planning and following a route. When the users click on emails, they are destined to another environment, like landing pages, websites, eCommerce, etc. So, we considered that one couldn't navigate emails. Thus, we removed this aspect of our framework.
4. Ease to use: the user quickly finds and clicks on links, buttons, or attachments related to the email template. We are not considering the interaction with the email service (webmail, software, etc.).
5. Attractive appearance: the appearance of the email design is beautiful with appropriate decoration, colors, enough space between features, proper fonts, precise, symmetric, etc.
6. Appropriate design: the web design is appropriate to the sender, the message being delivered, and the demographic information of the reader.

7. Sense of competence: the email design transmits professionalism, efficiency, and success.
8. Positive experience: as stated by ISO FDIS 9241-210, user experience is related to the perceptions and responses of a person regarding the use of a product, system, or service (Bevan, 2009). Thus, the user must have an overall positive experience using the email.

Influence (I)

We define influence (I) as the capacity to affect the decisions of others, for example, the decision to engage with emails. The awarded work about prospect theory (Kahneman & Tversky, 1979) divided the influence effect into losses and gains. It cited that, apparently, people are more affected when losing a sum of money than when gaining the same amount. A recent work (Greve et al., 2021) provided a theory that for decision-making under risk, individuals tend to opt for risky alternatives when there is the possibility of loss. As an example, loss aversion leads to risk-taking in gambling. Indeed, the results of this research showed that loss aversion for organizational or individual performance reduces decision-making quality and increases risk-taking. The same theory can be applied in the email context.

Email messages using the influence technique usually either reward individuals for more engagement or suggest a loss if there is no engagement. For example, email marketing offers coupons for a discount as a reward after an order. On the other hand, they can also describe that you will lose some unique opportunity if you don't click to buy an item in promotion for some hours.

Some research (Biswas & Mukhopadhyay, 2019; Goel et al., 2017; Williams & Polage, 2019) previously analyzed the influence techniques that affect phishing email clicks and considered loss-based emails a more effective approach.

Key points

- Usability is connected to the proportion of effectiveness, efficiency, and satisfaction that a product, system, or service delivers to a user (Bevan, 2009; Hornbæk, 2006; ISO, 2009). In addition, usability is also connected to design (Barnes & Vidgen, 2002; Norman, 2004).
- Persuasion uses words and technical arguments to change someone's behavior by first obtaining approval and trust, then using a gradual work of conviction (Cooper, 2021). Evidence suggests that the liking principle is very impactful in email engagement (P. Lawson et al., 2020; P. A. Lawson et al., 2019). The Liking principle states that people respond to requests made by those they like, even if they don't know this person. But they identify politeness and a "likable" personality (Cialdini, 1993).
- We define 'influence' as the capacity to affect the decisions of others. For example, the decision to engage with emails. Evidence suggests that the possibility of loss is very effective at impacting decisions (Kahneman & Tversky, 1979; Greve et al., 2021; Biswas & Mukhopadhyay, 2019; Williams & Polage, 2019).

CHAPTER 3: THE PHISHING ENGAGEMENT MARKETING OPTIMIZATION (PEMO) FRAMEWORK

This chapter describes an original conceptual framework called the Phishing Engagement Marketing Optimization (PEMO) Framework. The remaining sections are organized as follows. Section 'Introduction to PEMO' presents the framework, its best practices, and how to use it (11.1). Then, the section 'Application and expectations' brings a methodology explaining how InfoSec can use PEMO, introduces a hypothetical example, and describes our hypothesis (11.2). Finally, the section 'Key points' summarizes this chapter's most important findings (11.3).

PEMO description

In this study, we have introduced a distinctive framework known as the Phishing Engagement Marketing Optimization (PEMO) Framework. The primary objective of the PEMO framework is to exert an influence on the engagement level of phishing email campaigns, thereby contributing to the enhancement of cybersecurity awareness and response. Specifically applied within the context of this research, as introduced in Figure 1, the PEMO framework leverages three essential marketing practices: Persuasion, Usability, and Influence. These practices have been strategically selected to maximize the effectiveness of the framework in influencing user behavior toward phishing emails since they are commonly used in marketing and phishing (Akbar, 2014; Jayatilaka et al., 2021; Parsons et al., 2019; P. Lawson et al., 2019; P. Lawson et al., 2020; Steves et al., 2020; Tanvir, 2020; Tolsdorf & Lo lacono, 2020; Wright et al., 2014; Zielinska et al., 2016; Williams et al., 2018; Williams & Polage, 2019). Specifically, the persuasion practice leverages the liking principle, the usability practice leverages effectiveness, efficiency, satisfaction, and design, and the influence practice leverages loss.

In addition, the PEMO framework introduces a hierarchical structure consisting of four distinct levels of engagement: [Marked as phishing], [Deleted, ignored, or marked as spam], [Replied or forwarded], and [Clicked]. These engagement levels were carefully chosen and grouped to better identify the level of risk of decisions. The [Marked as phishing] engagement refers to the action of recognizing an email as phishing. The [Deleted, ignored, or marked as spam] engagement refers to the action of deleting an email, leaving it in the inbox, or recognizing that as spam, a marketing email sent without authorization. The [Replied or forwarded] is linked to the actions of answering an email to the sender or forwarding it to someone else. Finally, the [Clicked] engagement refers to the action of clicking on a phishing email link. We didn't include download as an engagement level on this framework since in this specific study we just studied phishing emails providing links. This stratified approach enables a comprehensive understanding of user responses to phishing emails, ranging from lower-risk decisions to higher-risk decisions.

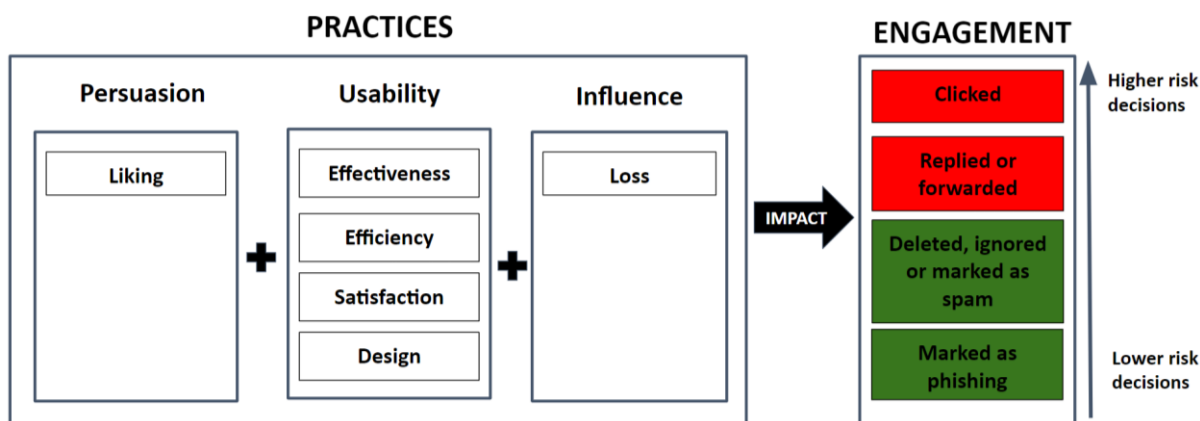


Figure 1: PEMO introduces the use of practices (Persuasion, Usability, and Influence) commonly used by marketing specialists and identified to be used in the phishing context to impact the level of engagement with emails. The engagement is classified according to the risk of decisions.

The PEMO Framework also introduces a list of rules for each of its practices. These rules were adapted from previous research or book publications to direct the professionals about the to-dos and not-to-dos to be applied in the phishing email creation

process to impact the level of engagement. Following this, we introduce the rules for each practice, as outlined in Table 3, Table 4 and Table 5.

Table 3: PEMO's Rules for the Persuasion Practice

Persuasion Practices: Liking		
Code	Rules for Persuasion Practices	Adapted from source
BP01	Use softness of expression or courtesy	(Nishikawa et al., 2020)
BP02	Conduct contextual aspects of email interaction, such as things done in the past, or the statements/conduct of other people	(Nishikawa et al., 2020)
BP03	Provide personalization in the interaction, like using the user's name and sending content that is relevant to users (also known as high premise alignment)	(Goldman, 2020; Gunelius, 2018)
BP04	Use of compliments	(Cialdini, 1993; Parsons et al., 2019)
BP05	Be informal when possible	(Parsons et al., 2019)
BP06	Don't send survey requests	(Parsons et al., 2019)
BP07	Establish similarity by sharing some background, interest, lifestyle, place where you were born or live, or opinion that you possibly have in common	(Cialdini, 1993)
BP08	Provide some positive compliments	(Cialdini, 1993)
BP09	Use a familiar name for the sender. Use names that users can recognize	(Cialdini, 1993; Gunelius, 2018)
BP10	Provide a picture of a good-looking sender	(Cialdini, 1993)
BP11	Create cooperation to achieve the goals for mutual benefits	(Cialdini, 1993)
BP12	Don't force the use of scarcity, for example, including features like the shortage of items, things, or privileges, or pushing urgent actions in an unpolite way.	Based on the findings of Chapter 2
BP13	Don't force the use of authority by using figures of power and demanding actions.	Based on the findings of Chapter 2
BP14	Talk about your success in a similar endeavor as the email receiver.	(Cialdini, 1993)
BP15	Deliver good news. Try not to associate your email with bad news	(Cialdini, 1993)

Table 4: PEMO's Rules for the Usability Practice

Usability Practices: effectiveness, efficiency, satisfaction, and design		
Code	Rules for Usability Practices	Adapted from source
P16	The call to action must be understandable (all links must be easy to see).	-
P17	Use well-formatted HTML with no broken coding.	(Gunelius, 2018)
P18	Don't use embedded forms (include a link to the form).	(Gunelius, 2018)
P19	Don't use excessive uppercase words.	(Ferreira & Teles, 2019; Gunelius, 2018)
P20	Don't use capitalization of the first letter of every word.	(Ferreira & Teles, 2019)
P21	Don't use excessive punctuation expressing strong feelings, emphasis, or interrogation ('!', '?').	(Ferreira & Teles, 2019; Gunelius, 2018; Steves et al., 2020)
P22	Don't use excessive symbols/non-alphanumeric characters (e.g., *, √).	(Ferreira & Teles, 2019)
P23	Review and correct spelling errors.	(Steves et al., 2020; Tanvir, n.d.)
P24	Use of real people's pictures.	(Furgison McEwen, 2016)
P25	Use images that can load quickly.	(Gunelius, 2018)
P26	Don't use Flash JavaScript or videos.	(Gunelius, 2018)
P27	Include more text than images.	(Gunelius, 2018)
P28	Include an easy-to-see unsubscribe link.	(Gunelius, 2018)
P29	Don't send messages with attachments.	(Gunelius, 2018)
P30	Avoid spam trigger words.	(Gunelius, 2018)
P31	Don't use a URL shortener.	(Gunelius, 2018)
P32	Use responsive messages that will adapt to mobile devices.	(Gunelius, 2018)
P33	If sending a business email, use your logo.	(Gunelius, 2018; Jayatilaka et al., 2021; Li et al., 2020; Steves et al., 2020; Williams & Polage, 2019) (Gunelius, 2018; Jayatilaka et al., 2021; Li et al., 2020; Steves et al., 2020; Tolsdorf & Lo Iacono, 2020; Williams & Polage, 2019)
P34	Include a footer.	(Jayatilaka et al., 2021)

Code	Rules for Usability Practices	Adapted from source
P35	Use minimal branding with the colors of your brand.	<u>(Steves et al., 2020)</u>
P36	Use a copyright statement.	<u>(Tolsdorf & Lo Iacono, 2020; Williams & Polage, 2019)</u>
P37	Use an email signature.	<u>(Parsons et al., 2019)</u>
P38	Include privacy info in the footer.	<u>(Jayatilaka et al., 2021)</u>
P39	Use URLs that are easy to identify and read.	<u>(Tanvir, 2020.)</u>
P40	Be sure to use an email that matches the brand and the URL.	<u>(Tanvir, 2020)</u>
P41	Provide a professional look in the overall email.	(Gunelius, 2018; Jayatilaka et al., 2021; Steves et al., 2020; Tolsdorf & Lo Iacono, 2020)

Table 5: PEMO's Rules for the Influence Practice

Influence Practices: loss		
Code	Rules for Influence Practices	Adapted from source
P42	Include a loss-based but soft tone, like, for example, suggesting that the user will lose access to something or lose a specific and unique opportunity	(Williams & Polage, 2019)
P43	Try to create competitiveness against another group(s)	(Cialdini, 1993)

Application and Expectations

We expect that the PEMO practices will impact the level of engagement with phishing emails and increase the level of decision risks. Information Security (InfoSec) departments can use this research to understand the factors that impact a user's decision regarding engagement with phishing emails, and the level of risk they are exposed to. Consistent with some authors (Downs et al., 2007; Pattinson et al., 2012), we believe that understanding why people fall for phishing attacks is relevant for professionals to face cybersecurity challenges. Consequently, we suggest that the PEMO framework contributes with the knowledge to reduce the risk of data loss and profitability of organizations.

Some previous research evidence that training can be effective in reducing the likelihood of people providing information in phishing attempts (Kumaraguru et al., 2009). So, we also planned the use of PEMO for training. The PEMO framework can possibly be applied to guide InfoSec on phishing simulations and help discover opportunities for improvements in training according to segments. For that, one must follow the six following steps, as presented in Figure 2.



Figure 2: Six steps to apply PEMO in phishing email simulations.

First, InfoSec needs to segment the users that will receive the campaigns. For example, create a segment for each department of the company; Following, InfoSec needs to decide how the campaigns will be managed according to the PEMO practices. InfoSec needs to answer these questions: will all the segments receive the same type of simulation? Do some segments can be more vulnerable to certain practices? After answering the questions, the professional can plan the campaigns. For example, segments A, and B will receive a phishing email simulation using rules of persuasion (P), segments D, and E will receive a phishing email simulation using rules of Usability + Influence (UI) and segment F will receive a phishing simulation with for all PEMO practices – Persuasion + Usability + Influence (PUI). Next, InfoSec needs to get some templates to use in the phishing simulation. Moving on, the templates need to be edited following the PEMO's rules according to the campaign plan. Later, InfoSec will schedule the simulation using some software. After running the simulation, the results will be analyzed and the target for improvement will be defined. For example, InfoSec can determine that the phishing simulations that received a certain percentage of clicks or replies will be the focus of training. Finally, the users who clicked or replied to the simulations selected as targets for improvement will be selected for specific training to be able to recognize phishing using the PEMO practices included in the simulation.

To help with the understanding of the PEMO application, we provide here a hypothetical example. John is an InfoSec professional in the company ABC who decided to incorporate PEMO in his phishing simulations. John segmented his users according to the department where they work. He planned to run seven different campaigns. In the first campaign, users would receive three phishing emails, each one using PEMO's rules for persuasion (P), usability (U), and influence(I). In the following week, in the second campaign, users would receive more than three emails, each one using PEMO's rules for PU, PI, or UI. In the third week, users would receive one email applying all the PEMO's rules (PUI). John planned the campaign this way, so he could better understand the practices that would have more impact in each department, in addition to individually understanding the vulnerability of his users. John selected 7 different phishing templates, each one with a different sender and topic. He updated all the templates according to the campaign plan and the PEMO's rules. He scheduled the simulation as the campaign plan. Once the campaigns finished, he analyzed the results. He determined that the phishing simulations that received 20% of clicks or 30% of responses would be the target for improvements. John noticed an increase in the phishing clicks when applying PUI practices for the sales department, and an increase in the phishing responses when applying P practices in the administrative department. John trained those two departments in the PEMO practices they were more vulnerable and how to identify red flags on them. He started with the sales department, since according to PEMO, clicks correspond to a higher-risk decision. Some months after it, one employee of the administrative department received a phishing using marketing practices and he reported it to InfoSec. John was able to inform all employees about the attempt and blocked the phishing email. ABC saved hundreds of thousands of dollars.

In this specific research, we want to analyze the effect of marketing practices on the phishing email context. So, we decided to create PEMO as our innovative framework to show how three specific practices commonly used in marketing and phishing could impact

the phishing engagement level and the rules that need to be used in email creation to simulate phishing emails applying marketing practices. Specifically, we wanted to understand if the marketing-derived practices from the PEMO framework would impact the phishing email engagement level when compared to some original phishing emails. If so, more specifically, we wanted to understand what practices of the PEMO framework have a higher effect on the phishing email engagement level. Therefore, we measured the impact of each of the PEMO framework conditions, consistent with each of the practices alone or in combination, over the phishing email engagement level. As an example, we used as PEMO conditions the Original Phishing Email (OPE), Persuasion (P), Usability (U), Influence (I), Persuasion + Usability (PU), Persuasion + Influence (PI), Usability + Influence (UI) and Persuasion + Usability + Influence (PUI) as introduced in Figure 3.

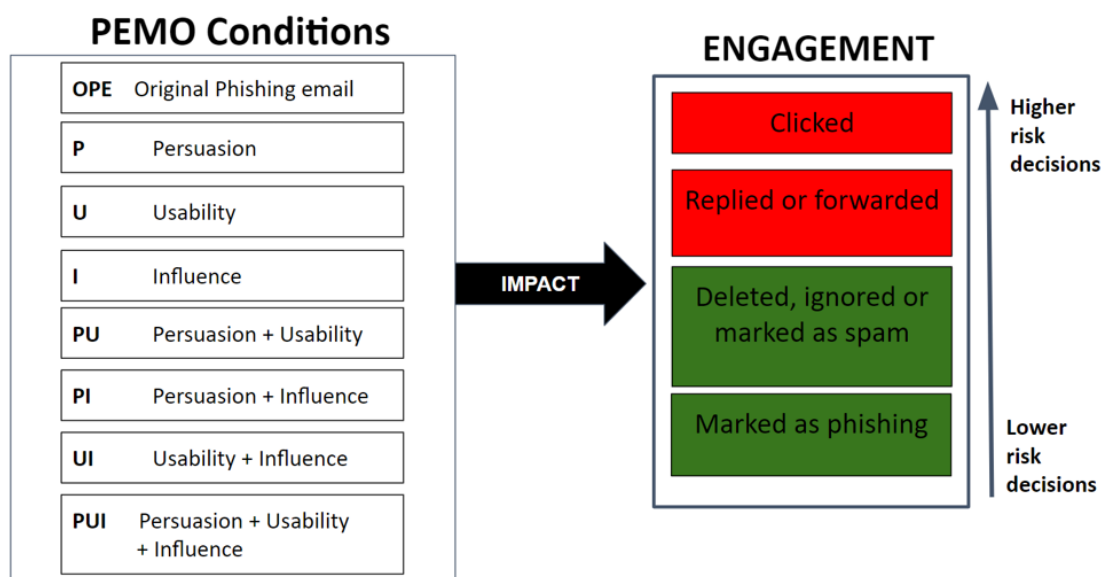


Figure 3: This research aims to measure how each of the PEMO conditions on the left impacts the level of engagement with phishing emails on the right.

To verify if the PEMO framework works as expected, these are our hypotheses

(H):

H0 - PEMO will not impact phishing engagement when compared to the original phishing emails.

H1 – PEMO will impact phishing engagement when compared to the original phishing emails.

H2 - [PU] will have the most significant negative impact over [marked as phishing] engagement when compared to the original phishing emails.

H3 - [I] will have the most significant negative impact over [deleted, ignored, or marked as spam] engagements when compared to the original phishing emails.

H4 - [PI] will have the most significant positive impact over the [replied or forwarded] engagements when compared to the original phishing emails.

H5 - [PU] will have the most significant positive impact over [clicked] engagement when compared to the original phishing emails.

H6 - PEMO practices will increase the level of decision risks.

Key points

- The PEMO framework leverages three essential marketing practices: Persuasion, Usability, and Influence.
- The persuasion practice leverages the liking principle, the usability practice leverages effectiveness, efficiency, satisfaction, and design, and the influence practice leverages loss.
- The PEMO framework introduces a hierarchical structure consisting of four distinct levels of engagement: [Marked as phishing], [Deleted, ignored, or marked as spam], [Replied or forwarded], and [Clicked]. The engagement is classified according to the risk of decisions.
- Information security professionals can use PEMO's rules to construct phishing simulations, identify areas of training needed, and prepare their users to face phishing emails using marketing practices.

CHAPTER 4: METHODOLOGY

This chapter intends to explain the methodology planned to test the stated hypothesis. The remaining sections are organized as follows. Section 'Participants' introduces the source of all participants (12.1). Section 'Methods and tools' provides a general overview of the approaches executed for this research (12.2). Section 'Procedure' introduces the phases of the study (12.3). Section 'Analysis technique' explains the methods used to analyze the data (12.4). Finally, the section 'Key points' summarizes this chapter's most important findings (12.5).

Participants

We recruited 400 participants for our study to target high statistical power to detect the effect of all 8 PEMO conditions over the engagement levels introduced in Chapter 3. We used Prolific, a research participant-finding website that was chosen for its reliability, and diverse user base and to facilitate an ease and fast data collection. Our inclusion criteria involved selecting individuals between the ages of 20 and 60 who currently reside in the United States. This age range was specifically chosen to ensure that our sample consisted of individuals with prior work experience, spanning across various fields. There was no minimum requirement for work experience, as we aimed to capture a broad range of perspectives. The average age of our participants was 34 years old, a significant parameter in the context of our research objective. We wanted participants to have previous experience with a work environment, to help companies understand professionals' behavior when dealing with phishing applying marketing practices. Fluency in the English language was a prerequisite for participation, allowing for effective communication during the study. As a token of appreciation for their time and effort, participants were provided with a compensation of \$5.

One participant didn't finish the research, so we ended with 399 participants. Our study had no restrictions based on gender, resulting in a gender distribution of 53% male participants, 46% female participants, and 1% who chose not to disclose their gender. By embracing gender diversity, we aimed to enhance the generalizability of our findings and mitigate potential biases that may arise from skewed gender representation. In terms of ethnicity, the breakdown of our participants was as follows: 72% identified as white, 9.5% as black, 6% as Asian, and 12.5% as belonging to other ethnicities. Self-identification was utilized for determining ethnic categorization. The inclusion of participants from diverse ethnic backgrounds allowed us to consider a range of perspectives and experiences. By adhering to a diverse participant selection criteria, we aimed to create a robust and representative sample for our study, ensuring that our findings apply to a broader population.

Methods and tools

Following the approach of previous studies (Downs et al., 2007; Lawson et al., 2020; Pattinson et al., 2012), we employed an online survey as our primary research method to investigate participants' engagement with various types of emails. An online survey was chosen due to its scalability, quicker delivery, and ease of data collection. The investigation of participants' engagement with emails can help to better understand what impacts the decision-making process to engage with phishing emails, thus supporting the capacitation of people to avoid it. The online survey was conducted using Qualtrics, a reputable online software platform known for its survey delivery capabilities. Through this survey, we aimed to assess the practical application of PEMO's (Persuasion Usability Framework) best practices within the context of phishing emails.

For the study, we collected a set of eight original phishing email templates from Knowbe4, a market leader platform specializing in security awareness training and simulated phishing attacks. Subsequently, we modified these phishing emails to manipulate each

dimension of PEMO, namely persuasion, usability, and influence. The label "yes" was used to indicate the application of PEMO's best practices, while "no" indicated the absence of such practices. Thus, our study employed a 2 (Persuasion: yes, no) x 2 (Usability: yes, no) x 2 (Influence: yes, no) factorial design, leading to the 8 PEMO conditions (OPE, P, U, I, PU, PI, UI, PUI) introduced in Chapter 3. We chose to work with a factorial design to understand the effect of each factor analyzed, but also the interaction between them. With this design, all the possible combinations of factor levels can be investigated in each replication. As an example, we could have as an outcome that Persuasion didn't have an effect on phishing email [clicked] engagement while the combination of Persuasion and Usability had a positive effect on it.

Procedure

In a previous study (Carella et al., 2017), it was noted that participants who were aware of their involvement in a phishing study tended to interact differently compared to the general population. Building upon this insight, as we wanted to guarantee that participants would interact as the general population, our research adopted a similar approach. To ensure transparency, no specific training was provided to participants, and they were informed that they would be engaging with various types of emails without explicitly mentioning the focus on phishing emails. As we had ethical concerns about the use of phishing emails on this study, the participants were explicitly notified about the use of deception. In addition, at the end of the study the participants received a message explaining the actual purpose of the research about the impact of marketing practices on phishing emails. Moreover, the participants learned which of the emails were phishing emails. Participants received a thorough explanation of the research objectives. We obtained informed consent and authorization for the publication of the research findings from all participants.

Participants were assigned a specific role-playing position in the experiment, taking inspiration from previous studies (Downs et al., 2007; Pattinson et al., 2012; Sawyer et

al., 2015). They assumed an administrative role within the fictitious organization "Cog Industries" and were responsible for processing forms containing sensitive information. In addition to their primary tasks, participants were required to interact with emails. Each participant was provided with a designated employee name, "Jordan Williams," and an associated email address, "administrative@cogindustries.com." The deliberate choice of an androgynous first name and a popular last name aimed to ensure that participants could easily identify with their assigned role-playing.

Participants were permitted to use their personal devices of any screen resolution during the study. No data regarding browser, resolution, or equipment specifications were gathered since the variability of those factors was not the focus of this specific study. Future research can analyze the impact of screen resolution on the phishing engagement level to check for example if participants using mobile devices would increase the level of risk decisions when dealing with phishing emails applying the PEMO practices. The research team had no access to personally identifiable information. Participants were informed in advance about the average time required to complete the tasks, but no specific time limit was imposed. On average, the participation duration was 29 minutes, with an average of 17 seconds spent per question.

Participants went through three phases: a pre-survey, an experiment, and a post-survey. An example with some questions of each phase can be found in Figure 4.

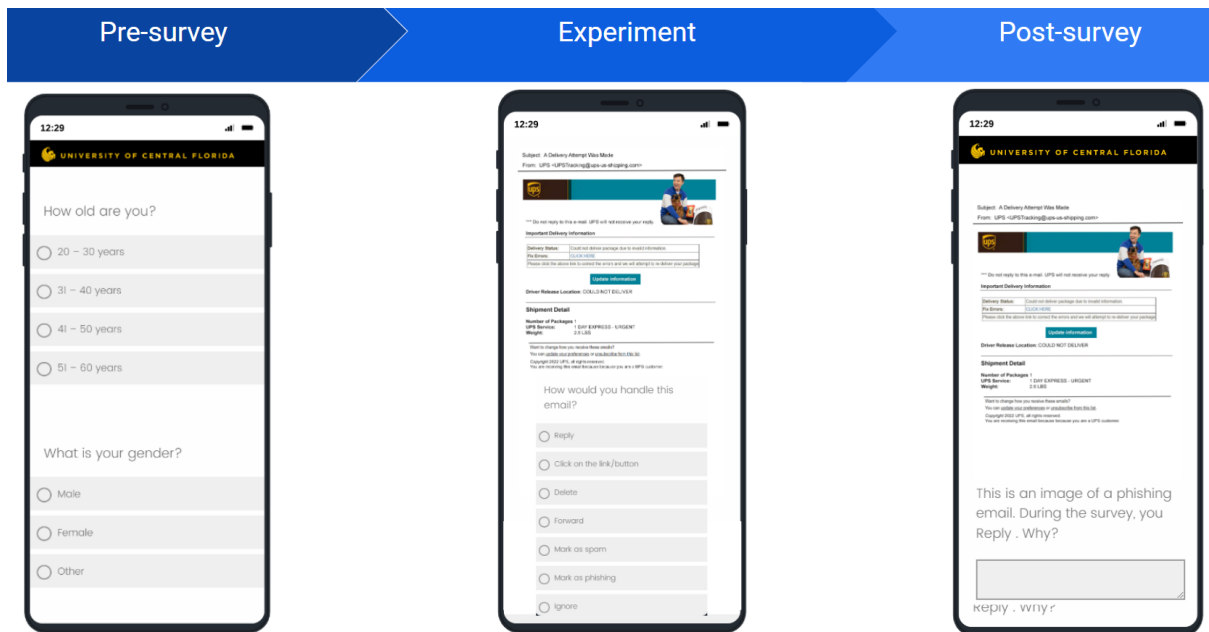


Figure 4: Example of questions for each phase of the research, starting on pre-survey, going to experiment, and finishing on post-survey.

In the pre-survey phase, we gathered basic demographic information, including age groups (20-30 years, 31-40 years, 41-50 years, 51-60 years) and gender (female, male, other).

During the experiment, participants were asked to assess their intended actions when engaging with emails. The response options included 'reply' or 'reply/upload file', 'delete', 'click on the link/button', 'download file', 'forward', 'mark as spam', 'mark as phishing', and 'ignore'. To determine the number of regular and phishing emails, we considered the Signal Detection Theory (SDT) (Wickens, 2002) and aimed to provide a naturalistic experience. Industry reports indicate that the average person receives and sends 121 business emails per day, with 1.2% being malicious (Chang, 2021). Therefore, each participant was presented with 100 email images to review, consisting of 92 regular email images, those that don't represent harm, and 8 phishing emails.

To ensure a comprehensive analysis, each phishing email represented a distinct email context. An email context is a circumstance, background, or environment of the email composed by the topic of the email, and the sender that matches the topic and the

content. In this research, each email incorporated variations in the sender, email topic, and format. We acknowledged that the email context plays a crucial role in shaping individuals' responses and their perception of message importance (Dabbish et al., 2005). Therefore, we specifically designed email contexts that were relevant to work-related scenarios.

Each email context was related to 8 email variations. One for the original phishing email and one for each PEMO condition (P, U, I, PU, PI, UI, PUI) totaling 7 more variations. The email variations were designed to explore the effects of PEMO techniques in a 2 (Persuasion: yes, no) x 2 (Usability: yes, no) x 2 (Influence: yes, no) factorial design. It is worth noting that while the original templates may have initially incorporated some PEMO practices, no further editing or modifications were made to them.

Participants were randomly assigned to one of eight groups (A, B, C, D, E, F, G, H), with an average of 50 participants per group. Each group (A to H) received a distinct phishing email variation for each email context, resulting in a total of 64 unique phishing email variations. Each person received all PEMO conditions. The email context was counterbalanced around each participant group. Table 6 provides an overview of the specific phishing email variations assigned to each group. The variations were designed to manipulate the factors of Persuasion (P), Usability (U), Influence (I), Persuasion + Usability (PU), Persuasion + Influence (PI), Usability + Influence (UI), and Persuasion + Usability + Influence (PUI). The original phishing email is denoted as 'OPE' in the table.

To create a realistic stimulus, we designed four types of emails: download requests, upload requests, emails with links, and emails with no response needed, as presented in

Table 7. As the role-play scenario revolved around administrative tasks, 50% of the stimuli were related to downloading and uploading documents, sourced from a previous research database (Sawyer et al., 2015). Additionally, 45% of the emails in the survey contained links, including the eight phishing emails, company communications, meeting

requests, email marketing, and spam. While the original templates were obtained from knowbe4, other emails were sourced from the author's personal email. Emails that did not require a response constituted 5% of the total, sourced from personal emails or customized. Each email was associated with specific email addresses and optionally included salutations and signatures, closely resembling real-world emails.

Table 6: List of phishing emails sent to 8 groups (A-H) with a total of 64 variations. It includes the 7 PEMO conditions (P, U, I, PU, PI, UI, PUI) and the Original Phishing Email (OPE). Each group received a different variation of each email context. Each person received all PEMO conditions. Email context was counterbalanced around each participant group.

#	Email context	A	B	C	D	E	F	G	H
1	Microsoft - email not delivered	P	U	I	PU	PI	UI	PUI	OPE
2	Employee bonus list	U	I	PU	PI	UI	PUI	OPE	P
3	Dropbox - Document shared	I	PU	PI	UI	PUI	OPE	P	U
4	PTO Policy Changes	PU	PI	UI	PUI	OPE	P	U	I
5	UPS: A Delivery Attempt Was Made	PI	UI	PUI	OPE	P	U	I	PU
6	LinkedIn: Join my network	UI	PUI	OPE	P	U	I	PU	PI
7	IT: Software Update	PUI	OPE	P	U	I	PU	PI	UI
8	DocuSign: Your DocuSign account is suspended	OPE	P	U	I	PU	PI	UI	PUI

Table 7: Plan of emails to provide a stimulus similar to the real world. The table presents the email type, the number of emails, and the source of the emails.

Email type	# of emails	Source
Download request	25	Previous research (Sawyer et al., 2015)
Upload request	25	Previous research (Sawyer et al., 2015)
Emails with link	45	Knowbe4 for phishing email. Personal emails for spam, email marketing, etc.
Emails with no response needed	5	Personal emails or makeup emails

In the final phase, participants completed a post-survey consisting of eight open-text questions aimed at capturing their motivations for engaging with phishing emails. For each phishing email template previously evaluated, participants were presented with the corresponding image and asked the question: "This is an image of a phishing email. During the survey, you [action executed]. Why?" The post-survey provided an opportunity to gather participants' perspectives and insights in their own words regarding their reasons for engaging with phishing emails.

Analysis technique

Our goal was to identify how the PEMO practices would impact the phishing engagement level when compared to the original phishing emails, using age, total duration, and gender as a controller. The engagement with regular emails was not the object of this research.

We collected the age group of participants (20 to 30 years, 31 to 40 years, 41 to 50 years, and 51 to 60 years), the gender (female, male, and others), and the total duration in seconds that each participant spent on the survey. In addition, we collected the engagement level ([marked as phishing], [deleted, marked as spam or ignored], [replied or forwarded], [clicked]) with each of the eight phishing emails the participants were exposed to (one for each PEMO Conditions (OPE, P, U, I, PU, PI, UI, PUI)), and the motive why they decided to engage in that way with each of the eight phishing emails.

First, we analyzed which PEMO Conditions had statistically significant effects on engagements ([marked as phishing], [deleted, marked as spam, or ignored], [replied or forwarded], [clicked]). We used a repeated measures analysis of covariance (MANCOVA) to examine if the application of the PEMO conditions (independent variables) were significant for each phishing engagement level (dependent variables) while controlling per age group, gender, and duration (covariate). We chose to work with MANCOVA because age, gender,

and duration were not the main focus of our analysis, however, those factors could have an effect on the relationship between the independent and dependent variables. The use of covariate allowed the reduction of the error variance, thus increasing the change to better calculate the F value and reject the null hypothesis. In addition, we eliminated duration as a confounding variable that was not manipulated.

Figure 5 presents the relationship between independent variables, covariates, and dependent variables. The use of covariate allowed the reduction of the error variance, thus increasing the change to better calculate the F value and reject the null hypothesis. In addition, we eliminated total duration as a confounding variable that was not manipulated.

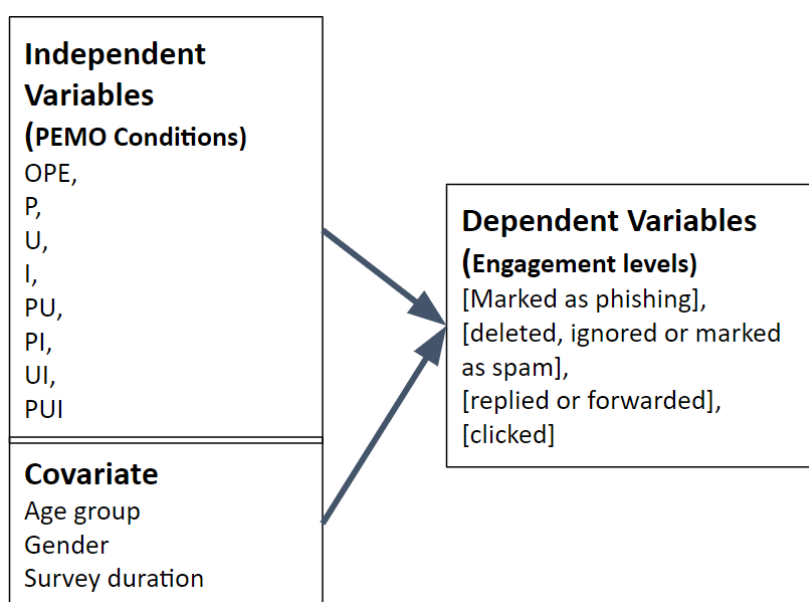


Figure 5: Relationship between variables included in the MANCOVA analysis.

Then, for each engagement level with significant effects, we compared the relevant conditions to the Original Phishing Emails (OPE) to discover the level of impact. For the significant results of the MANCOVA, we plotted a whisker plot for further analysis of the impact compared to the OPE. We analyzed first the higher order interaction (PUI) to predict the effect of the PEMO conditions acting together. The lower-order interactions were just

analyzed for the engagement levels when the higher-order interactions didn't reach a significant effect.

Following, for the most relevant significant impact, we proceeded with further analysis to understand the motives for the behavior. The categorization of participants was performed based on the level of risk of engagement, following the methodology outlined by (Gordon et al. 2019). In their study, (Gordon et al. 2019) adopted a participant grouping approach, classifying them into two categories: offenders and non-offenders, with a threshold engagement rate of 25% (click) as the distinguishing factor. However, it's important to note that (Gordon et al. 2019) did not consider the categories of replied and forwarded engagements in their analysis. Notably, both clicked, replied or forwarded engagements are potential pathways to successful phishing attacks. In our study, we expanded upon this classification approach by incorporating [clicked], [replied, or forwarded] engagements to delineate the offender category. Specifically, participants were labeled as offenders if they engaged with 2 or more phishing emails through [clicked], [replied or forwarded] actions. Conversely, participants were categorized as non-offenders if their engagement encompassed no more than 1 instance of [clicked], [replied or forwarded] actions. Figure 6 presents a summary of the classification of participants.

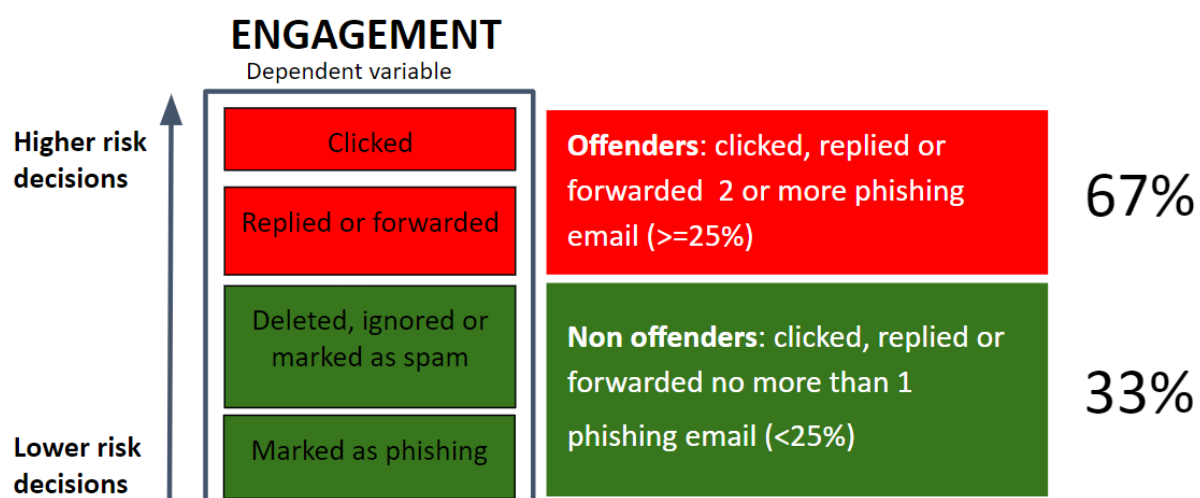


Figure 6: Classification of participants in offenders and non-offenders according to the number of clicked, replied or forwarded engagement levels.

Moving on, we identified questions that needed further analysis about the participants' behavior. For example, as we discovered that UI had the most significant impact on reducing the [marked as phishing] engagement, we proceeded with a question to understand “Why the UI condition significantly reduced the [Marked as Phishing] engagement level?”.

Then, we compared the OPE with the PEMO condition being analyzed and identified the engagement levels affected by offenders and non-offenders. For example, we compared the rates for each engagement level between OPE and UI, creating two bar charts, one for the offenders and another one for the non-offenders. This helped to understand the movement of engagement, as participants [deleted, ignored, or marked as spam] instead of recognizing phishing emails.

Following, a two-step thematic analysis was conducted, where we grouped responses that shared the same or similar words or phrases, providing evidence for the assumptions inferred. It is important to note that we excluded 3 participants from our thematic analysis because the answers didn't provide any relevant information. In the first step of our thematic analysis, the data was manually analyzed by carefully reading each response to identify common themes, patterns, and recurring ideas. Furthermore, we utilized ChatGPT, an Artificial Intelligence (AI) language model developed by OpenAI, which has been trained on a vast amount of text data. We engaged with ChatGPT by providing instructions and queries related to the post-survey data, and it generated responses based on its training and understanding of the text prompts. We engaged with the ChatGPT explaining what the research was about. For each piece of data that we asked it to analyze, we explained what the participant classification (offenders or non-offenders) was, the PEMO condition applied, and the engagement that participants answered. We asked it to provide a thematic analysis to identify common themes, patterns, and recurring ideas. We also asked for some citations as evidence of the analysis. Finally, we compared our manual analysis with the AI analysis.

These generated responses served as supplementary information in our analysis, enhancing our insights and perspectives. However, it is important to note that they were not considered the sole basis for drawing conclusions. We understand that the use of an AI model, such as ChatGPT, to provide qualitative analysis has some limits. While ChatGPT can provide valuable insights and support, it is important to exercise caution due to the model's training data and potential biases. To mitigate those limitations, we used various techniques to analyze the responses and gain insights, including both manual analysis and support from ChatGPT.

Finally, based on the evidence provided for the analysis process, we suggested areas of training that each group of participants needed to focus on. We analyzed the experiment to understand the PEMO conditions that most negatively impacted the group. Then, we identified the cause of the behavior by looking at the post-survey. Following, we provided suggestions for the PEMO practices that the group should be trained to be able to reduce the risk when in contact with the PEMO conditions previously identified.

Keypoints

- We recruited 400 participants for our study using Prolific, a research participant-finding website known for its reliability and diverse user base. Our inclusion criteria involved selecting individuals between the ages of 20 and 60 who currently reside in the United States. 399 participants were included in the analysis.
- Participants went through three phases: a pre-survey, an experiment, and a post-survey. In the pre-survey phase, we gathered basic demographic information. In the experiment, each participant was presented with 100 email images to review, consisting of 92 regular email images, those that don't represent harm, and 8 phishing emails. We collected information about how they engaged with each phishing email. In the final phase, participants completed a post-survey consisting of eight open-text questions aimed at capturing their motivations for engaging with phishing emails.

- Our goal was to identify how the PEMO framework practices would impact the phishing engagement level when compared to the original phishing emails, using age, total duration, and gender as a controller.

CHAPTER 5: RESULTS AND DISCUSSION

In this chapter, we intend to explain the research results. The remaining sections are organized as follows. Section 'Participants information' (13.1) introduces demographic information about the participants. Then, section 'Results' (13.2) presents the data analysis including the pre-survey, experiment, and post-survey. Following, section 'Discussion' (13.3) explains what we learned from the results. Finally, the Section 'Keypoints' introduces a summary of the chapter (13.4).

Participants information

This research includes 399 participants who finished our survey. Among them, 54% identified as male, 45% identified as female, and 1% preferred not to disclose their gender. Figure 7 presents information related to gender. In terms of ethnicity, introduced in Figure 8, the participant distribution was as follows: 72% identified as white, 9.5% as black, 6% as Asian, and 12.5% as other. Regarding the age, presented in Figure 9, 36% of participants fell within the 20-30 age range, 40% were between 31 and 40 years old, 17% were between 41 and 50 years old, and 7% were between 51 and 60 years old. This age range was important for our goal to survey participants who had previous experience in a work environment.

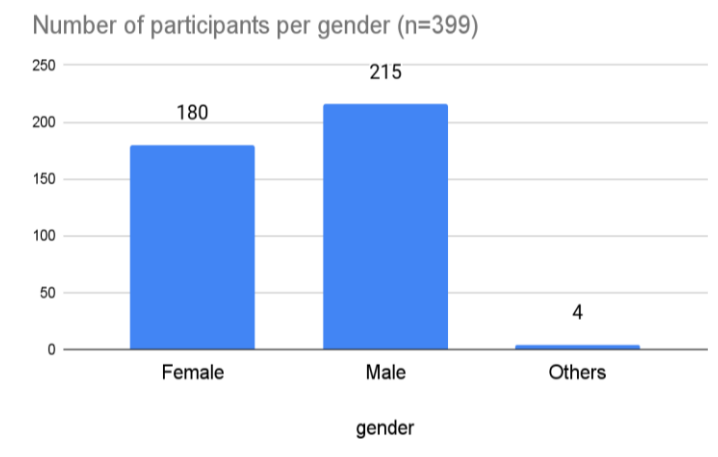


Figure 7: Participants per gender

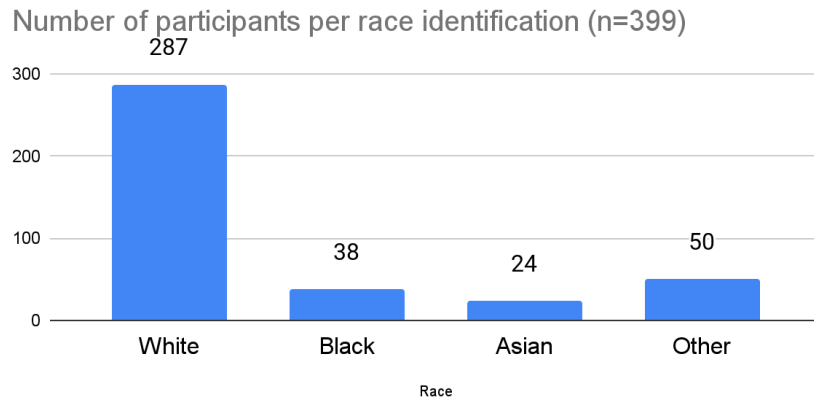


Figure 8: Participants per race identification

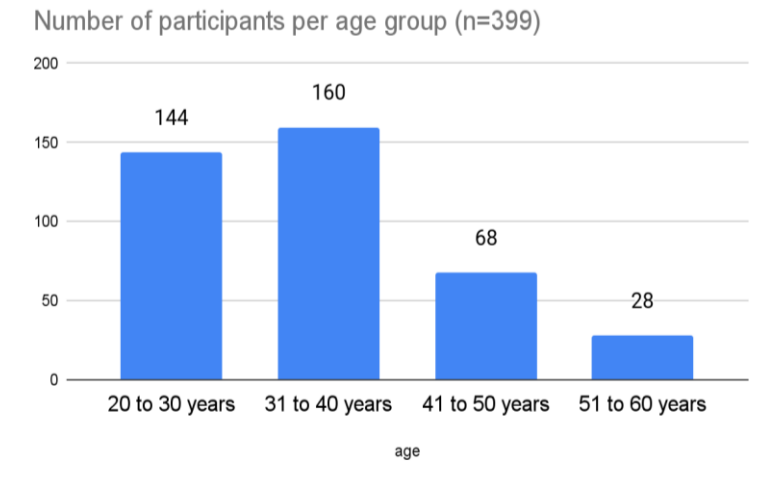


Figure 9: Participants per age group

67 % of participants were classified as offenders, those who clicked, replied, or forwarded 2 or more phishing emails ($\geq 25\%$), and 33% were classified as non-offenders, those who clicked, replied, or forwarded no more than 1 phishing email ($< 25\%$), as introduced in Figure 10.

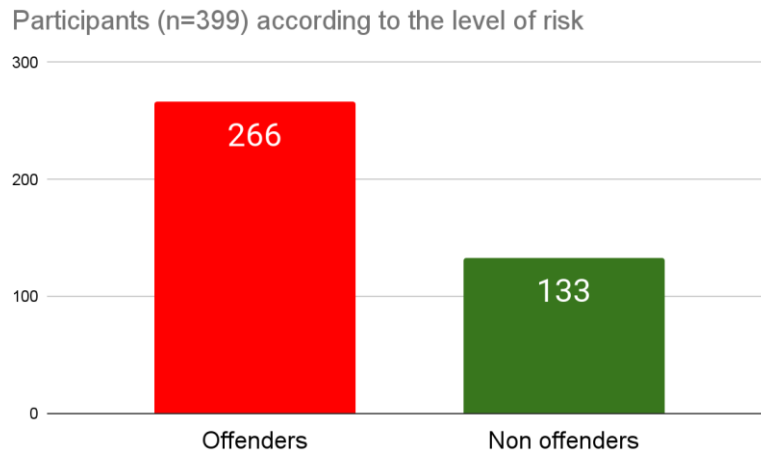


Figure 10: Participants per level of risk

We had 114 participants (28.6%) who didn't click on any phishing email received, whereas 4 participants (1%) were able to identify all the phishing emails received and engaged with them as [marked as phishing]. On the other hand, we had 13 participants (3.2%) who clicked on all the phishing emails they received.

The average time to complete the survey was 29.01 minutes, with the average email engagement time of 17.41 sec.

Results

A repeated measures MANCOVA was performed to examine whether the engagement level ([replied or forwarded], [clicked]) differed between the application of PEMO conditions (OPE, P, U, I, PU, PI, UI, PUI) while controlling for age group, gender, and total duration spent on the survey, and using the original phishing emails (OPE) as a control group.

A Univariate within-subject test score using Greenhouse-Geisser correction determined that Persuasion + Usability + Influence (PUI) proved to be statistically significant for [deleted, ignored or marked as spam] ($F(1)=5.378$, $p=0.021$, partial $\eta^2 = 0.013$), in addition to [marked as phishing] ($F(1)=7.008$, $p=0.008$, partial $\eta^2 = 0.017$), as presented in Table 8.

Hence, we refuted our null hypothesis and confirmed our H1 - PEMO will impact phishing engagement when compared to the original phishing emails.

Table 8: Univariate Tests for Persuasion + Usability + Influence (PUI). The significant effects are highlighted in gray.

Univariate Tests										
Source		Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared	Noncent. Parameter	Observed Power ^a	
P * U * I	Clicked	Greenhouse-Geisser	0.050	1.000	0.050	0.328	0.567	0.001	0.328	0.088
	Replied or forwarded	Greenhouse-Geisser	0.011	1.000	0.011	0.203	0.653	0.001	0.203	0.073
	Deleted, ignored, or marked as spam	Greenhouse-Geisser	0.927	1.000	0.927	5.378	0.021	0.013	5.378	0.638
	Marked as phishing	Greenhouse-Geisser	0.715	1.000	0.715	7.008	0.008	0.017	7.008	0.752

The higher-order interactions (PUI, PU, PI, UI) weren't significant for [clicked], [replied or forwarded] engagements. Therefore, we proceeded to analyze the lower interaction for those specific types of engagements. A Univariate within-subject test score using Greenhouse-Geisser correction determined that Persuasion (P) proved to be significant for [clicked] ($F(1.00)=19.946$, $p=0.000$, Partial ETA Squared = 0.048) and for [replied or forwarded] ($F(1.00)=5.156$, $p=0.024$, Partial ETA Squared = 0.013), as presented in Table 9.

Table 9: Univariate Tests for Persuasion (P). The significant effects are highlighted in gray.

Univariate Tests										
Source		Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared	Noncent. Parameter	Observed Power ^a	
P	Clicked	Greenhouse-Geisser	3.204	1.000	3.204	19.946	0.000	0.048	19.946	0.994
	Replied or Forwarded	Greenhouse-Geisser	0.406	1.000	0.406	5.156	0.024	0.013	5.156	0.620
	Deleted, ignored, or marked as spam	Greenhouse-Geisser	1.721	1.000	1.721	7.824	0.005	0.019	7.824	0.797
	Marked as phishing	Greenhouse-Geisser	0.025	1.000	0.025	0.177	0.674	0.000	0.177	0.070

A Univariate within-subject test score using Greenhouse-Geisser correction determined that Usability (U) proved to have a significant effect on [deleted, ignored or marked as spam] ($F(1.00)=9.938$, $p=0.002$, Partial ETA Squared = 0.025), in addition to [marked as

phishing] engagements ($F(1.00)=7.959$, $p=0.005$, Partial ETA Squared = 0.020), as presented in Table 10. All those effects were further analyzed with the higher-order interactions.

Table 10: Univariate Tests for Usability (U). The significant effects are highlighted in gray.

Univariate Tests										
Source			Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared	Noncent. Parameter	Observed Power ^a
U	Clicked	Greenhouse-Geisser	0.002	1.000	0.002	0.012	0.912	0.000	0.012	0.051
	Replied or Forwarded	Greenhouse-Geisser	0.276	1.000	0.276	3.593	0.059	0.009	3.593	0.472
	Deleted, ignored, or marked as spam	Greenhouse-Geisser	2.163	1.000	2.163	9.938	0.002	0.025	9.938	0.882
	Marked as phishing	Greenhouse-Geisser	0.974	1.000	0.974	7.959	0.005	0.020	7.959	0.804

Our results present a small Partial Eta Squared, that could imply that the statistically significant effects might not have substantial practical significance in terms of explaining the variability in your dependent variables. However, our results are still significant since a slight improvement in detecting phishing emails could still lead to substantial security enhancements in an organizational setting. In addition, a small effect size can still be reliable and valid if using robust methods. Our study design minimizes potential biases and enhances the internal validity of your results. Moreover, even a small effect size can provide valuable insights that refine or extend existing theories.

Table 11 presents the results of the engagement rate for each PEMO condition. P yielded a significant effect on [Clicked], [Replied or Forwarded], and [Deleted, Ignored or Marked as Spam] while U and PUI yielded significant effect on [Deleted, Ignored or Marked as Spam] and [Marked as Phishing]. PU, PI, UI, and I did not yield significant effects at any engagement level. We had an average of 30% for clicked, 9% for replied or forwarded, 40% for deleted, ignored, or marked as spam, and 23% for marked as phishing. Even though the effects of U (34%), I (33%), and UI (32%) were not statistically significant, it is important to notice that there is a slight difference related to OPE (35%).

Table 11: Engagement rate for each PEMO condition. Highlighted are the statistically significant effects for each engagement level.

PEMO Condition	Clicked	Replied or Forwarded	Deleted, Ignored, or Marked as spam	Marked as phishing
AVERAGE	30%	9%	40%	23%
OPE	35%	10%	33%	22%
P	26%*	14%*	36%*	25%
U	34%	6%	41%*	20%*
I	33%	7%	36%	25%
PU	25%	6%	51%	19%
PI	21%	18%	35%	27%
UI	32%	7%	44%	18%
PUI	27%	9%	46%*	18%*

P, U, and PUI conditions were the focus of further analysis since they had significant effects on engagement levels. We analyzed first the higher order interaction (PUI) to predict the effect of the PEMO conditions acting together. The lower order interactions (P, U) were just analyzed for the engagement levels when the higher order interactions didn't reach a significant effect.

Analysis of the [Marked as Phishing] engagement level

We started analyzing the higher-order interaction (PUI) for the [Marked as Phishing] engagement level. Figure 11 and Figure 12 present the whisker plots for [Marked as Phishing], adjusted for the interaction of the covariates age group, gender, and survey duration. In comparison to the original phishing email, P, I, and PI had a slight increase in [Marked as Phishing] engagement level. On the other hand, U showed a slight decrease in [Marked as Phishing] engagement. While Influence I increased the [Marked as Phishing] engagement, UI reduced it, slightly surpassing the effectiveness of PUI, as well as PU. Hence,

our second hypothesis was negative. H2 - [PUI] will have the most significant negative impact over [marked as phishing] engagement when compared to the original phishing emails. However, our sixth hypothesis was positive since PEMO reduced the ability of participants to detect and report phishing emails. H6 - PEMO practices will increase the level of decision risks.

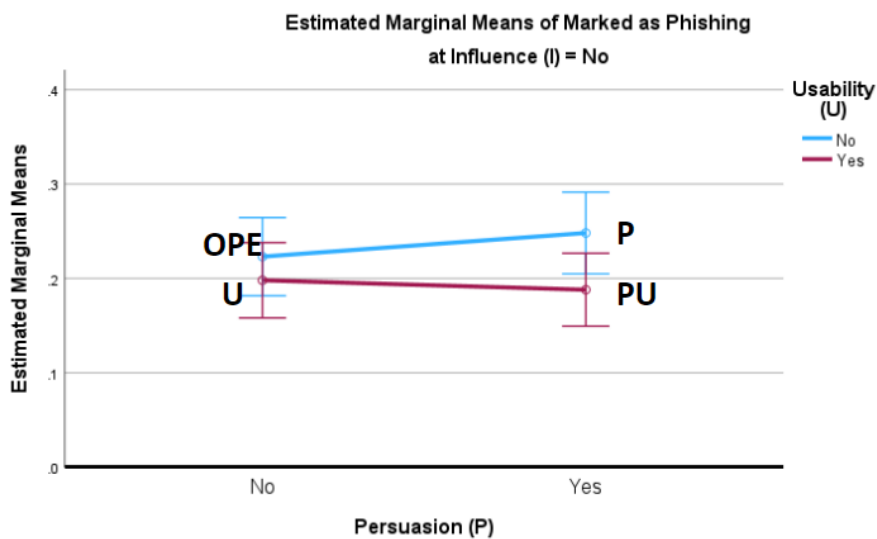


Figure 11: Whisker Plot for Marked as phishing engagement level including P, U, PU, and OPE conditions. Covariates appearing in the model are evaluated at the following values: AGE_GROUP = .94, GENDER = .55, DURATION = 1741.06. Error bars: +/- 2 SE

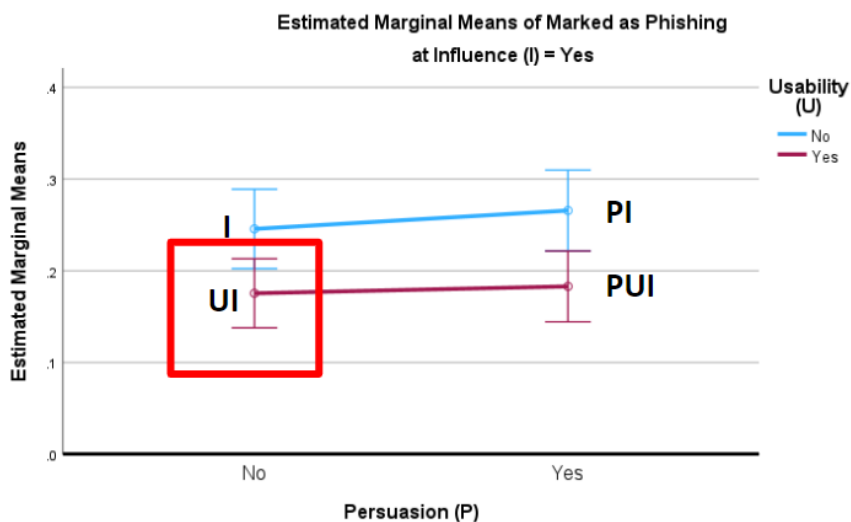


Figure 12: Whisker Plot for Marked as phishing engagement level including I, PI, UI, and PUI conditions. The UI condition is highlighted because it had the most negative impact in marked as phishing. Covariates appearing in the model are evaluated at the following values: AGE_GROUP = .94, GENDER = .55, DURATION = 1741.06. Error bars: +/- 2 SE

To understand why the UI condition significantly reduced the [Marked as Phishing] engagement level for each group of participants (offenders, who clicked, replied, or forwarded 2 or more phishing emails and non-offenders, who clicked, replied, or forwarded no more than 1 phishing email), we compared the rates of UI for each engagement level with the rates of OPE for each engagement level. Figure 13 presents the rates for each engagement level achieved in the OPE (in red) and UI (in blue) conditions, according to non-offenders. The marked as phishing engagement is highlighted because it showed statistical significance in the previous analysis.

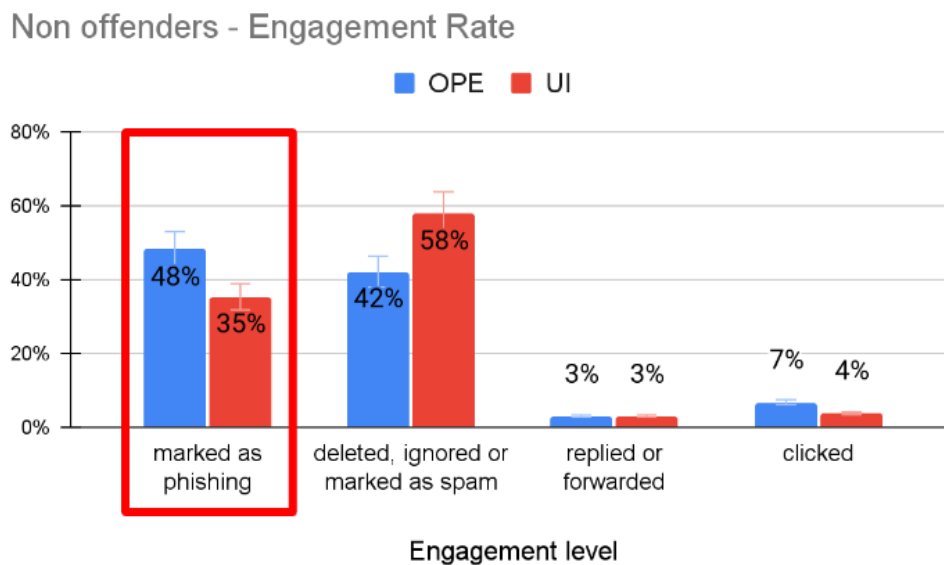


Figure 13: Rates for each engagement level achieved in the OPE and UI conditions, according to non-offenders. The marked as phishing engagement is highlighted because it showed statistical significance in the previous analysis.

Results showed that non-offenders in contact with UI condition presented an observed moderate reduction in the [marked as phishing] and [clicked] engagements. On the other hand, they presented an observed moderate increase in the [Deleted, Ignored, or Marked as Spam] engagements. We identified that the non-offenders reduced the [Marked as Phishing] engagement because they increased the [Deleted, Ignored, or Marked as Spam] engagement levels. In the post-survey phase where we collected the motives for the engagement with phishing, non-offenders reported they were unsure if the email was phishing. For example, participant 20 described “I didn’t recognize the company and figured it was fake

when I saw it was regarding a 'bonus list' but I wasn't sure and just in case I needed the service in the future I didn't mark it as spam so I would still be able to see future emails from the company". In addition, some participants confused the phishing with spam. For example, participant 400 mentioned "I recognized it as a promotion from an outside organization that was not relevant to my job; therefore, I marked it as spam. This allows me to remove the message". Even though the non-offenders were unsure if the email was a phishing attempt, they lacked interest in clicking on it. For example, Participant 111 mentioned that "I didn't trust it but didn't know it was phishing. Just didn't seem important".

In a different approach, offenders in contact with UI condition presented an observed moderate reduction in the [replied or forwarded] and [clicked] engagements. In addition, they presented an observed moderate increase in the [Deleted, Ignored, or Marked as Spam] engagements. However, the [marked as phishing] engagement had no observed changes. Figure 14 presents the rates for each engagement level achieved in the OPE (in blue) and UI (in red) conditions, according to offenders. The marked as phishing engagement is highlighted because it showed statistical significance in the previous analysis.

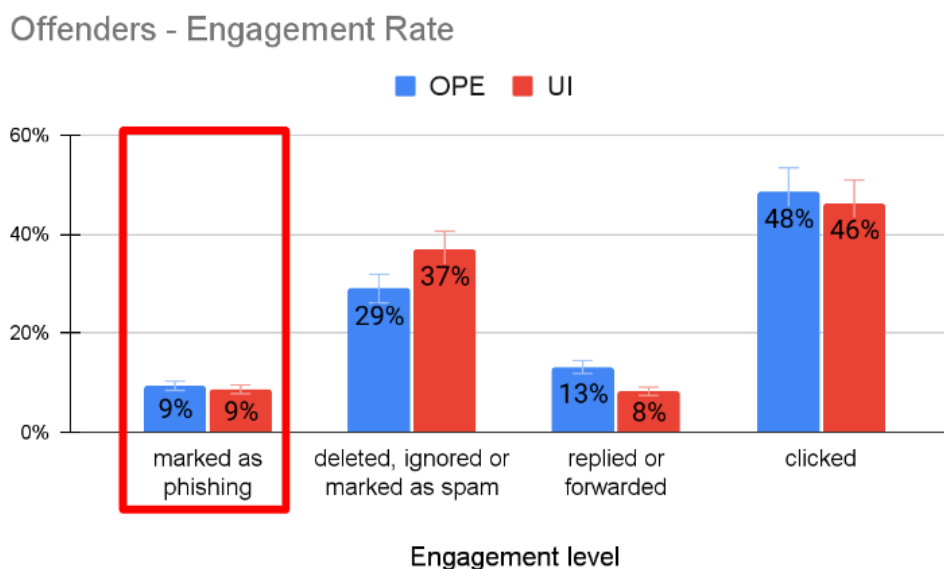


Figure 14: Rates for each engagement level achieved in the Original Phishing Email (OPE) and Usability + Influence(UI) conditions, according to offenders. The marked as phishing engagement is highlighted because it showed statistical significance in the previous analysis.

Even though offenders didn't suffer impact from UI in the [marked as phishing] engagement level, they still presented a high clicked rate. Hence, we decided to analyze the post-survey to better understand the risky behavior. 46% of offenders were still deceived by the UI condition. Offenders thought the phishing email was a regular email due to perceived legitimacy and trust in the sender. For example, participant 27 reported that "The email looked like a typical email that you would receive from UPS". Offenders specifically mentioned practices that enhanced the visual design, including elements such as professionalism, copyright, footer, and logo/branding. For example, participant 84 mentioned "I thought this was an email from our own department. It has our logo and email tag at the top". Offenders thought the phishing email was urgent and important because of the context and the possibility of loss. As an example, participant 68 reported "It baited me with 'protect your account' line."

Analysis of the [Deleted, Ignored, or Marked as Spam] engagement levels.

Following the analysis, we proceeded to look at the higher-order interaction (PUI) for the [Deleted, Ignored, or Marked as Spam] engagement levels. Figure 15 and Figure 16 present the Whisker Plot for [Deleted, Ignored, or Marked as Spam] engagement levels, adjusted for the interaction of the covariates (age group, gender, and survey duration). Compared to the Original phishing emails, P, I, and PI demonstrated a marginal growth in [Deleted, Ignored, or Marked as Spam] engagements. In addition, U, UI, or PUI exhibited a moderate enhancement in terms of increasing the frequency of [Deleted, Ignored, or Marked as Spam] engagements. Finally, PU exhibited a statistically significant positive effect in [Deleted, Ignored, or Marked as Spam] engagements. Hence, our third hypothesis was negative. H3 - [I] will have the most significant negative impact over [deleted, ignored or marked as spam] engagements when compared to the original phishing emails.

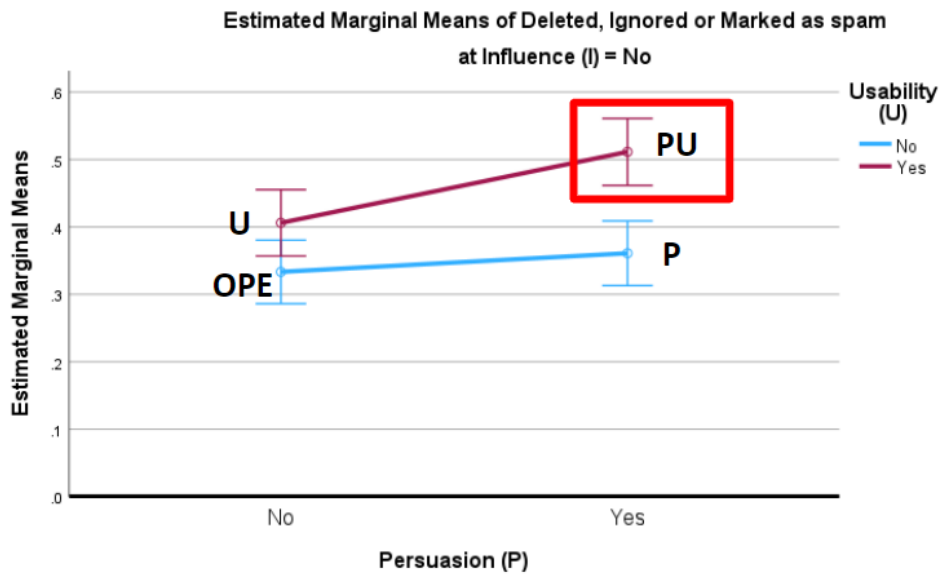


Figure 15: Whisker Plot for [Deleted, Ignored or Marked as Spam] engagement levels including P, U, PU and OPE conditions. Covariates appearing in the model are evaluated at the following values: AGE_GROUP = .94, GENDER = .55, DURATION = 1741.06. Error bars: +/- 2 SE

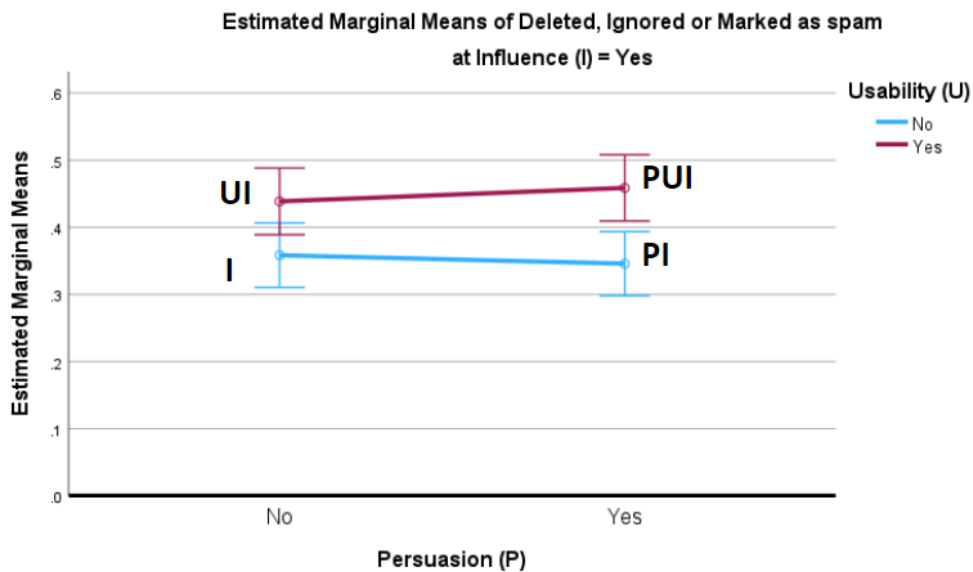


Figure 16: Whisker Plot for [Deleted, Ignored, or Marked as Spam] engagement levels including I, PI, UI, and PUI conditions. The UI condition is highlighted because it had the most negative impact in marked as phishing. Covariates appearing in the model are evaluated at the following values: AGE_GROUP = .94, GENDER = .55, DURATION = 1741.06. Error bars: +/- 2 SE

To understand why the PU condition significantly increased [Deleted, Ignored, or Marked as Spam] engagement level for each group of participants (offenders and non-offenders), we compared the rates of PU for each engagement level with the rates of OPE for each engagement level. Figure 17 presents the rates for each engagement level achieved in the OPE and PU conditions, according to non-offenders, and Figure 18 presents results for

offenders. The [deleted, ignored, or marked as spam] engagement level is highlighted because it showed statistical significance in the previous analysis.

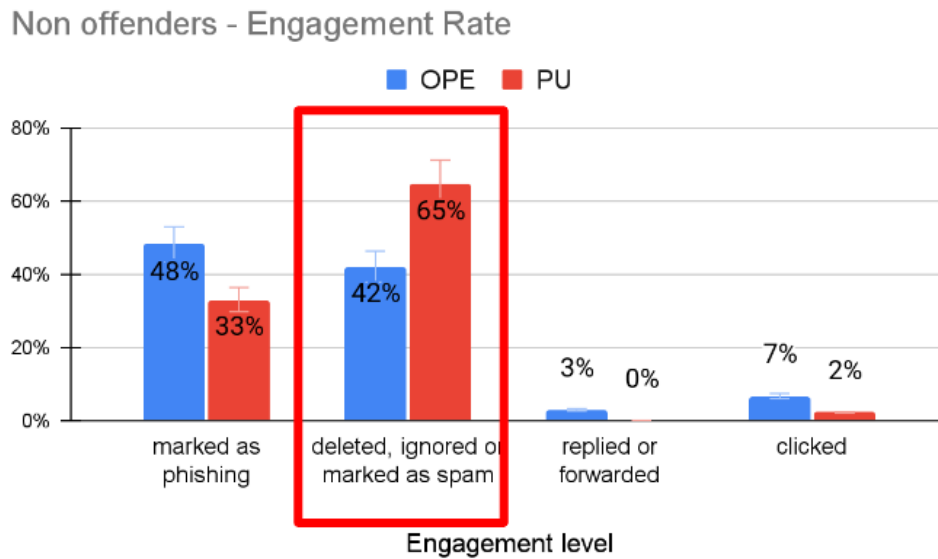


Figure 17: Rates for each engagement level achieved in the OPE and PU conditions, for non-offenders. The deleted, ignored, or marked as spam engagement is highlighted because it showed statistical significance in the previous analysis.

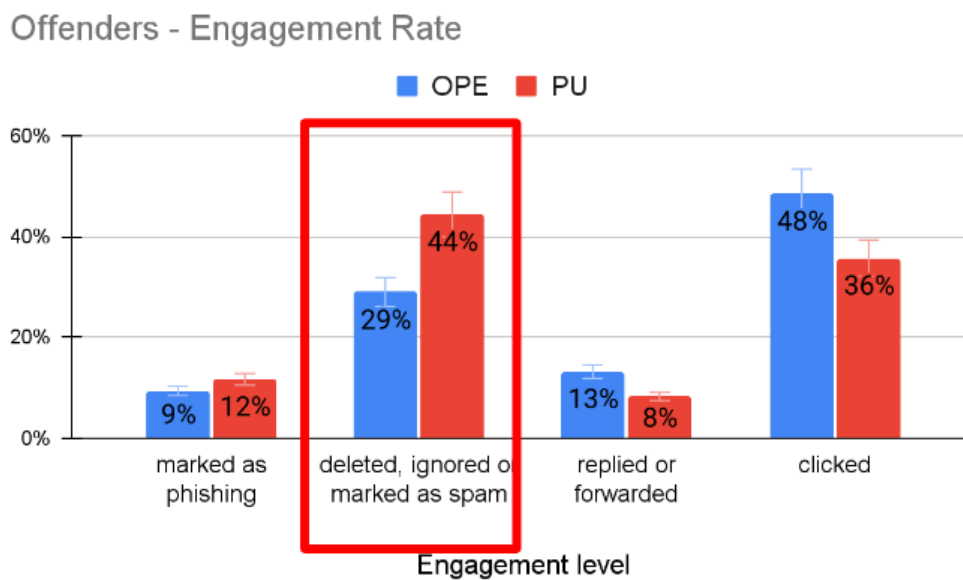


Figure 18: Rates for each engagement level achieved in the OPE and PU conditions, for offenders. The deleted, ignored, or marked as spam engagement is highlighted because it showed statistical significance in the previous analysis.

Results showed that non-offenders in contact with the PU condition had an observed significant increase in the [deleted, ignored, or marked as spam] engagement level.

On the other hand, they had an observed significant reduction in the [marked as phishing], and a slight reduction in the [replied or forwarded], and [clicked] engagements levels. Just as important, offenders in contact with PU condition had an observed significant increase in [deleted, ignored, or marked as spam] and a slight increase in the [marked as phishing] engagement levels. In contrast, offenders had an observed moderate reduction in the [replied or forwarded] and [clicked] engagement levels.

The post-survey analysis showed that offenders and non-offenders were unsure if the email was phishing. For example, Participant 27 described “I wasn't sure if this was a phishing email or not. It looks somewhat professional, but I didn't want to click on any links because I wasn't sure”. In addition, some participants confused the phishing email with spam. Specifically, Participant 35 described “It seemed like it was spam to me, and the link seemed like it may lead to a spam area”. Evidence also pointed out that suspicion or lack of interest in advertisements impacted participants' decisions. As an example, Participant 231 explained “It is irrelevant to me”.

Analysis of the [Clicked] vs. [Replied or Forwarded] engagement levels.

Following the analysis, we proceeded to look at the lower order interaction P for the [Clicked] and [Replied or Forwarded] engagement levels, since the higher order interaction PUI didn't present a statistically significant effect on those engagement levels. Figure 19 presents the Whisker Plot for [Clicked] engagement level and Figure 20 presents the Whisker Plot for [Replied or Forwarded] engagement levels, both adjusted for the interaction of the covariates age group, gender, and survey duration. P revealed a significant reduction in [clicked], suggesting its effectiveness in mitigating user susceptibility to deceptive attempts. However, it is important to note that P demonstrated success in increasing [replied or forwarded] engagement which also poses a high level of risk. The phisher can exploit this continued interaction, potentially leading to a successful phishing attack on the email recipient. Hence, our fourth and fifth hypothesis were negative. H4 - [PI] will have the most significant

positive impact over the [replied or forwarded] engagements when compared to the original phishing emails and H5 - [PU] will have the most significant positive impact over [clicked] engagement when compared to the original phishing emails. However, we confirmed that our sixth hypothesis was positive since P demonstrated success in increasing [replied or forwarded] engagement.

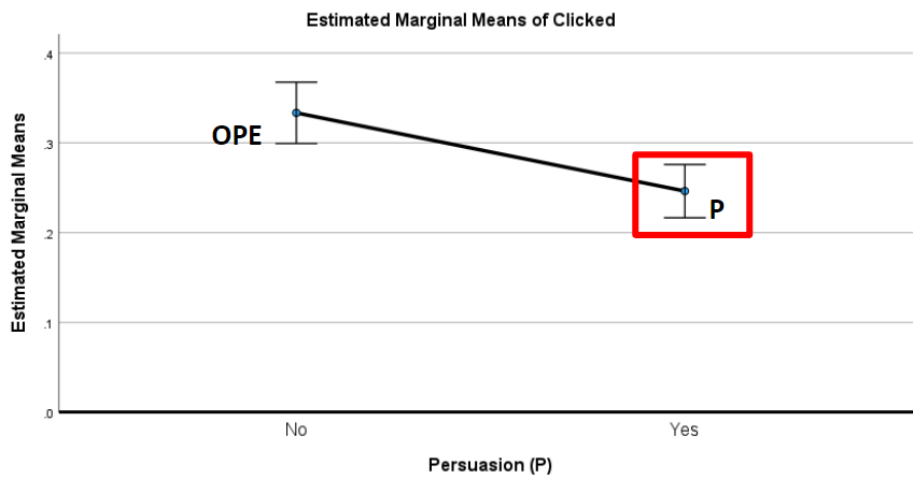


Figure 19: Whisker Plot for [Clicked] engagement level including P condition. Highlighted is the P condition. Covariates appearing in the model are evaluated at the following values: AGE_GROUP = .94, GENDER = .55, DURATION = 1741.06. Error bars: +/- 2 SE

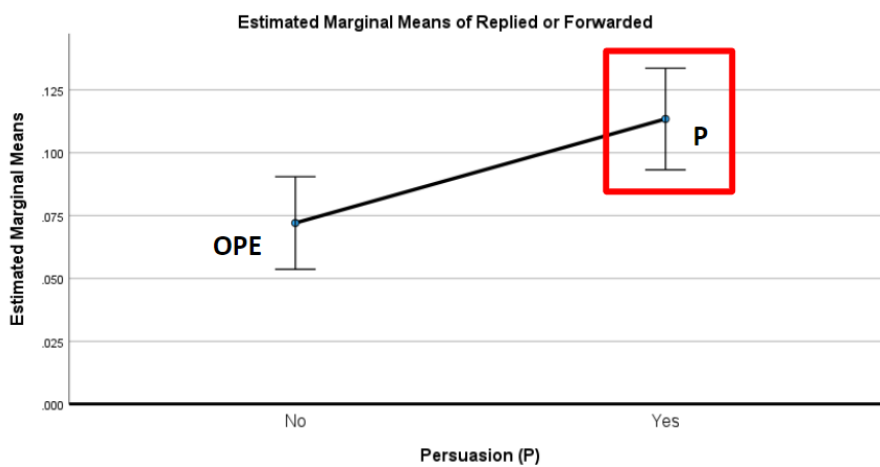


Figure 20: Whisker Plot for [Replied or Forwarded] engagement level including P condition. Highlighted is the P condition. Covariates appearing in the model are evaluated at the following values: AGE_GROUP = .94, GENDER = .55, DURATION = 1741.06. Error bars: +/- 2 SE

To understand why the P condition significantly increased the [Replied or Forwarded] engagement levels and significantly reduced the [Clicked] engagement level for each group of participants (offenders and non-offenders), we compared the rates of P for each engagement level with the rates of OPE for each engagement level. Figure 21 presents the rates for each engagement level achieved in the OPE and P conditions, according to non-offenders, and Figure 22 presents results for offenders. The [replied or forwarded] engagement level is highlighted because it showed statistical significance in the previous analysis.

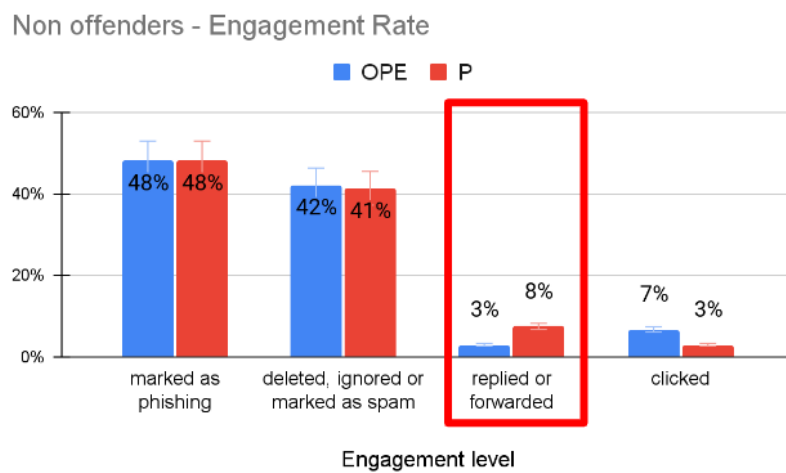


Figure 21: Rates for engagement level achieved in the Original Phishing Email (OPE) and Persuasion (P), according to non-offenders.

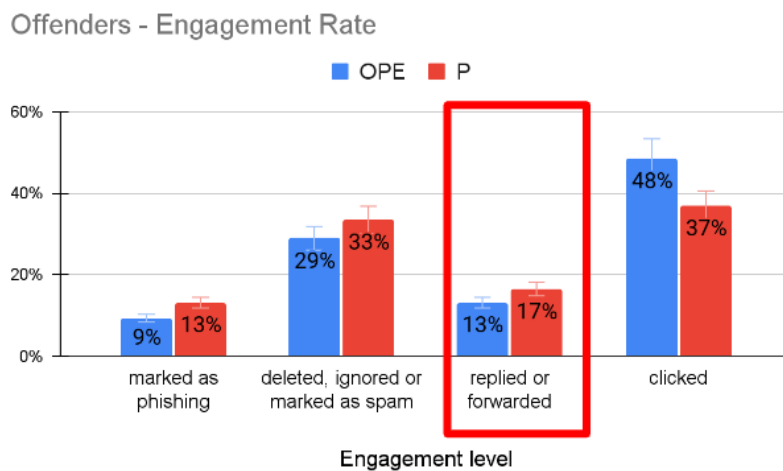


Figure 22: Rates for engagement level achieved in the Original Phishing Email (OPE) and Persuasion (P), according to offenders.

Results showed that non-offenders in contact with P had an observed moderate increase in the [replied or forwarded] engagement levels. On the other hand, they had an observed moderate reduction in the [clicked] engagement level. Just as important, offenders in contact with P had an observed moderate increase in the [marked as phishing], observed a slight increase in the [deleted, ignored, or marked as spam], and observed moderate increase [replied or forwarded] engagements levels. In contrast, offenders had an observed moderate reduction in the [clicked] engagement level.

The post-survey analysis showed that both offenders and non-offenders were interested in the context and wanted more information. For example, Participant 89 stated “I was interested in what was offered and wanted more information” and Participant 111 said “I thought she wanted to meet for coffee so I was gonna ask a time”. In addition, offenders and non-offenders thought the phishing email was a regular email due to perceived legitimacy. The Participant 75 stated that “Couldn't really tell if these are phishing or not. Sometimes they are so good in detail” while the Participant 327 mentioned “I thought it was an actual UPS driver sending a message. I have had UPS drivers send a message through the UPS app and it looked legit”.

Discussion

In this section, we delve into the results pertaining to non-offenders, individuals who engaged as clicked, replied, or forwarded with only one of the eight phishing emails they received during the study. We also discuss the results for offenders, individuals who exhibited a higher level of risk decisions, by clicking, replying to, or forwarding two or more of the eight phishing emails they received during the study. It is important to notice that non-offenders and offenders are categorized in this study according to their actions in the experiment. No broader characterization is implied here.

It's evident that non-offenders exhibit a heightened awareness of common phishing red flags, such as unusual email addresses and spelling errors. However, these participants would greatly benefit from targeted training to enhance their ability to detect phishing attempts applying UI and PU practices. The study also unveils the noteworthy influence of Usability practices like visual design elements, including brand logos and footers, on the perceived legitimacy and trustworthiness of phishing email communications. Simultaneously, the application of the Influence practice serves to amplify the perceived importance of these messages among non-offenders.

Interestingly, non-offenders often maintained a sense of suspicion or uncertainty regarding whether an email constituted phishing or spam, an unsolicited message sent to recipients for the purpose of commercial advertising. Consequently, they erred on the side of caution by engaging with these emails in ways that minimize risk - typically by opting to engage as deleted, ignored, or marked as spam. The lack of personal interest in the content of these emails played a pivotal role in shaping their decision-making process. It is important to note though that confusing a phishing email with spam can lead to a high-level of risk decision. As the lack of interest in the content was the motive to minimize risk, it is an open question if the non-offenders would engage differently with a phishing email that he confuses with spam and provides content that attracts his interest.

Based on these findings, we recommend implementing targeted training programs, with a particular emphasis on enhancing the detection of phishing emails that apply usability practices. The rules for usability and common phishing red flags must be reviewed. This approach holds promise in empowering non-offenders to bolster their resilience against phishing attempts, ultimately contributing to improved cybersecurity awareness and practices among this demographic.

We found different findings related to offenders' behavior when dealing with phishing emails applying marketing practices. Notably, offenders displayed a heightened

sense of curiosity coupled with a somewhat lowered sense of caution. This intriguing trait might render them more susceptible to falling victim to phishing attacks, given their propensity to interact with content that could potentially prove harmful. One prominent observation is that offenders appear more inclined to place trust in emails that convincingly mimic legitimate sources. This inclination exposes them to a heightened risk of falling victim to sophisticated phishing tactics that expertly emulate trusted entities.

However, it is clear from the study that offenders would greatly benefit from targeted training aimed at honing their ability to recognize phishing attempts, particularly those employing Persuasion practices. It is important to highlight that Persuasion practices revealed a significant reduction in [clicked], suggesting its effectiveness in mitigating user susceptibility to deceptive attempts. However, demonstrated success in increasing [replied or forwarded] engagement that also poses a high level of risk. These findings underscore the importance of equipping this group with the knowledge and skills necessary to identify and prevent phishing attacks effectively. Participants within this category reported a notably higher level of interest in the phishing emails applying Persuasion practices, resulting in an increased propensity to engage further by replying to or forwarding these messages. Such heightened engagement levels can significantly elevate the risk of successful phishing attacks.

This study discerns notable disparities between offenders and non-offenders. Offenders exhibited heightened curiosity and reduced caution, potentially rendering them more vulnerable to phishing attacks due to their inclination to interact with potentially malicious content and trust seemingly legitimate sources. They necessitated further training, particularly in identifying phishing attempts employing persuasion practices. Conversely, non-offenders demonstrated greater familiarity with typical phishing indicators such as unusual email addresses and misspellings. Nevertheless, they too required training to improve their ability to discern phishing emails using usability practices. Notably, visual design elements, such as branding and footers, appeared to influence their perceptions of legitimacy and trust. Although

non-offenders often approached suspicious emails with skepticism or uncertainty, their engagement typically involved low-risk actions, such as deleted or marked as spam, primarily driven by a lack of interest in the content. These findings emphasize the importance of tailored training and awareness initiatives to mitigate phishing risks among both groups, with offenders benefiting from education on persuasion practices recognition and non-offenders necessitating guidance on identifying phishing attempts via usability practices. Understanding these distinctions is vital for the development of effective cybersecurity strategies.

It is important to highlight that the efficiency of the training proposed on this study was not measured on this research. However, previous research (Castilho Grao, 2023) showed that having previous experience with phishing, like in trainings for example, can impact the decision-making with phishing emails and reduce vulnerability. In addition, users without phishing awareness training are 6 times more likely to click on phishing emails (Carella et al., 2017).

Cybersecurity researchers can gain valuable insights by acknowledging the study's limitations. Specifically, we employed a survey-based approach, which offered cost-effectiveness and accelerated timelines. However, it's worth noting that this study involved participants evaluating 100 emails in a controlled setting, which differs from the typical work environment where professionals manage emails continuously while juggling various tasks. This inability to replicate a naturalistic setting could impact the generalizability of our findings. Future research incorporating phishing simulations within real-world, multitasking email scenarios may yield diverse outcomes and a deeper understanding of phishing behaviors in professional contexts.

Another limitation of our study lies in the inability to achieve a balanced representation of participants in terms of ethnicity. While we successfully ensured demographic symmetry concerning age and gender, a substantial majority of our participants self-identified as white. This potential demographic bias poses challenges when examining

the impact of sender images within the PEMO framework. As illustrated by one participant's comment, "I thought it might be a phishing email, then I thought maybe I was just being racist because the picture looks like a guy from Nigeria. White guilt." The lack of ethnic diversity within our sample raises concerns about the generalizability of our findings. Thus, addressing this ethnicity imbalance would enhance the comprehensiveness and impartiality of our analysis.

Even with the limitations, our findings can help Information Security departments to classify professionals and to provide targeted training for them. As an example, non-offenders can learn about the PEMO usability rules and refresh their knowledge about phishing red flags, common indicators of phishing attempts. This will help them to be able to recognize and report phishing emails applying usability practices. On the other hand, offenders can learn about the PEMO persuasion rules and learn about the phishing red flags. This can help them to recognize and avoid replying to phishing emails applying persuasion practices.

Keypoints

- Gender and duration spent on the survey had no effect when analyzing the impact of PEMO conditions on phishing engagement.
- Non-offenders need training to be able to better identify phishing using UI and PU practices. They kept a low level of risk by engaging as deleted, ignored, or marked as spam. The lack of interest impacted their decision. We suggest focused training on Usability for non-offenders, as this practice is on both conditions that affected this group.
- Offenders need more training to identify phishing using Persuasion practices. Participants reported more interest and increased the replied and forwarded engagement, which can lead to a successful phishing attack.

- P revealed a significant reduction in [clicked], suggesting its effectiveness in mitigating user susceptibility to deceptive attempts. However, it is important to note that P demonstrated success in increasing [replied or forwarded] engagement which also poses a high level of risk.

CHAPTER 6: CONCLUSIONS

Phishing emails are a common cybercrime that companies need to deal with, and its impact recently became even more expensive. Cybersecurity grew into a \$1 trillion problem over five years, with companies of all sizes investing more in security tools (Keller, 2021; Morgan, 2020; Stock, 2020). Consistent with some authors (Downs et al., 2007; Pattinson et al., 2012), we believe that understanding why people fall for phishing attacks is relevant for professionals to face cybersecurity challenges. Consequently, reducing the amount of capital spent on phishing emails' consequences.

This research rests on the assumption that scammers use email marketing practices to enhance their phishing email attacks. Indeed, we analyzed and introduced a literature review on previous research with practices commonly used in email marketing and phishing email. Although these studies were able to identify the most efficient approach of each marketing practice analyzed (persuasion, usability and influence) to impact vulnerability to phishing emails, they were not able to answer if phishers could use marketing practices to be successful in their endeavor. Specifically, they were not able to identify how the application of more than one marketing practice in the same phishing email would impact the phishing email engagement. Moreover, they were not able to provide evidence about what marketing practices have the most significant effect on phishing engagement levels. We decided to change that. We created the Phishing Engagement Marketing Optimization (PEMO) framework, a unique tool based on marketing practices that can be applied in phishing email simulations to help prepare users to better identify phishing using marketing practices. PEMO, as applied in this work, incorporates 3 practices: Persuasion (P), Usability (U), and Influence (I), and includes a guideline with rules to be applied in the process of email creation to simulate the technique of applying marketing practices into phishing emails.

In this work, we also analyzed which PEMO conditions (P, U, I, PU, PI, UI, PUI) have a significant effect on phishing email engagement levels (marked as phishing or deleted,

ignored and marked as spam or replied and forwarded or clicked) in comparison with some original phishing emails. Specifically, we hypothesized which PEMO conditions would have the most effect on each engagement level. The experiment design was a 2 Persuasion (yes, no) x 2 Usability (yes, no), x 2 Influence (yes, no) factorial design, that allowed us to analyze each of the PEMO conditions individually or in combination. 399 participants finished a three-phase study, pre-survey, experiment and post-survey. First, they joined a pre-survey to answer demographic information. Then, they joined an experiment where they engaged with 100 pictures of emails (92 regular emails and 8 phishing emails) and answered how they would engage with the email (marked as phishing or deleted, ignored, and marked as spam or replied and forwarded or clicked). Each of the phishing emails that an individual participant received incorporated practices of one different PEMO condition. Finally, they received a post-survey to answer the motive for the engagement with each of the 8 phishing emails evaluated.

Our results evidenced that non-offenders, individuals who avoided higher-risk decisions and engaged as replied, forwarded, or clicked on just one email, were not able to identify phishing emails applying Usability + Influence (UI) and Persuasion + Usability (PU) practices during the experiment. Indeed, they reported that some usability features like logo, footer and copyright led them to think that the email was legit. Non-offenders kept a low level of risk with UI and PU phishing emails by engaging as deleted, ignored, or marked as spam. The lack of interest impacted their low level of risk decision. However, it is an open question if they would engage in a higher level of risk if they had interest on the content. Based on the findings, we identified that non-offenders need focused training on Usability to be able to better identify phishing applying UI and PU practices.

We also analyzed the offenders, individuals who exhibited a higher level of risk decisions, by clicking, replying to, or forwarding two or more of the eight phishing emails. The results showed that offenders reduced the clicked engagement, suggesting its effectiveness in mitigating user susceptibility to deceptive attempts. However, they increased the replied

and forwarded engagement with phishing applying Persuasion (P) practices, that also poses a high level of risk. They reported more interest and curiosity in P phishing emails. Offenders need more training to identify phishing using Persuasion practices to avoid a successful phishing attack.

This paper provides important contributions, as anti-phishing techniques have little academic advancement (Carella et al., 2017). Through our research, we contributed to the improvement of cybersecurity practices by helping to understand how marketing practices impact phishing email engagements. We provided valuable guidance for organizations, particularly their Information Security departments, with a unique framework (PEMO) and a methodology to incorporate marketing practices in phishing simulations and better train professionals to identify phishing applying marketing practices. In addition, we provided a unique method of analysis that can be replicated to evaluate the effect of practices on phishing engagement that leads to the suggestion of training per group of participants according to the level of risk. Finally, we offered actionable insights to empower individuals to make informed decisions when confronted with phishing attempts.

We here provided a first step towards exploring and preventing the impact of marketing practices in phishing emails. However, this research presents several opportunities for future work. First, our experiment was conducted in the form of a survey, which allowed for cost reduction and expedited timelines. However, it would be valuable to replicate the experiment in a naturalistic environment, such as by sending emails within a work context in a phishing simulation, to explore potential variations in the results. Second, we compared the application of PEMO with real phishing emails, some of which already incorporated elements of PEMO. To further understand the impact of PEMO, future studies could explore the comparison between the application of PEMO practices and the absence of such practices. Third, one intriguing avenue for future research is the exploration of whether a phisher, armed with a deeper understanding of one specific non-offenders interest, could tailor phishing

attempts with content that impacts that non-offenders decisions to engage in a higher level of risk, including replied, forwarded, or clicked engagements. Lastly, future research would benefit from achieving a more balanced representation of participants in terms of ethnicity to provide a more broadly finding.

APPENDIX A:
PHISHING EMAIL IMAGES

Microsoft

Your message couldn't be delivered



Christopher Smith from Microsoft Support support@microsoft.com
para mim ▾

Hello **Jordan Williams**,

I hope you are having a great day. My name is Christopher Smith. I am a customer support specialist at Microsoft. Some months ago, Cog Industries contracted our support service. I am sending this email to help you to be successful using the Microsoft email tools.

When I started to use email tools I had some challenges configuring it, even more, when some messages returned. Then, I have specialized in email tools and today I can assist other people to have an easier path.

I just notice that your last message to director@cogindustries.com couldn't be delivered. I discovered that it happened because your mail program is using out-of-date address information. But don't worry, I am here to help you to solve this problem easily. Following you can check more information about the issue and how to fix it.

Office 365

administrative@cogindustries.com

Action Required

Out-of-date FROM address

How to Fix It

Click [here](#) and update the information requested about your email.

Was this helpful? [Send feedback](#).

Figure: phishing email for Microsoft - email not delivered, manipulating best practices of persuasion (yes), usability (no), influence (no)

Your message couldn't be delivered

Microsoft Support support@microsoft.com

para mim ▾



Your message to director@cogindustries.com couldn't be delivered. Your mail program is using out-of-date address information for administrative@cogindustries.com.

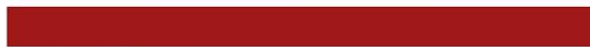
Office 365

administrative@cogindustries.com

2022

Action Required

Recipient



Out-of-date FROM address

How to Fix It

Click on the button above and update the information requested about your email.

[Update email information](#)

Was this helpful? [Send feedback](#)

Microsoft Support Team

support@microsoft.com

1 Microsoft Way, Redmond, Washington 98052-8300

Support line: 1 (425) 882-8080

Copyright © 2022 Microsoft, All rights reserved.

You are receiving this emails because your company has Microsoft support.

Want to change how you receive these emails?

You can [update your preferences](#) or [unsubscribe from this list](#).

Figure: phishing email for Microsoft - email not delivered, manipulating best practices of persuasion (no), usability (yes), influence (no)

Your message couldn't be delivered

Microsoft Support support@microsoft.com
para mim ▾

Your message to director@cogindustries.com couldn't be delivered. Your mail program is using out-of-date address information. Don't let your director lose access to important opportunities.

Office 365

administrative@cogindustries.com

Action Required

Out-of-date FROM address

How to Fix It

Be the first in your company to keep your information updated. Click [here](#) and update the information requested about your email.

Was this helpful? [Send feedback](#).

Figure: phishing email for Microsoft - email not delivered, manipulating best practices of persuasion (no), usability (no), influence (yes)

Your message couldn't be delivered



Christopher Smith from Microsoft Support support@microsoft.com
para mim ▾

inglês > português Traduzir mensagem



Hello **Jordan Williams**,

I hope you are having a great day. My name is Christopher Smith. I am a customer support specialist at Microsoft. Some months ago, Cog Industries contracted our support service. I am sending this email to help you to be successful using the Microsoft email tools.

When I started to use email tools I had some challenges configuring it, even more, when some messages returned. Then, I have specialized in email tools and today I can assist other people to have an easier path.

I just notice that your last message to director@coindustries.com couldn't be delivered. I discovered that it happened because your mail program is using out-of-date address information. But don't worry, I am here to help you to solve this problem easily. Following you can check more information about the issue and how to fix it.

Office 365

administrative@coindustries.com

2022

Action Required

Recipient

Out-of-date FROM address

How to Fix It

Click on the button above and update the information requested about your email.

[Update email information](#)

Was this helpful? [Send feedback](#).



Christopher Smith
Microsoft Support Team
support@microsoft.com
1 Microsoft Way, Redmond, Washington 98052-8300
Support line: 1 (425) 882-8080

Copyright © 2022 Microsoft, All rights reserved.

You are receiving this emails because your company has Microsoft support.

Want to change how you receive these emails?

You can [update your preferences](#) or [unsubscribe from this list](#).

Figure: phishing email for Microsoft - email not delivered, manipulating best practices of persuasion (yes), usability (yes), influence (no)

Your message couldn't be delivered



Christopher Smith from Microsoft Support support@microsoft.com

para mim ▼

Hello **Jordan Williams**,

I hope you are having a great day. My name is Christopher Smith. I am a customer support specialist at Microsoft. Some months ago, Cog Industries contracted our support service. I am sending this email to help you to be successful using the Microsoft email tools.

When I started to use email tools I had some challenges configuring it, even more, when some messages returned. Then, I have specialized in email tools and today I can assist other people to have an easier path.

I just notice that your last message to director@cogindustries.com couldn't be delivered. I discovered that it happened because your mail program is using out-of-date address information. I don't want that your director loses access to important opportunities or you to lose access to your account. So don't worry, I am here to help you to solve this problem easily. Following you can check more information about the issue and how to fix it.

Office 365

administrative@cogindustries.com

Action Required

Out-of-date FROM address

How to Fix It

Be the first in your company to keep your information updated. Click [here](#) and update the information requested about your email.

Was this helpful? [Send feedback](#).

Figure: phishing email for Microsoft - email not delivered, manipulating best practices of persuasion (yes), usability (no), influence (yes)

Your message couldn't be delivered



Microsoft Support support@microsoft.com

para mim ▾

🌐 inglês ▾ > português ▾ Traduzir mensagem



Your message to director@cogindustries.com couldn't be delivered. Your mail program is using out-of-date address information for administrative@cogindustries.com. Don't let your director lose access to important opportunities.

Office 365

administrative@cogindustries.com

2022

Action Required

Recipient



Out-of-date FROM address

How to Fix It

Be the first in your company to keep your information updated. Click on the button above and update the information requested about your email.

[Update email information](#)

Was this helpful? [Send feedback](#)

Microsoft Support Team

support@microsoft.com

1 Microsoft Way, Redmond, Washington 98052-8300

Support line: 1 (425) 882-8080

Copyright © 2022 Microsoft, All rights reserved.

You are receiving this emails because your company has Microsoft support.

Want to change how you receive these emails?

You can [update your preferences](#) or [unsubscribe from this list](#).

Figure: phishing email for Microsoft - email not delivered, manipulating best practices of persuasion (no), usability (yes), influence (yes)

Your message couldn't be delivered

 **Christopher Smith from Microsoft Support** support@microsoft.com
para mim ▾



Hello **Jordan Williams**,

I hope you are having a great day. My name is Christopher Smith. I am a customer support specialist at Microsoft. Some months ago, Cog Industries contracted our support service. I am sending this email to help you to be successful using the Microsoft email tools.

When I started to use email tools I had some challenges configuring it, even more, when some messages returned. Then, I have specialized in email tools and today I can assist other people to have an easier path.

I just notice that your last message to director@coindustries.com couldn't be delivered. I discovered that it happened because your mail program is using out-of-date address information. I don't want that your director loses access to important opportunities or you to lose access to your account. So don't worry, I am here to help you to solve this problem easily. Following you can check more information about the issue and how to fix it.

Office 365

administrative@coindustries.com

2022

Action Required

Recipient



Out-of-date FROM address

How to Fix It

Be the first in your company to keep your information updated. Click here and update the information requested about your email.

[Update email information](#)

Was this helpful? [Send feedback](#)



Christopher Smith
Microsoft Support Team
support@microsoft.com
1 Microsoft Way, Redmond, Washington 98052-8300
Support line: 1 (425) 882-8080

Copyright © 2022 Microsoft. All rights reserved.

You are receiving this emails because your company has Microsoft support.

Want to change how you receive these emails?

You can [update your preferences](#) or [unsubscribe from this list](#).

Figure: phishing email for Microsoft - email not delivered, manipulating best practices of persuasion (yes), usability (yes), influence (yes)

Your message couldn't be delivered

Microsoft Support support@microsoft.com

para mim ▾

Your message to director@cogindustries.com couldn't be delivered. Your mail program is using out-of-date address information.

Office 365

administrative@cogindustries.com

Action Required

Out-of-date FROM address

How to Fix It

Click [here](#) and update the information requested about your email.

Was this helpful? [Send feedback](#).

Figure: phishing email for Microsoft - email not delivered, manipulating best practices of persuasion (no), usability (no), influence (no)

Employee bonus list

Please review the following document

Laura Marroquin <L.marroquin@orders-legal.com>

I have been contacted by your Cog Industries employer's head office to have you review the following documentation. Here is Cog Industries Employees Bonus List for the next month.

[https://docs.google.com/document/b/\[\[random_number_6\]\]](https://docs.google.com/document/b/[[random_number_6]])

Please review this document to make sure that the people on this list are accurate and that everyone is currently on this document. On the second page, you can find the reason for the employment contract bonuses for each employee in Cog Industries.

Please sign the second page once you have finished reviewing the information in its entirety.

I tried to reach you early this morning, but you were not available.

Best regards,

Figure: phishing email for Employee bonus list, manipulating best practices of persuasion (no), usability (no), influence (no)

Please review the following document

From: Laura Marroquin <L.marroquin@orders-legal.com>



I have been contacted by your employer's head office to have you review the following documentation. Here is Employees Bonus List for the next month.

[Review document](#)

Please review this document to make sure that the people on this list are accurate and that everyone is currently on this document. On the second page, you can find the reason for the employment contract bonuses for each employee in your company.

Please sign the second page once you have finished reviewing the information in its entirety.

I tried to reach you early this morning, but you were not available.

Best regards,

Laura Marroquin
Analyst
(485) 813-8960

Copyright © * 2022 * Bellis and Manuel Law, All rights reserved.
You are receiving this email because your company has Microsoft support.

Want to change how you receive these emails?
You can [update your preferences](#) or [unsubscribe from this list](#).

Figure: phishing email for Employee bonus list, manipulating best practices of persuasion (no), usability (yes), influence (no)

Please review the following document

Laura Marroquin <L.marroquin@orders-legal.com>

Hello **Jordan Williams**,

I hope you are doing well. My name is Laura Marroquin. I am an analyst at Bellis and Manuel Law Firm. I have been contacted by Cog Industries head office to help you to prepare the Employee's Bonus List for the next month. The head office had chosen me to assist you because when I started to work in administrative activities, I had some challenges preparing documents in a legally-oriented way. Then, I created a method that worked for me, and today I can assist other people to have an easier path.

To facilitate your task, I have prepared a [draft of the document](#). Please click [here](#) to review this document to make sure that the people on this list are accurate and that everyone is currently on this document. On the second page, you can find the reason for the employment contract bonuses for each employee in your company.

Please sign the second page once you have finished reviewing the information in its entirety.

I tried to reach you early this morning, but you were not available.

Best regards,

Figure: phishing email for Employee bonus list, manipulating best practices of persuasion (yes), usability (no), influence (no)

Please review the following document

Laura Marroquin <L.marroquin@orders-legal.com>

I have been contacted by your Cog Industries employer's head office to have you review the following documentation. Here is Cog Industries Employees Bonus List for the next month.

[https://docs.google.com/document/b/\[\[random_number_6\]\]](https://docs.google.com/document/b/[[random_number_6]])

Please review this document to make sure that the people on this list are accurate and that everyone is currently on this document. On the second page, you can find the reason for the employment contract bonuses for each employee in Cog Industries.

Please sign the second page once you have finished reviewing the information in its entirety.

Be the first company to finish this task and don't lose the due date to pay the bonus.

I tried to reach you early this morning, but you were not available.

Best regards,

Figure: phishing email for Employee bonus list, manipulating best practices of persuasion (no), usability (no), influence (yes)

Please review the following document

From: Laura Marroquin <L.marroquin@orders-legal.com>



Hello **Jordan Williams**,

I hope you are doing well. My name is Laura Marroquin. I am an analyst at Bellis and Manuel Law Firm. I have been contacted by Cog Industries head office to help you to prepare the Employee's Bonus List for the next month. The head office has chosen me to assist you because when I started to work in administrative activities I had some challenges preparing documents in a legally-oriented way. Then, I created a method that worked for me, and today I can assist other people to have an easier path.

To facilitate your task, I have prepared a [draft of the document](#). Please click [here](#) to review this document to make sure that the people on this list are accurate and that everyone is currently on this document. On the second page, you can find the reason for the employment contract bonuses for each employee in your company.

[Review document](#)

Please sign the second page once you have finished reviewing the information in its entirety.

I tried to reach you early this morning, but you were not available.

Best regards,

Laura Marroquin
Analyst
(485) 813-8960

Copyright © * 2022 * Bellis and Manuel Law, All rights reserved.
You are receiving this email because your company has Microsoft support.

Want to change how you receive these emails?
You can [update your preferences](#) or [unsubscribe from this list](#).

Figure: phishing email for Employee bonus list, manipulating best practices of persuasion (yes), usability (yes), influence (no)

Please review the following document

From: Laura Marroquin <L.marroquin@orders-legal.com>

Hello **Jordan Williams**,

I hope you are doing well. My name is Laura Marroquin. I am an analyst at Bellis and Manuel Law Firm. I have been contacted by Cog Industries head office to help you to prepare the Employee's Bonus List for the next month. The head office had chosen me to assist you because when I started to work in administrative activities, I had some challenges preparing documents in a legally-oriented way. Then, I created a method that worked for me, and today I can assist other people in having an easier path.

To facilitate your task, I have prepared a [draft of the document](#). Please click [here](#) to review this document to make sure that the people on this list are accurate and that everyone is currently on this document. On the second page, you can find the reason for the employment contract bonuses for each employee in your company.

I know that paying the bonus until the due date is critical, so if you finish it soon, I will put you as the first company to attend.

Please sign the second page once you have finished reviewing the information in its entirety.

I tried to reach you early this morning, but you were not available.

Best regards,

Figure: phishing email for Employee bonus list, manipulating best practices of persuasion (yes), usability (no), influence (yes)

Please review the following document

From: Laura Marroquin <L.marroquin@orders-legal.com>



I have been contacted by your employer's head office to have you review the following documentation. Here is Employees Bonus List for the next month.

[Review document](#)

Please review this document to make sure that the people on this list are accurate and that everyone is currently on this document. On the second page, you can find the reason for the employment contract bonuses for each employee in your company.

Be the first company to finish this task and don't lose the due date to pay the bonus.

Please sign the second page once you have finished reviewing the information in its entirety.

I tried to reach you early this morning, but you were not available.

Best regards,

Laura Marroquin
Analyst
(485) 813-8960

Copyright © * 2022 * Bellis and Manuel Law, All rights reserved.
You are receiving this email because your company has Microsoft support.

Want to change how you receive these emails?
You can [update your preferences](#) or [unsubscribe from this list](#).

Figure: phishing email for Employee bonus list, manipulating best practices of persuasion (no), usability (yes), influence (yes)

Please review the following document

From: Laura Marroquin <L.marroquin@orders-legal.com>



Hello **Jordan Williams**,

I hope you are doing well. My name is Laura Marroquin. I am an analyst at Bellis and Manuel Law Firm. I have been contacted by Cog Industries head office to help you to prepare the Employee's Bonus List for the next month. The head office has chosen me to assist you because when I started to work in administrative activities I had some challenges preparing documents in a legally-oriented way. Then, I created a method that worked for me, and today I can assist other people to have an easier path.

To facilitate your task, I have prepared a [draft of the document](#). Please click [here](#) to review this document to make sure that the people on this list are accurate and that everyone is currently on this document. On the second page, you can find the reason for the employment contract bonuses for each employee in your company.

[Review document](#)

Please sign the second page once you have finished reviewing the information in its entirety.

I know that paying the bonus until the due date is critical, so if you finish it soon, I will put you as the first company to attend.

I tried to reach you early this morning, but you were not available.

Best regards,

Laura Marroquin
Analyst
(485) 813-8960

Copyright © * 2022 * Bellis and Manuel Law, All rights reserved.
You are receiving this email because your company has Microsoft support.

Want to change how you receive these emails?

Figure: phishing email for Employee bonus list, manipulating best practices of persuasion (yes), usability (yes), influence (yes)

APPENDIX B:
IRB DOCUMENTS



UNIVERSITY OF CENTRAL FLORIDA

Institutional Review Board

FWA00000351
IRB00001138, IRB00012110
Office of Research
12201 Research Parkway
Orlando, FL 32826-3246

EXEMPTION DETERMINATION

September 6, 2022

Dear Erica Leite De Castilho Grao:

On 9/2/2022, the IRB determined the following submission to be human subjects research that is exempt from regulation:

Type of Review:	Initial Study
Title:	EVALUATION OF THE PERSUASIVE USABILITY FRAMEWORK
Investigator:	Erica Leite De Castilho Grao
IRB ID:	STUDY00004309
Funding:	None
Grant ID:	None
Documents Reviewed:	<ul style="list-style-type: none"> • appendix - images of emails.docx, Category: Survey / Questionnaire; • HRP-509 - Debriefing Statement.pdf, Category: Consent Form; • Protocol, Category: IRB Protocol; • STUDY 4309 HRP-254-FORM Explanation of Research_v4.pdf, Category: Consent Form;

This determination applies only to the activities described in the IRB submission and does not apply should any changes be made. If changes are made, and there are questions about whether these changes affect the exempt status of the human research, please submit a modification request to the IRB. Guidance on submitting Modifications and Administrative Check-in are detailed in the Investigator Manual (HRP-103), which can be found by navigating to the IRB Library within the IRB system. When you have completed your research, please submit a Study Closure request so that IRB records will be accurate.

If you have any questions, please contact the UCF IRB at 407-823-2901 or irb@ucf.edu. Please include your project title and IRB number in all correspondence with this office.

Sincerely,

Gillian Bernal
Designated Reviewer

Figure: Letter with the IRB Exemption Determination

APPENDIX C:
CITI TRAINING COMPLETION CERTIFICATE



Completion Date 15-Jul-2021
Expiration Date 14-Jul-2024
Record ID 41755910

This is to certify that:

Erica Grao

Has completed the following CITI Program course:

Not valid for renewal of certification through CME.

Responsible Conduct of Research for Engineers
(Curriculum Group)

Responsible Conduct of Research for Engineers
(Course Learner Group)

1 - RCR
(Stage)

Under requirements set by:

University of Central Florida




Verify at www.citiprogram.org/verify/?w0ecef91e-7a34-4aef-b8af-450b9378373a-41755910

APPENDIX D:
AUTHORIZATION FOR USE OF WEBQUAL 4.0

Copyright information

[Report message](#) · [Block user](#)



Erica Castilho Grão 2 days ago

Hello Dr Barnes,
Hope you are doing well.
My name is Erica Castilho, and I am a PhD student at the University of Central Florida. I am developing my dissertation proposal, that includes the creation of a conceptual framework to improve effectiveness of emails. I intend to use the structure of dimensions and factors of your method WEBQUAL4.0 to categorize the features that impacts decision-making in emails according to quality dimensions.
I would like to know if I need some authorization or to buy some copyright to do it, or just to cite your work is enough.
Best,
Erica



Stuart J. Barnes to you 1 day ago

Hi Erica
Citing our work should be enough. Good luck with your research
Best wishes
Stuart


[Reply](#)

[Mark as unread](#)


[More](#) ▾

Copyright information

[Report message](#) · [Block user](#)

 **Erica Castilho Grão** 2 days ago

Hello Dr Barnes,
Hope you are doing well.
My name is Erica Castilho, and I am a PhD student at the University of Central Florida. I am developing my dissertation proposal, that includes the creation of a conceptual framework to improve effectiveness of emails. I intend to use the structure of dimensions and factors of your method WEBQUAL4.0 to categorize the features that impacts decision-making in emails according to quality dimensions.
I would like to know if I need some authorization or to buy some copyright to do it, or just to cite your work is enough.
Best,
Erica

 **Richard Vidgen** to you 2 days ago

Hi Erica
All the Webqual material is in the public domain, none of it is subject to copyright. Please feel free to use and cite the original work in the normal way.
Richard Vidgen

APPENDIX E:
SPSS CONFIGURATION FOR MANCOVA

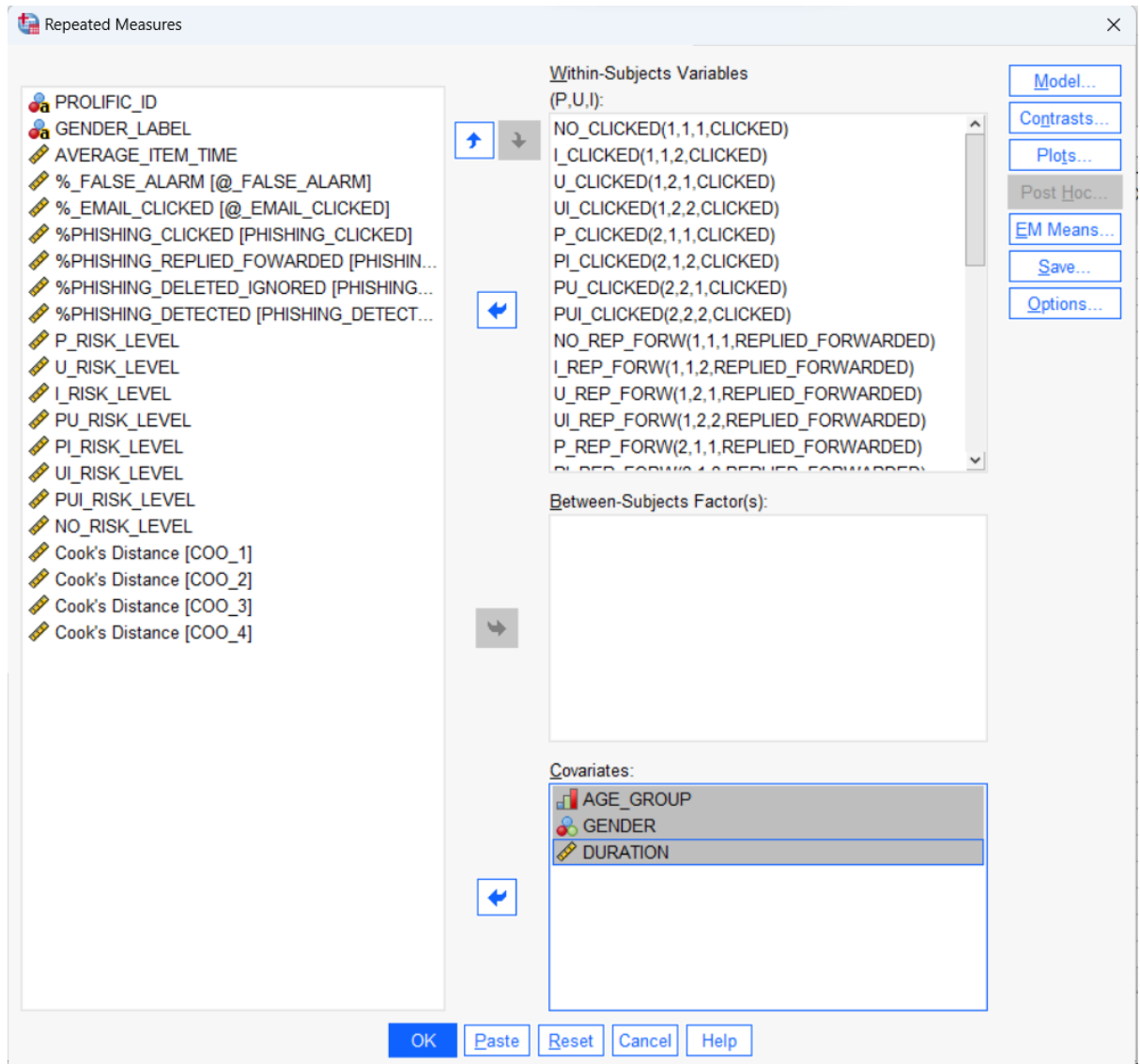


Figure: Page 1 for configuration of Repeated Measures MANCOVA

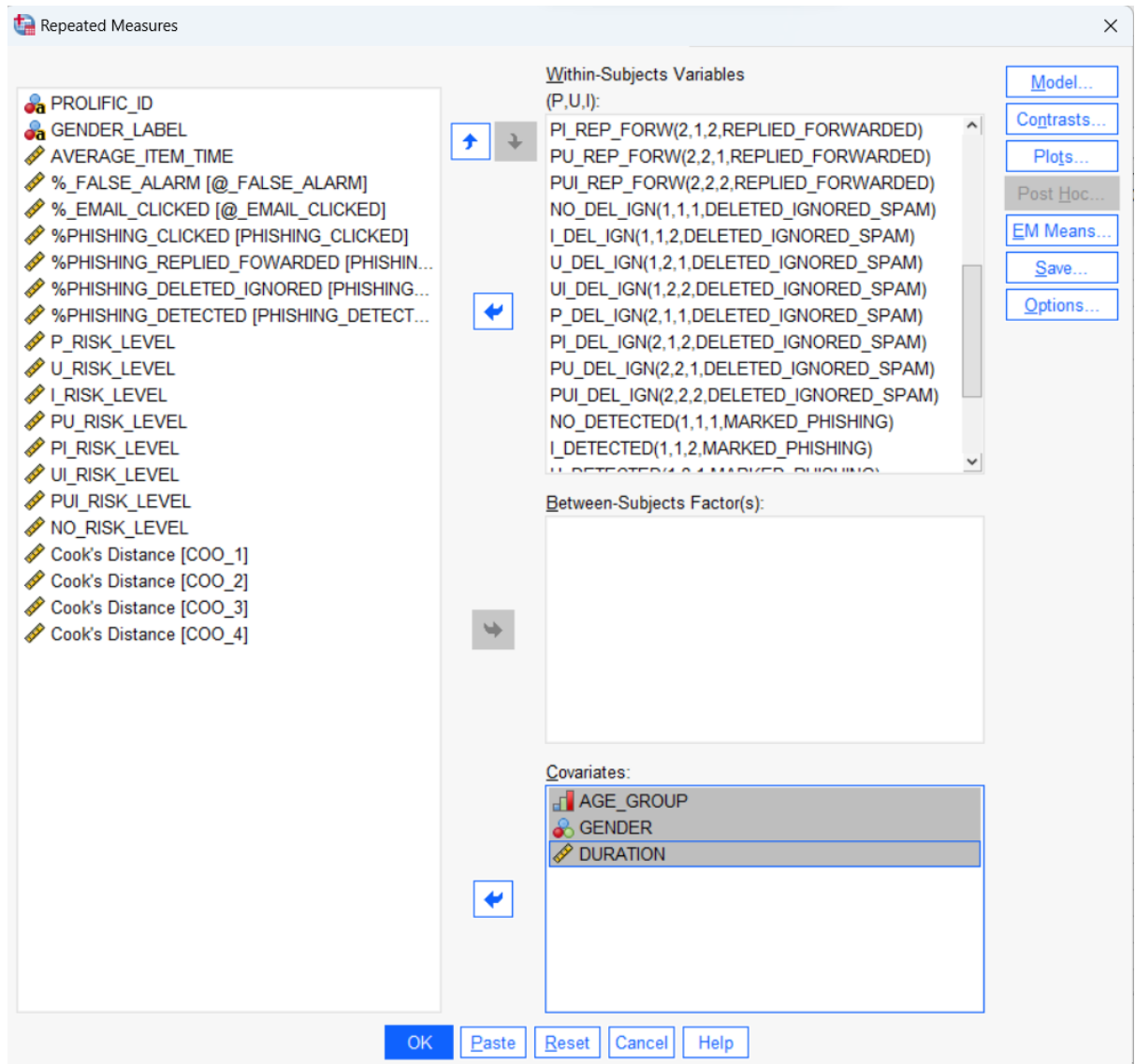


Figure: Page 2 for configuration of Repeated Measures MANCOVA

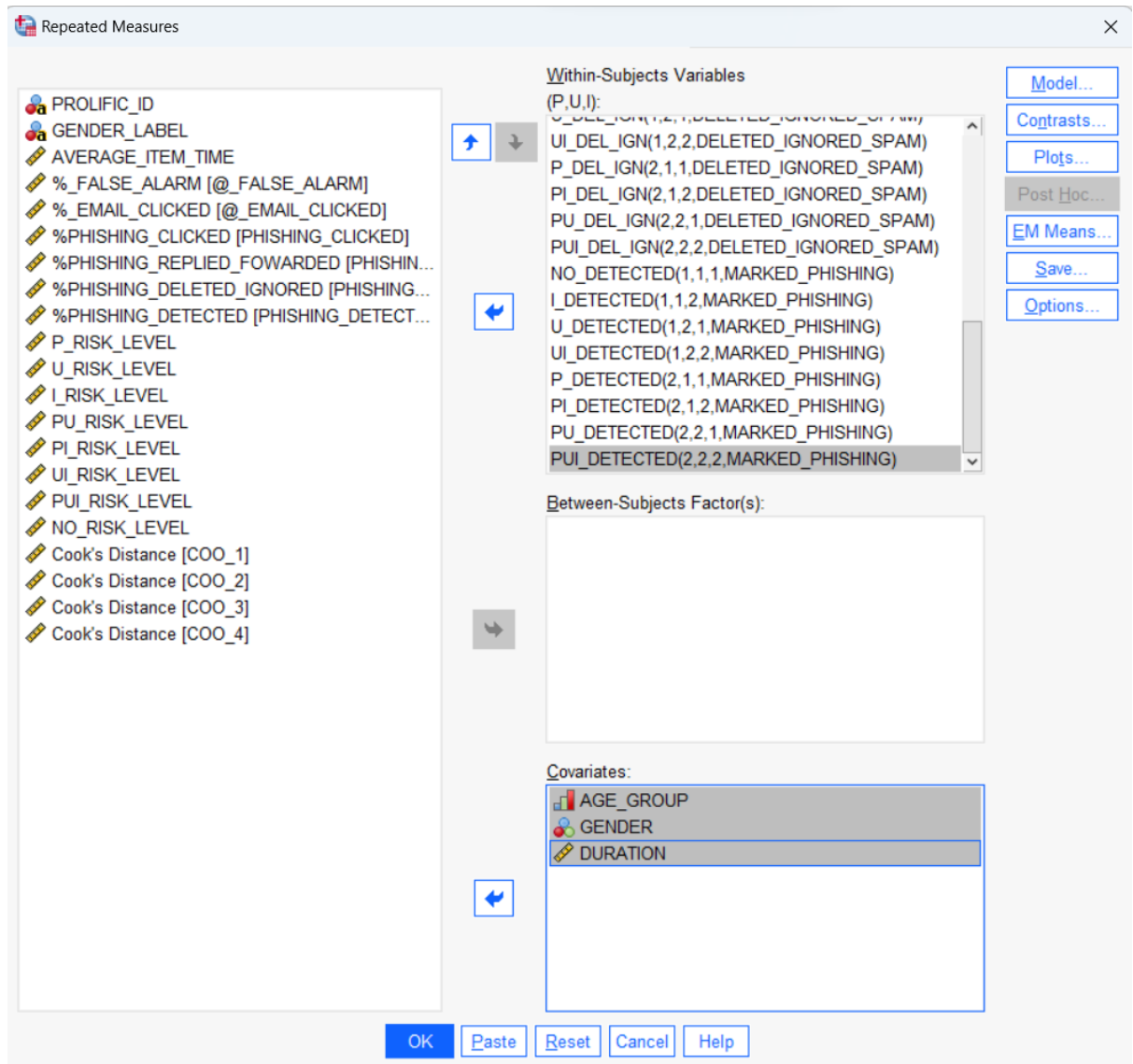


Figure: Page 3 for configuration of Repeated Measures MANCOVA

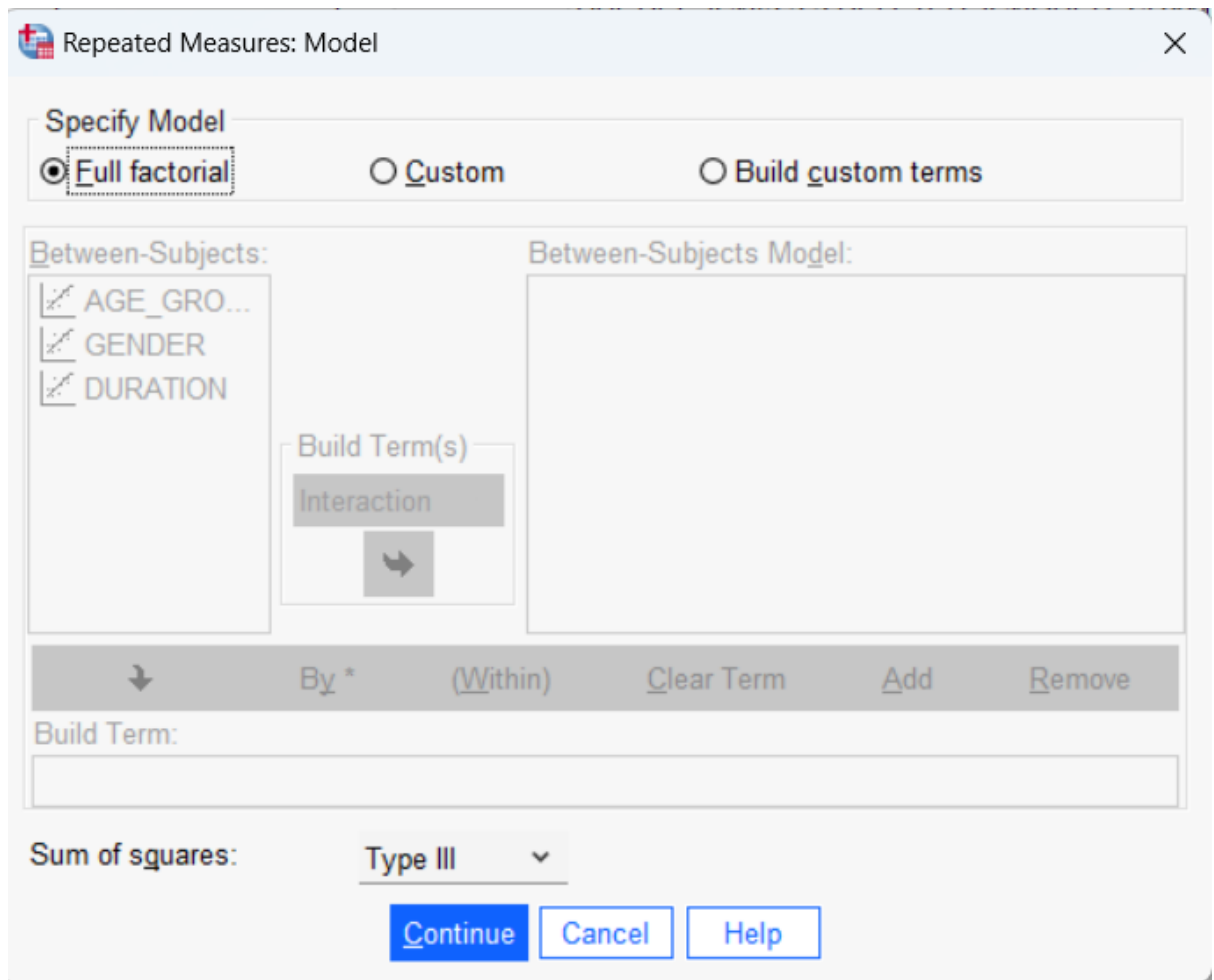


Figure: Model screen, after clicking the model button

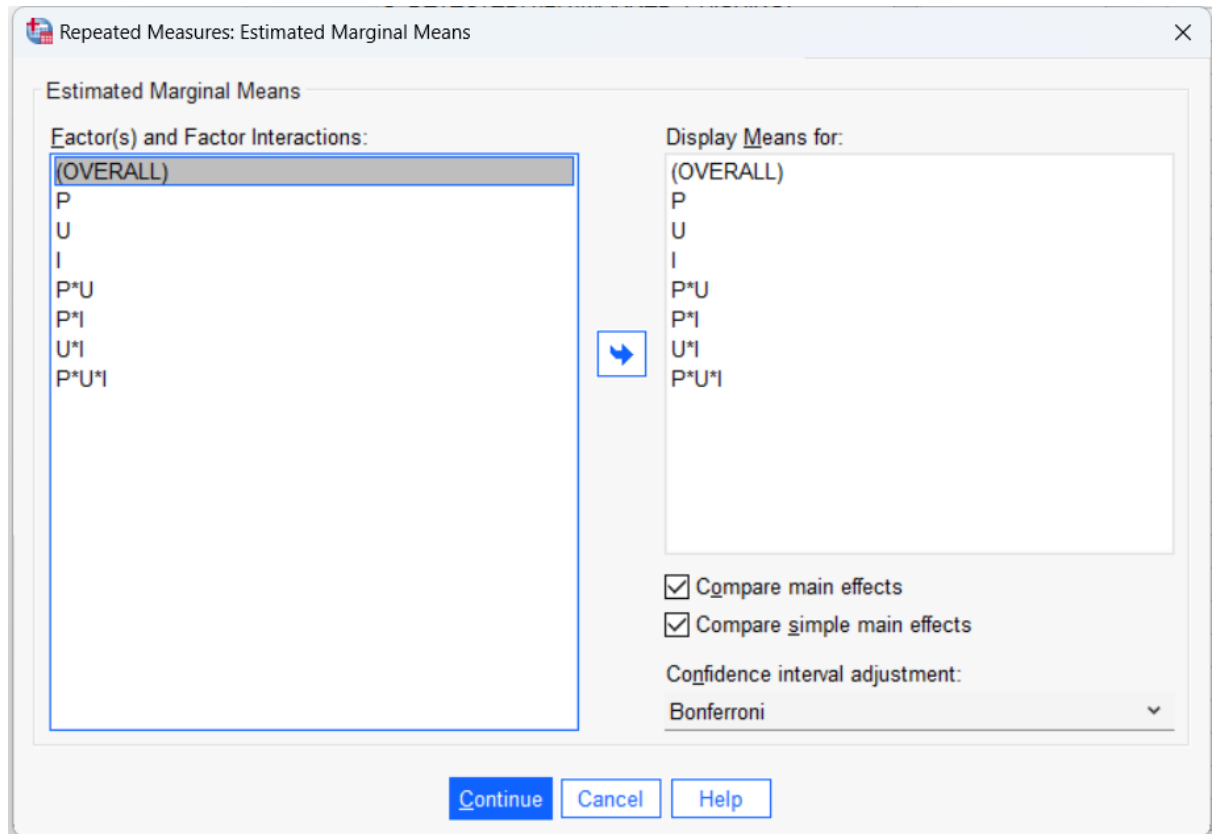


Figure: EM Means screen

Repeated Measures: Profile Plots

Factors:

- P
- U
- I

Horizontal Axis:

Separate Lines:

Separate Plots:

Plots: Add Change Remove

- P*U
- P*I
- U*I
- P*U*I

Chart Type:

Line Chart

Bar Chart

Error Bars

Include Error bars

Confidence Interval (95.0%)

Standard Error Multiplier: 2

Include reference line for grand mean

Y axis starts at 0

Continue Cancel Help

Figure: Profile Plots

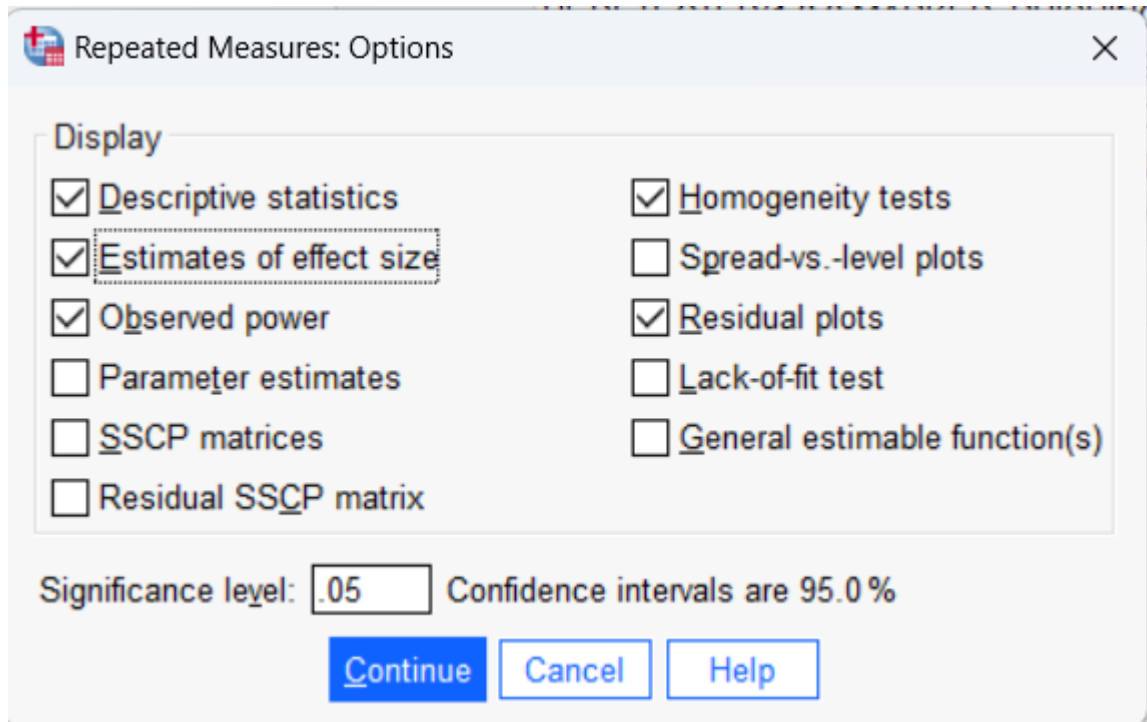


Figure: Options screen, after clicking the options button

Descriptive Statistics

	Mean	Std. Deviation	N
NO_CLICKED	.35	.476	399
I_CLICKED	.33	.470	399
U_CLICKED	.34	.474	399
UI_CLICKED	.32	.467	399
P_CLICKED	.26	.437	399
PI_CLICKED	.21	.408	399
PU_CLICKED	.25	.431	399
PUI_CLICKED	.27	.446	399
NO_REP_FORW	.10	.297	399
I_REP_FORW	.07	.251	399
U_REP_FORW	.06	.233	399
UI_REP_FORW	.07	.247	399
P_REP_FORW	.14	.343	399
PI_REP_FORW	.18	.383	399
PU_REP_FORW	.06	.229	399
PUI_REP_FORW	.09	.280	399
NO_DEL_IGN	.33	.472	399
I_DEL_IGN	.36	.480	399
U_DEL_IGN	.41	.492	399
UI_DEL_IGN	.44	.497	399
P_DEL_IGN	.36	.481	399
PI_DEL_IGN	.35	.476	399
PU_DEL_IGN	.51	.501	399
PUI_DEL_IGN	.46	.499	399
NO_DETECTED	.22	.417	399
I_DETECTED	.25	.431	399
U_DETECTED	.20	.399	399
UI_DETECTED	.18	.381	399
P_DETECTED	.25	.432	399
PI_DETECTED	.27	.442	399
PU_DETECTED	.19	.391	399
PUI_DETECTED	.18	.387	399

Figure: SPSS results for descriptive statistics

Multivariate Tests^a

Effect			Value	F	Hypothesis df	Error df	Sig.	Partial Eta Squared	Noncent. Parameter	Observed Power ^c
Between Subjects	Intercept	Pillai's Trace	.682	281.143 ^b	3.000	393.000	<.001	.682	843.430	1.000
		Wilks' Lambda	.318	281.143 ^b	3.000	393.000	<.001	.682	843.430	1.000
		Hotelling's Trace	2.146	281.143 ^b	3.000	393.000	<.001	.682	843.430	1.000
		Roy's Largest Root	2.146	281.143 ^b	3.000	393.000	<.001	.682	843.430	1.000
	AGE_GROUP	Pillai's Trace	.013	1.707 ^b	3.000	393.000	.165	.013	5.122	.446
		Wilks' Lambda	.987	1.707 ^b	3.000	393.000	.165	.013	5.122	.446
		Hotelling's Trace	.013	1.707 ^b	3.000	393.000	.165	.013	5.122	.446
		Roy's Largest Root	.013	1.707 ^b	3.000	393.000	.165	.013	5.122	.446
	GENDER	Pillai's Trace	.024	3.201 ^b	3.000	393.000	.023	.024	9.602	.737
		Wilks' Lambda	.976	3.201 ^b	3.000	393.000	.023	.024	9.602	.737
		Hotelling's Trace	.024	3.201 ^b	3.000	393.000	.023	.024	9.602	.737
		Roy's Largest Root	.024	3.201 ^b	3.000	393.000	.023	.024	9.602	.737
	DURATION	Pillai's Trace	.014	1.909 ^b	3.000	393.000	.127	.014	5.728	.493
		Wilks' Lambda	.986	1.909 ^b	3.000	393.000	.127	.014	5.728	.493
		Hotelling's Trace	.015	1.909 ^b	3.000	393.000	.127	.014	5.728	.493
		Roy's Largest Root	.015	1.909 ^b	3.000	393.000	.127	.014	5.728	.493

SPSS results for multivariate Tests. Gender had effects on the phishing engagement. Age and duration didn't present statistically significant effects on the phishing engagement.

Tests of Between-Subjects Effects

Transformed Variable: Average

Source	Measure	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared	Noncent. Parameter	Observed Power ^a
Intercept	CLICKED	71.741	1	71.741	109.506	<.001	.217	109.506	1.000
	REPLIED_FORWARDED	5.275	1	5.275	24.082	<.001	.057	24.082	.998
	DELETED_IGNORED_SPAM	105.200	1	105.200	186.149	<.001	.320	186.149	1.000
	MARKED_PHISHING	9.568	1	9.568	17.899	<.001	.043	17.899	.988
AGE_GROUP	CLICKED	1.118	1	1.118	1.706	.192	.004	1.706	.256
	REPLIED_FORWARDED	.018	1	.018	.083	.773	.000	.083	.060
	DELETED_IGNORED_SPAM	.373	1	.373	.660	.417	.002	.660	.128
	MARKED_PHISHING	2.350	1	2.350	4.397	.037	.011	4.397	.552
GENDER	CLICKED	5.933	1	5.933	9.055	.003	.022	9.055	.851
	REPLIED_FORWARDED	.004	1	.004	.018	.894	.000	.018	.052
	DELETED_IGNORED_SPAM	2.364	1	2.364	4.183	.041	.010	4.183	.532
	MARKED_PHISHING	.923	1	.923	1.726	.190	.004	1.726	.259
DURATION	CLICKED	.032	1	.032	.049	.825	.000	.049	.056
	REPLIED_FORWARDED	.018	1	.018	.083	.773	.000	.083	.060
	DELETED_IGNORED_SPAM	2.160	1	2.160	3.823	.051	.010	3.823	.496
	MARKED_PHISHING	2.033	1	2.033	3.803	.052	.010	3.803	.494
Error	CLICKED	258.780	395	.655					
	REPLIED_FORWARDED	86.513	395	.219					
	DELETED_IGNORED_SPAM	223.230	395	.565					
	MARKED_PHISHING	211.142	395	.535					

a. Computed using alpha = .05

Figure: MANCOVA tests of between-subjects effects. GENDER was the only covariate that had statistically significant impact over clicked and deleted, ignored or marked as spam engagement levels. The other covariates didn't present significant results.

APPENDIX F:
SPSS MANOVA RESULTS

In this session we present the analysis in a different approach, by using MANOVA instead of MANCOVA. We opted to use MANCOVA to deliver our results. But we compared the results with MANOVA to check differences.

Multivariate Tests ^a										
Effect			Value	F	Hypothesis df	Error df	Sig.	Partial Eta Squared	Noncent Parameter	Observed Power ^c
Between Subjects	Intercept	Pillai's Trace	.903	1232.601 ^b	3.000	396.000	<.001	.903	3697.804	1.000
		Wilks' Lambda	.097	1232.601 ^b	3.000	396.000	<.001	.903	3697.804	1.000
		Hotelling's Trace	9.338	1232.601 ^b	3.000	396.000	<.001	.903	3697.804	1.000
		Roy's Largest Root	9.338	1232.601 ^b	3.000	396.000	<.001	.903	3697.804	1.000
Within Subjects	P	Pillai's Trace	.105	15.535 ^b	3.000	396.000	<.001	.105	46.605	1.000
		Wilks' Lambda	.895	15.535 ^b	3.000	396.000	<.001	.105	46.605	1.000
		Hotelling's Trace	.118	15.535 ^b	3.000	396.000	<.001	.105	46.605	1.000
		Roy's Largest Root	.118	15.535 ^b	3.000	396.000	<.001	.105	46.605	1.000
	U	Pillai's Trace	.140	21.498 ^b	3.000	396.000	<.001	.140	64.495	1.000
		Wilks' Lambda	.860	21.498 ^b	3.000	396.000	<.001	.140	64.495	1.000
		Hotelling's Trace	.163	21.498 ^b	3.000	396.000	<.001	.140	64.495	1.000
		Roy's Largest Root	.163	21.498 ^b	3.000	396.000	<.001	.140	64.495	1.000
	I	Pillai's Trace	.007	.873 ^b	3.000	396.000	.455	.007	2.619	.241
		Wilks' Lambda	.993	.873 ^b	3.000	396.000	.455	.007	2.619	.241
		Hotelling's Trace	.007	.873 ^b	3.000	396.000	.455	.007	2.619	.241
		Roy's Largest Root	.007	.873 ^b	3.000	396.000	.455	.007	2.619	.241
	P * U	Pillai's Trace	.043	5.871 ^b	3.000	396.000	<.001	.043	17.614	.953
		Wilks' Lambda	.957	5.871 ^b	3.000	396.000	<.001	.043	17.614	.953
		Hotelling's Trace	.044	5.871 ^b	3.000	396.000	<.001	.043	17.614	.953
		Roy's Largest Root	.044	5.871 ^b	3.000	396.000	<.001	.043	17.614	.953
	P * I	Pillai's Trace	.027	3.667 ^b	3.000	396.000	.012	.027	11.000	.800
		Wilks' Lambda	.973	3.667 ^b	3.000	396.000	.012	.027	11.000	.800
		Hotelling's Trace	.028	3.667 ^b	3.000	396.000	.012	.027	11.000	.800
		Roy's Largest Root	.028	3.667 ^b	3.000	396.000	.012	.027	11.000	.800
	U * I	Pillai's Trace	.010	1.289 ^b	3.000	396.000	.278	.010	3.867	.344
		Wilks' Lambda	.990	1.289 ^b	3.000	396.000	.278	.010	3.867	.344
		Hotelling's Trace	.010	1.289 ^b	3.000	396.000	.278	.010	3.867	.344
		Roy's Largest Root	.010	1.289 ^b	3.000	396.000	.278	.010	3.867	.344
	P * U * I	Pillai's Trace	.010	1.278 ^b	3.000	396.000	.281	.010	3.834	.342
		Wilks' Lambda	.990	1.278 ^b	3.000	396.000	.281	.010	3.834	.342
		Hotelling's Trace	.010	1.278 ^b	3.000	396.000	.281	.010	3.834	.342
		Roy's Largest Root	.010	1.278 ^b	3.000	396.000	.281	.010	3.834	.342

a. Design: Intercept
Within Subjects Design: P + U + I + P * U + P * I + U * I + P * U * I

b. Exact statistic

c. Computed using alpha = .05

Figure: Results of multivariate Tests for a MANOVA showed statistically significant results for P, U and PU. This differs from the MANCOVA, which presented statistically significant results for P, U and PUI.

Univariate Tests										
Source			Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared	Noncent. Parameter	Observed Power ^a
P	CLICKED	Greenhouse-Geisser	6.053	1.000	6.053	37.453	0.000	0.086	37.453	1.000
	REPLIED_FORWARDED	Greenhouse-Geisser	1.365	1.000	1.365	17.444	0.000	0.042	17.444	0.986
	DELETED_IGNORED_SPAM	Greenhouse-Geisser	0.982	1.000	0.982	4.442	0.036	0.011	4.442	0.557
	MARKED_PHISHING	Greenhouse-Geisser	0.091	1.000	0.091	0.632	0.427	0.002	0.632	0.125
U	CLICKED	Greenhouse-Geisser	0.070	1.000	0.070	0.485	0.486	0.001	0.485	0.107
	REPLIED_FORWARDED	Greenhouse-Geisser	2.317	1.000	2.317	30.055	0.000	0.070	30.055	1.000
	DELETED_IGNORED_SPAM	Greenhouse-Geisser	8.633	1.000	8.633	39.553	0.000	0.090	39.553	1.000
	MARKED_PHISHING	Greenhouse-Geisser	2.827	1.000	2.827	22.827	0.000	0.054	22.827	0.997
P * U	CLICKED	Greenhouse-Geisser	0.228	1.000	0.228	1.743	0.188	0.004	1.743	0.261
	REPLIED_FORWARDED	Greenhouse-Geisser	0.847	1.000	0.847	14.883	0.000	0.036	14.883	0.971
	DELETED_IGNORED_SPAM	Greenhouse-Geisser	0.607	1.000	0.607	3.267	0.071	0.008	3.267	0.438
	MARKED_PHISHING	Greenhouse-Geisser	0.113	1.000	0.113	1.139	0.286	0.003	1.139	0.187

a. Computed using alpha = .05

Table: Univariate tests for P, U, PU for the MANOVA analysis. Significant results are highlighted in grey.

APPENDIX G:
PUBLICATIONS

The following publications were based on this work:

1. Castilho Grão, Erica & Canham, Matthew & Sawyer, Ben D. (2023) Invasion of the Killer Phish From Planet UX: Applying Practices of Marketing to Phishing Attacks. CHI, 2024. (Under review)
2. Castilho Grão, Erica (2023). Navigating with Sharks: A Guide to Apply Marketing Practices on Phishing Email Simulations. CHI, 2024. (Under review)

REFERENCES

- Akbar, N. (2014, October). Analysing Persuasion Principles in Phishing Emails [Info:eu-repo/semantics/masterThesis]. University of Twente. <http://essay.utwente.nl/66177/>
- Barnes, S. J., & Vidgen, R. T. (2002). AN INTEGRATIVE APPROACH TO THE ASSESSMENT OF E-COMMERCE QUALITY. 3(3), 14.
- Bevan, N. (2009, August). What is the difference between the purpose of usability and user experience evaluation methods. In Proceedings of the Workshop UXEM (Vol. 9, No. 1, pp. 1-4).
- Biswas, B., & Mukhopadhyay, A. (2019). Why do I get phished? The role of persuasion, design authenticity and contextualization. *AMCIS 2019 Proceedings*.
https://aisel.aisnet.org/amcis2019/info_security_privacy/info_security_privacy/28
- Brown, D., & Fiorella, S. (2013). Influence marketing: How to create, manage, and measure brand influencers in social media marketing. Que Publishing.
- Canham, M., Constantino, M., Hudson, I., Fiore, S. M., Caulkins, B., & Reinerman-Jones, L. (2019). The Enduring Mystery of the Repeat Clickers. *15th Symposium on Usable Privacy and Security (SOUPS 2019)*. *USENIX Advanced Computing Systems Association*.
- Carella, A., Kotsoev, M., & Truta, T. M. (2017). Impact of security awareness training on phishing click-through rates. *2017 IEEE International Conference on Big Data (Big Data)*, 4458–4466. <https://doi.org/10.1109/BigData.2017.8258485>
- Castilho Grão, Erica & Canham, Matthew & Sawyer, Ben D. (2023) Invasion of the Killer Phish From Planet UX: Applying Practices of Marketing to Phishing Attacks. CHI, 2024. (Under review)
- Chang. (2021, June 9). *56 Email Statistics You Must Learn: 2022 Data on User Behaviour & Best Practices*. Financesonline.Com. <https://financesonline.com/email-statistics/>

- Cialdini, R. B. (1993). *Influence: The psychology of persuasion* (Rev. ed.). Morrow.
- Cooper, W. (2021). *Dark Psychology and Manipulation: Discover 40 Covert Emotional Manipulation Techniques, Mind Control, Brainwashing. Learn How to Analyze People, NLP Secret ... Effect, Subliminal Influence Book 1*.
- Dabbish, L. A., Kraut, R. E., Fussell, S., & Kiesler, S. (2005). Understanding email use: Predicting action on a message. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 691–700.
- Downs, J. S., Holbrook, M., & Cranor, L. F. (2007). Behavioral response to phishing risk. *Proceedings of the Anti-Phishing Working Groups 2nd Annual ECrime Researchers Summit*, 37–44. <https://doi.org/10.1145/1299015.1299019>
- Farook, F. S., & Abeysekara, N. (2016). Influence of social media marketing on customer engagement. *International Journal of Business and Management Invention*, 5(12), 115-125.
- Ferreira, Ana, and Soraia Teles. "Persuasion: How Phishing Emails Can Influence Users and Bypass Security Measures." *International Journal of Human-Computer Studies*, vol. 125, May 2019, pp. 19–31, <https://doi.org/10.1016/j.ijhcs.2018.12.004>.
- Flavián, Carlos, et al. "The Role Played by Perceived Usability, Satisfaction and Consumer Trust on Website Loyalty." *Information & Management*, vol. 43, no. 1, 2006, pp. 1–14, <https://doi.org/10.1016/j.im.2005.01.002>.
- Furgison McEwen, L. (2016, April 18). 6 FAQs About Heat Maps for Your Website and Email Campaigns. *Pinpointe Marketing Blog*. <https://www.pinpointe.com/blog/6-frequently-asked-questions-about-heat-maps-for-your-website-and-email-campaigns>
- Goel, S., Williams, K., & Dincelli, E. (2017). Got Phished? Internet Security and Human Vulnerability. *Journal of the Association for Information Systems*, 18(1), 22–44. <https://doi.org/10.17705/1jais.00447>

- Goldman, J. (2020, November 11). *Email Marketing 2020, The Pandemic Makes This Touchpoint Increasingly Relevant for Marketers and Consumers*. Insider Intelligence. <https://www.emarketer.com/content/email-marketing-2020>
- Gordon, W. J., Wright, A., Glynn, R. J., Kadakia, J., Mazzone, C., Leinbach, E., & Landman, A. (2019). Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system. *Journal of the American Medical Informatics Association*, 26(6), 547-552.
- Greve, Henrich R., et al. "Rational Fouls? Loss Aversion on Organizational and Individual Goals Influence Decision Quality." *Organization Studies*, vol. 42, no. 7, July 2021, pp. 1031–51, <https://doi.org/10.1177/0170840619878462>.
- Gunelius, S. (2018). *Ultimate Guide to Email Marketing for Business*. Entrepreneur Press.
- Hamilton, B. L. (1977). An empirical investigation of the effects of heterogeneous regression slopes in analysis of covariance. *Educational and Psychological Measurement*, 37(3), 701-712.
- Hornbæk, K. (2006). Current practice in measuring usability: Challenges to usability studies and research. *International Journal of Human-Computer Studies*, 64(2), 79–102. <https://doi.org/10.1016/j.ijhcs.2005.06.002>
- Ibrahim, Nurulhuda, et al. Proposed Model of Persuasive Visual Design for Web Design. ACIS, 2014, <https://openrepository.aut.ac.nz/handle/10292/8044>.
- ISO. (2009). *Human-centred design process for interactive systems*. <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/20/52075.html>
- Jayatilaka, A., Arachchilage, N. A. G., & Babar, M. A. (2021). Falling for Phishing: An Empirical Investigation into People's Email Response Behaviors. *ArXiv:2108.04766 [Cs]*. <http://arxiv.org/abs/2108.04766>

- Kahneman, D., & Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk. *Econometrica*, 47(2), 263. <https://doi.org/10.2307/1914185>
- Keller, G. (2021, January 27). *Security and remote working—How to think about access*. TechRadar. <https://www.techradar.com/news/security-and-remote-working-thinking-about-access>
- Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). School of phish: A real-word evaluation of anti-phishing training. *Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09*, 1. <https://doi.org/10.1145/1572532.1572536>
- Kumar, A. (2021). An empirical examination of the effects of design elements of email newsletters on consumers' email responses and their purchase. *Journal of Retailing and Consumer Services*, 58, 102349.
- Lawson, Patrick A., et al. "Baiting the Hook: Exploring the Interaction of Personality and Persuasion Tactics in Email Phishing Attacks." *Proceedings of the 20th Congress of the International Ergonomics Association (IEA 2018)*, edited by Sebastiano Bagnara et al., Springer International Publishing, 2019, pp. 401–06, https://doi.org/10.1007/978-3-319-96077-7_42.
- 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. <https://doi.org/10.1016/j.apergo.2020.103084>
- Li, X., Zhang, D., & Wu, B. (2020, June). Detection method of phishing email based on persuasion principle. In *2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)* (Vol. 1, pp. 571-574). IEEE.
- McLean, J. E. (1979). *The Care and Feeding of ANCOVA*.

- Morgan, S. (2020, November 13). Cybercrime To Cost The World \$10.5 Trillion Annually By 2025. *Cybercrime Magazine*. <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>
- Nishikawa, Hiroki, et al. "Analysis of Malicious Email Detection Using Cialdini's Principles." 2020 15th Asia Joint Conference on Information Security (AsiaJCIS), 2020, pp. 137–42, <https://doi.org/10.1109/AsiaJCIS50894.2020.00032>.
- Norman, D. A. (2004). *Emotional Design: Why We Love (or Hate) Everyday Things*. Basic Books.
- Pallant, J. (2011). *Survival manual. A step by step guide to data analysis using SPSS*, 4.
- Parsons, K., Butavicius, M., Delfabbro, P., & Lillie, M. (2019). Predicting susceptibility to social influence in phishing emails. *International Journal of Human-Computer Studies*, 128, 17–26. <https://doi.org/10.1016/j.ijhcs.2019.02.007>
- Pattinson, M., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others? *Information Management & Computer Security*, 20(1), 18–28. <https://doi.org/10.1108/09685221211219173>
- Phumdoung, S. (2004). Inconsistency and ceiling effect in repeated measures of labor pain using VAS. *Songklanagarind Medical Journal*, 22(3), 155-161.
- Sawyer, B. D., Finomore, V. S., Funke, G. J., Mancuso, V. F., Miller, B., Warm, J., & Hancock, P. A. (2015). *Evaluating Cybersecurity Vulnerabilities with the Email Testbed: Effects of Training*. 6.
- Sjouwerman, S. (2020, December 3). *Automated Security Awareness Program | KnowBe4*. Knowbe4. <https://blog.knowbe4.com/knowbe4-fresh-content-updates-from-november-including-a-new-holiday-training-resource-kit>
- Steves, M., Greene, K., & Theofanos, M. (2020). Categorizing human phishing difficulty: A Phish Scale. *Journal of Cybersecurity*, 6(1). <https://doi.org/10.1093/cybsec/tyaa009>

- Stock, J. (2020, August 4). *INTERPOL report shows alarming rate of cyberattacks during COVID-19*. Interpol. <https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19>
- Stojnic, T., Vatsalan, D., & Arachchilage, N. A. (2021). Phishing email strategies: understanding cybercriminals' strategies of crafting phishing emails. *Security and privacy*, 4(5), e165.
- Tanvir, T. (2020). The Relationship Between Social Persuasion Strategies, Phishing Features and Email Exposure Time. 50.
- Tolsdorf, J., & Lo Iacono, L. (2020). Vision: Shred If Insecure – Persuasive Message Design as a Lesson and Alternative to Previous Approaches to Usable Secure Email Interfaces. *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, 172–177. <https://doi.org/10.1109/EuroSPW51379.2020.00031>
- Valecha, Rohit, et al. “Phishing Email Detection Using Persuasion Cues.” *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 2, Mar. 2022, pp. 747–56, <https://doi.org/10.1109/TDSC.2021.3118931>.
- Walker, J. (2014). *Launch: An internet millionaire's secret formula to sell almost anything online, Build a business you love, and live the life of your dreams*. Morgan James Publishing.
- Wickens, T. D. (2002). *Elementary signal detection theory*. Oxford University Press, USA.
- Williams, Emma J., et al. “Exploring Susceptibility to Phishing in the Workplace.” *International Journal of Human-Computer Studies*, vol. 120, Dec. 2018, pp. 1–13, <https://doi.org/10.1016/j.ijhcs.2018.06.004>.
- 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), 184–197. <https://doi.org/10.1080/0144929X.2018.1519599>

Wright, Ryan T., et al. "Research Note—Influence Techniques in Phishing Attacks: An Examination of Vulnerability and Resistance." *Information Systems Research*, vol. 25, no. 2, June 2014, pp. 385–400, <https://doi.org/10.1287/isre.2014.0522>.

Zielinska, Olga A., et al. "A Temporal Analysis of Persuasion Principles in Phishing Emails." *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 60, no. 1, Sept. 2016, pp. 765–69, <https://doi.org/10.1177/1541931213601175>.