

Radboud University



Should we learn from the past or forget what we know about phishing in today's rapidly changing environment?

A study about the influence of phishing cue knowledge on the relationship between human made vs GenAI made spear phishing emails on consumer vulnerability

Master thesis 2025: AI fraud

Name:	Quinten Krekels
Student number:	s1083681
Email:	quinten.krekels@ru.nl
Supervisor:	dr. K. Sidaoui
Second examiner:	I.W.A. Weeterings
Date:	16-06-2025

Abstract

As generative artificial intelligence is becoming increasingly better at generating realistic spear phishing emails, gaining a better understanding of the impact of this on consumer vulnerability is becoming more important than ever.

This study aims to investigate the impact of GenAI made spear phishing emails on consumer vulnerability compared to human made spear phishing emails, while exploring the moderating role of phishing cue knowledge. A between subjects experiment (N=205) was conducted in which participants were tasked to sort a set of emails to determine their detection accuracy. This set of emails contained spear phishing emails either made by humans or by GenAI, depending on what group participants got in. Next to the spear phishing emails, the set also include genuine emails for both groups. After that participants filled in a survey to measure their phishing cue knowledge, fear of online identity theft and conscientiousness. All participants were Dutch and 18 years old or above.

Results showed that GenAI made spear phishing emails caused an increase in consumer vulnerability, compared to human made spear phishing emails. Phishing cue knowledge was not found to moderate this relationship.

These findings contribute to the literature about spear phishing and consumer vulnerability by being among the first to empirically test the impact of GenAI. The findings also show the importance for managers to take action and rethink security measures to account for the increasing dangers of GenAI.

Index

Abstract	2
1. Introduction	5
1.1. Research question	6
1.2. Relevance.....	7
1.2.1. Theoretical relevance	7
1.2.2. Practical relevance.....	7
1.3. Structure.....	8
2. Theoretical background.....	8
2.1. Systematic literature review	8
2.2. Phishing and spear phishing	9
2.3. Generative Artificial Intelligence and spear phishing	10
2.4. Phishing knowledge.....	11
2.5. Hypotheses and conceptual model	12
3. Method	15
3.1. Research strategy	15
3.2. Sampling.....	15
3.3. Operationalization	16
3.3.1. Spear phishing emails.....	16
3.3.2. Measuring consumer vulnerability.....	19
3.3.3. Measuring the independent variables	19
3.4. Procedure	20
3.5. Data analysis.....	20
3.7. Ethics	21
4. Results	22
4.1. Data preparation and cleaning	22
4.1.1. Sample description	23
4.1.2. Attention check	23
4.1.3. Missing data analysis	23
4.2. Confirmatory factor analysis	24
4.3. Reliability analysis	26
4.4. Assumptions	27
4.5. Hypothesis testing.....	28
4.5.1. Control variables	29
4.6. Post hoc analyses	29
5. Discussion	32
5.1. Theoretical contributions	32

5.2. Practical contributions	33
5.3. Limitations.....	35
5.4. Future research	36
5.5. Conclusion	37
References	38
Appendix A: Item list.....	44
Appendix B: Persona.....	46
Appendix C: Analyses.....	48

1. Introduction

With the way that internet-related communication technologies have developed over the years, people engage in online activities at an increasing rate (Yang et al., 2022). This has many benefits like how it improves the financial development on a national level (Yang et al., 2022). However, it also has negative impacts on the individual level by for example the increase in online frauds. Phishing is one of these online frauds that has become one of the most threatening ones with the potential to cause huge financial losses (Yang et al., 2022).

Phishing is defined by Khonji et al. (2013) as “a type of computer attack that communicates socially engineered messages to humans via electronic communication channels in order to persuade them to perform certain actions for the attacker’s benefit” (p. 2092). In most cases this message is sent by email. While traditional phishing concerns a generic message that is easy to spot, today’s phishing mails are better written and employ different techniques to invoke trust (Kävrestad et al., 2022). Furthermore, attackers can make use of a technique called spear phishing. Spear phishing attacks are focused at one recipient and exploit the knowledge of this victim and often their organization to increase the credibility of this message (Burns et al., 2019). This means that they are targeted at just one victim, but they tend to have a higher success rate due to customized messages.

With the increase of online frauds in both scale and impact, this is one the most significant global risks according to the World Economic Forum (WEF) (Schmitt & Flechais, 2024). In the Netherlands it was discovered that one out of six people fell victim to online fraud in 2021, which is about two and a half million people (Akkermans et al., 2023). To counter this problem, Artificial Intelligence (AI) technologies have proven to be effective in detecting phishing attacks. However, AI can also be used to cause even more harm and increase the effectiveness of online frauds (Schmitt & Flechais, 2024). When it comes to social engineering attacks AI can increase the deception capabilities of these messages as these AI systems are becoming increasingly better at mimicking human communication and trust signals (Schmitt & Flechais, 2024). According to Schmitt & Flechais (2024) Generative AI can be used as a tool to increase automation, realism and overall effectiveness in social engineering attacks. Overall, it has been found that AI allows spear phishing mails to be less generic and appear as they have been written by a person (Eze & Shamir, 2024).

The reason why spear phishing attacks are this effective is because they target the people, which are generally seen as the weakest link in a security network (Yang et al., 2022). There are many factors determining consumer susceptibility that have been widely researched

in the literature, and one of these determinants is phishing knowledge (Gan et al., 2024; Sturman et al., 2024). It has been found that phishing knowledge makes people significantly more willing to implement online security management practices (Gan et al., 2024). Phishing knowledge is found to increase the phishing detection but also leads to a bias of classifying real emails as phishing emails (Sturman et al., 2024). Phishing experience is also of importance, as consumers with a higher level of both phishing knowledge and experience have a reduced chance of falling victim to a phishing scam (Yang et al., 2022).

Phishing knowledge has been measured in different ways however, leading to different results (Sturman et al., 2024). Some research focusses on the phishing awareness aspect of phishing knowledge which mainly looks at the risks associated with phishing, instead of objective knowledge that helps people identify phishing emails (Sturman et al., 2024). What is often missing is the knowledge about the email features that characterize phishing emails (Sturman et al., 2024). These features in the email itself are also referred to as cues (Williams et al., 2023). This research will focus on the specific knowledge about phishing related to cues, which will be referred to as phishing cue knowledge. Consumers can protect themselves against phishing scams by having both knowledge about these cues, and experience of past encounters with these cues that give consumers the skills to differentiate phishing emails from genuine emails (Sturman et al., 2024). By gaining a better understanding about the impact of phishing cue knowledge on consumer vulnerability in the context of GenAI made spear phishing emails, a gap in the literature is addressed and managers can gain valuable insights into what countermeasures they should take against this issue.

1.1. Research question

To address this goal this research will try and answer the following research question:

How does phishing cue knowledge influence the relationship between spear phishing email type and consumer vulnerability?

As mentioned before answering this question will contribute to theory by filling in the gap on consumer vulnerability, specifically on the topic of phishing knowledge and experience by looking at the extent into which phishing cue knowledge impacts consumer vulnerability to spear phishing emails made by AI. By answering this question people will gain a better insight into how vulnerable they are against spear phishing, and what they can look further into to protect them from AI made spear phishing emails. With the development of AI there is still a lot undiscovered in the literature, as this new technique may lead to new consequences.

There is already a lot of research on models for detecting phishing emails, and even though these are effective, it is still very important to map what makes consumers vulnerable to phishing (Yang et al., 2022).

1.2. Relevance

1.2.1. Theoretical relevance

This research aims at improving the understanding of consumer vulnerability for spear phishing emails by looking at the influence of phishing cue knowledge as a moderating variable. Existing literature extensively explored several factors influencing phishing vulnerability (Iuga et al., 2016; Yang et al., 2022), yet a clear understanding of the role of phishing cue knowledge is still limited (Sturman et al., 2024). Past research has often focused on broad phishing knowledge as an awareness level (Yang et al., 2022) instead of understanding the specific cues. By building on the cue utilization theory, the role of objective knowledge about these cues can be further explored.

Additionally, while there is an increasing amount of research about the emerging dangers of GenAI in online fraud, there is still a lack of evidence to what extent GenAI increases consumer vulnerability to spear phishing emails. When combining the role of GenAI emails and the impact of phishing cue knowledge on consumer vulnerability a theoretical gap is addressed.

1.2.2. Practical relevance

As Pastor-Galindo et al. (2021) indicated, it is assumed that the internet will be containing an increasing amount of open data of people. This in combination with the increasing effectiveness of AI-based online fraud will become an increasing danger to modern society (Pastor-Galindo et al., 2021). It is therefore needed to find effective countermeasures, and to do this it is necessary to find out what makes consumers susceptible to phishing. Awareness training and simple education is not enough to help consumers against these new online frauds using AI (Schmitt & Flechais, 2024), but teaching people about the new techniques can help consumers recognize these threats. Combining this with new insights into what individuals are at an increased risk of falling victim to these online frauds can be valuable against protecting consumers and companies from their data getting stolen.

1.3. Structure

To be able to answer the research question this paper is structured as follow: first there will be a theoretical background to explore the literature about the important concepts of this paper and the hypothesized effects will be addressed. Next the method of this research will be explained. This is followed by the results in section four. At last section five will contain the discussion.

2. Theoretical background

2.1. Systematic literature review

In order to explore the literature in a systematic way and to discover the existing literature, theories and possible gaps on spear phishing, a systematic literature review was performed. This process was performed in a group for organizing and time saving purposes. To find the relevant literature the following search term was developed: "TS=(phish* OR ((digital OR online OR cyber OR email) NEAR/0 (scam* OR fraud* OR hoax*)) OR cyberscam* OR cyberfraud*)". This search term was put into the Web Of Science Core Collection on January 31, 2025, and gave a total of 4.883 articles. These articles where then filtered based on several criteria. All of the filtering steps taken with corresponding criteria can be seen in figure 1. Figure 1 displays a PRISMA diagram (Mishra & Mishra, 2023) that is created to show the transparent and complete reporting of the systematic literature review. All articles published in a journal with an impact factor lower than 2 were excluded, as this was also done by Ciuchita et al. (2023) to maintain publication quality criteria while also being as inclusive as possible. The impact factor of the journals were found using the Journal Citation Report (Clavariate, 2020). Each article was assessed by two people to maintain the inter-coder reliability. The intercoder reliability was calculated by dividing the instances where both researchers came to the same conclusion by the total number of articles that were assessed. This resulted in a coder reliability of 0.93, which is above the minimum acceptable value of 0.80 (Wilson-Lopez et al., 2019). At the end 263 articles were left to be coded and used as a base for the theoretical perspectives in this paper.

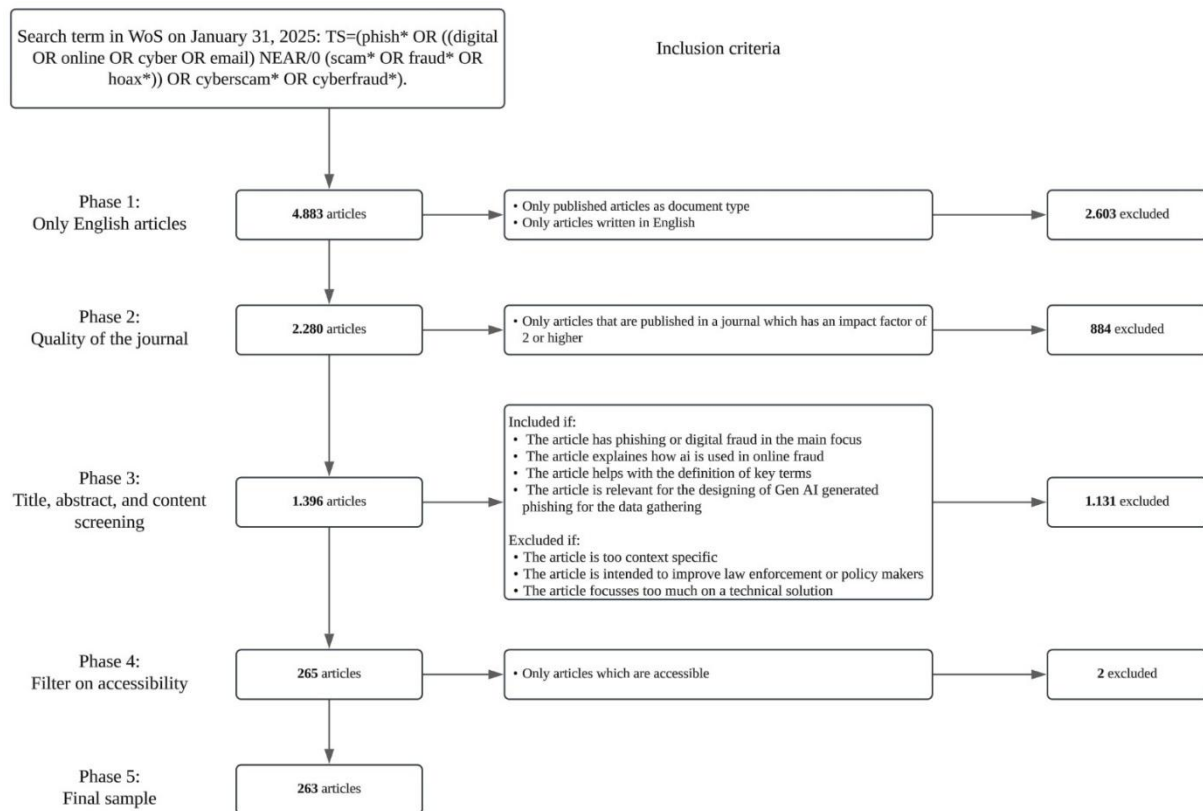


Figure 1: SLR filtering strategy and inclusion criteria in a PRISMA diagram

2.2. Phishing and spear phishing

Phishing can take on multiple forms to achieve different goals, but the underlying idea is always the same however: an attacker attempts to trick the consumer into insecure behavior (Kävrestad et al., 2022). This insecure behavior usually entails clicking on either the malicious attachment, clicking on the fraudulent link or replying to the email with personal information (Gupta et al., 2018). For organizations phishing is a huge problem, as it is the main method used to infiltrate organizations and cause cyber-espionage (Burns et al., 2019). This is usually done by a technique called spear phishing. Spear phishing is characterized by the focus on credibility and specificity of their target, giving them better targeting but also making them cost more resources (Burns et al., 2019). Because of this increased targeting, they are also less scalable since spear phishing campaigns require more resources per victim than normal phishing campaigns (Herley, 2010). This also gives spear phishing attacks a higher success rate, but a narrower success radius (Herley, 2010). To make these emails seem specific and credible, attackers often do research about the victim to make sure that the content of the email is something the victim would normally expect to receive, given their interests or job status (Kävrestad et al., 2022).

2.3. Generative Artificial Intelligence and spear phishing

The rise of ‘advanced open-source generative AI tools’ has shown the progress in machine learning and AI overall (Schmitt & Flechais, 2024). AI powered systems can do various things like automating tasks and analyzing vast amounts of data to gain valuable insights. One of the AI systems in question is Generative Artificial Intelligence (GenAI). According to Schmitt & Flechais (2024), GenAI can be described as the following: “AI models – based on deep learning – designed to generate new content that resembles the input data they have been trained on” (p. 324). GenAI has proven to be capable of creating incredibly realistic content in the form of text, audio and visuals (Schmitt & Flechais, 2024; Neupane et al., 2023). There are however also many concerns that this technology will be used for malicious purposes like spreading false information or creating fake identities (Eze & Shamir, 2024; Neupane et al., 2023).

When it comes to phishing, GenAI is a way for attackers to get around traditional spam detection security measures that look at the same phishing email that was sent to many different targets (Eze & Shamir, 2024). These security measures would recognize the pattern and detect the phishing email (Eze & Shamir, 2024). GenAI however allows attackers to send different emails to different targets, that also all appear to be written by a person and have perfect grammar (Eze & Shamir, 2024). All of this comes with minimal effort, making phishing much more accessible for attackers (Eze & Shamir, 2024). Like this there are various ways in which GenAI can enhance the effectiveness of social engineering attacks including spear phishing (Schmitt & Flechais, 2024). As mentioned GenAI can create realistic content for spear phishing emails. It can even imitate human communication styles (Schmitt & Flechais, 2024). The main threat of GenAI capabilities that Schmitt & Flechais (2024) identified in the context of spear phishing can be classified into three pillars: realistic content creation, advanced targeting and personalization and automated attack infrastructure. Thus GenAI enhances spear phishing campaigns by creating realistic content that can imitate human communication styles, improved targeting of the emails with more personalized messages, and it allows this process to be automated to make it cost far less resources to build these spear phishing emails while also lowering the expertise needed to do so (Eze & Shamir, 2024; Pastor-Galindo et al., 2021; Schmitt & Flechais, 2024).

2.4. Phishing knowledge

Cyber security awareness is a very important concept nowadays and is something that should be a bigger part of national security programs, however this is often still missing making people unaware of certain issues (Alharbi & Tassaddiq, 2021).

The relationship between technical knowledge and phishing vulnerability is not yet completely understood in the literature (Althobaiti, 2021). It has been found however, that experience with phishing and technical knowledge improve consumers' threat perception and anti-phishing behavior (Althobaiti, 2021; Iuga et al., 2016). Focusing on the social engineering online frauds, some studies have looked at software to detect phishing emails, and other studies have looked at consumer vulnerability to educate consumers about cyber security (Althobaiti, 2021). Althobaiti (2021) Also found that the overall phishing awareness was low, leading to a higher phishing vulnerability. Other important factors that influence phishing risks are knowledge and experience related to phishing (Yang et al., 2022). It is found that those with higher levels of knowledge and experience about phishing are less likely to click on links provided in phishing mails (Yang et al., 2022). It also helps people better distinguish between real and phishing emails. One reason why knowledge and experience is effective in detecting phishing emails is because people with higher levels of knowledge and experience know the cues which they should look for (Downs et al., 2006). This specific phishing knowledge and experience is called phishing cue knowledge and entails the objective knowledge about the features that characterize phishing emails that help consumers with identifying these phishing emails (Sturman et al., 2024). Repeated exposure to these cues reinforces them in consumers' long-term memory, which allows for faster and non-conscious recalling when exposed to these cues the next time (Williams et al., 2023). Because of this knowledge and experience with these cues, consumers become better at understanding what cues are relevant and what actions need to be taken in specific situations (Williams et al., 2023). Cues are retained in consumers' long-term memory and the identification of certain features in phishing emails than activates these cues (Sturman et al., 2023). The grouping of multiple cues creates a mental model for consumers, leading to a more comprehensive understanding of the process or event (Morrison et al., 2025). Cue utilization is then the ability to recognize and take appropriate action to the demands of a certain context, by mentally organizing specific cues that are being recalled (Morrison et al., 2025; Sturman et al., 2024; Williams et al., 2023). Consumers with a relatively higher cue utilization should be

able to more accurately classify phishing emails by identifying the present features better (Sturman et al., 2023).

There are many phishing features that consumers use as cues to detect phishing emails, like for example a poor visual presentation, grammar and spelling, a suspicious sender's address, questionable URL links or a warning for urgency and importance (Bayl-Smith et al., 2020; Parsons et al., 2016; Vishwanath et al., 2011). In this research phishing cue knowledge will be assessed by consumer's attention to the sender, grammar and urgency because these are measurable using existing scales from Vishwanath et al. (2011) that have already been validated.

2.5. Hypotheses and conceptual model

Based on the theory some hypothesis are created that will be empirically tested in this research. There is already a vast amount of research about the factors that influence phishing vulnerability, specifically what factors make people more vulnerable to deception (Yang et al., 2022). What is still missing however, is a clear evidence on how GenAI affects consumer vulnerability. Based on the three pillars by Schmitt & Flechais (2024), it is expected that GenAI made spear phishing emails will lead to an increase in consumer vulnerability compared to human made spear phishing emails. This is because GenAI allows the overall process to be more effective and efficient (Schmitt & Flechais, 2024), meaning that it can be applied on a larger scale with less effort. Because of the increased autonomy of AI technologies (Pastor-Galindo et al., 2021) it can be assumed that creating spear phishing messages will become more accessible with the use of AI technologies, and thus become more frequent. The first hypothesis therefore goes as follows:

H1: Spear phishing emails made by GenAI will lead to an increase in consumer vulnerability compared to human made spear phishing emails.

Consumer vulnerability is negatively influenced by phishing knowledge, meaning that consumers with prior knowledge and experience with phishing are less likely to be phished (Yang et al., 2022). This is because phishing knowledge makes consumers aware of certain cues which they utilize to detect phishing emails (Downs et al., 2006). These cues work by recognizing features in the email that people associate with phishing (Sturman et al., 2024). This means that people who rely on cues to detect phishing emails, need those features to be present in order to detect the phishing email. One of the applications of GenAI in creating spear phishing emails is that it allows the message to look like it was written by a person (Eze

& Shamir, 2024). GenAI is also very good at using perfect grammar and spelling according to Eze & Shamir (2024), which causes major problems when relying on those cues. This would lead to the expectation that people with higher levels of phishing cue knowledge are more vulnerable to GenAI made spear phishing emails compared to people with lower levels of phishing cue knowledge. It is therefore expected that phishing cue knowledge acts as a moderator on the relationship between email type and consumer vulnerability, leading to the following hypothesis:

H2: Phishing cue knowledge moderates the relationship between email type and consumer vulnerability.

Control variables

Fear of online identity theft

One of the fraudulent purposes of phishing emails is for fraudsters to commit online identity theft (Guedes et al., 2022). Online Identity theft is defined by Guedes et al. (2022) as “the illicit and improperly use, via internet, of the personal and financial data which was obtained without prior consent and knowledge by the cyber-criminal.” Online identity theft has been recognized as a public health problem while being one of the fastest growing and most feared crimes (Burnes et al., 2020).

Various studies have explored the relationship between fear of online identity theft and the technical skills on the internet related to online crime (Abdulai, 2020; Virtanen, 2017), this led to varying results however. It is therefore relevant to test the effects of fear of online identity theft on consumer vulnerability by assessing how this affects the overall research model. The study of Guedes et al. (2022) also found that individuals with higher levels of fear of online identity theft, adopted more avoiding behaviours. This leads to the expectation that individuals with higher levels of fear of online identity theft are also less vulnerable to spear phishing, given that they avoid online activity more than people with lower levels of fear of online identity theft.

Conscientiousness

Consumers with lower conscientiousness are more vulnerable to phishing attacks and are more prone to become a victim of cybercrime (Williams et al., 2023). This is because they are more vulnerable to social persuasion strategies, which are present in phishing (Williams et al., 2023). Conscientiousness is one of the big five personality traits and is found to be the most consistent predictor of behaviour and intention (Conner & Abraham, 2001).

Conscientiousness is explained by Williams et al. (2023) to be associated with self regulation, persistence, reliability and individual differences in information processing and decision making styles. It is also expected that higher conscientiousness protects consumers from phishing by reducing impulsivity (Williams et al., 2023). It is therefore expected that conscientiousness will have an impact on consumer vulnerability and the way that consumers deal with phishing cues, due to the different decision making.

Age

Prior research about phishing vulnerability has indicated that age is a predictor for consumer vulnerability (Yang et al., 2022). According to Darwish et al. (2012) age linearly predicts phishing vulnerability, where younger people are more vulnerable compared to older people. Among consumers with higher digital literacy, older people where also less likely to fall victim to a phishing scam compared to younger people (Darwish et al., 2012). This could potentially be explained by older people having more experience and knowledge about phishing cues compared to younger people. It is therefore expected that age will effect the main effect of this study. The relationships and variables discussed above can be seen in the conceptual model in figure 2.

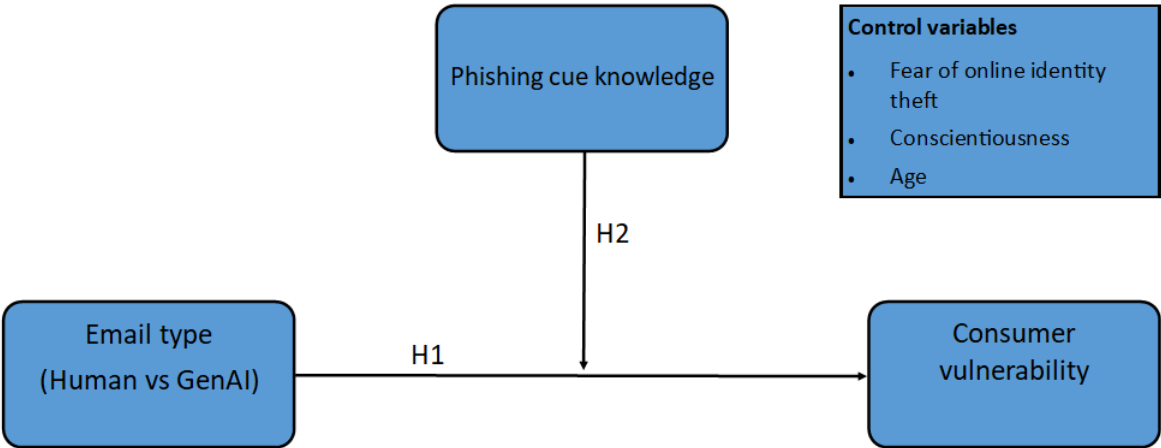


Figure 2: Conceptual model

3. Method

3.1. Research strategy

To answer the central question in this research, a between subjects experiment is conducted. This design was chosen because it allows to compare two groups with different manipulations from the independent variable on their scores on the dependent variable, while also being able to explore the effect of a moderation effect in the form of an individual characteristic. This is based on the study from Zhou et al. (2022), which also employed a between subjects experiment in the context of phishing and consumer vulnerability.

In order to reach a bigger audience and gather more participants, this experiment will be conducted online using the application Qualtrics (*Qualtrics XM*, z.d.).

When conducting an experiment about spear phishing vulnerability it is crucial to work with a fictional persona to replicate the target context (Xu et al., 2023). When creating this fictional persona there are four information types that need to be provided which are primary, personal, professional and interests' information (Xu et al., 2023). The description of the persona given to the participants can be seen in appendix B. In order to measure the consumer vulnerability in Qualtrics (*Qualtrics XM*, z.d.), participants will be equally divided into one of the two email type groups. The participants will then be shown a series of emails after which they have to answer a question after each email.

3.2. Sampling

Since the experiment will be conducted online and therefore spread by a link that the researchers will share, the sampling technique which will mostly be used is convenience sampling. This technique is overall easier, and more cost-effective than the preferred technique which is random sample (Vennix, 2019). With random sampling every element of the population has an equal chance of being in the sample (Vennix, 2019). Since convenience sampling will be used the external validity will be lower compared to the use of random sampling. Convenience sampling does however allow for better participant gathering in the limited timeframe under which this research will be conducted. The population under which this sampling will be performed are Dutch citizens with the age of eighteen or above.

3.3. Operationalization

To measure the concept phishing vulnerability participants are split into two different groups that both get a different manipulation to test the differences between human made spear phishing emails and AI made spear phishing emails. In order to be able to test for the phishing cue knowledge, each email contains one phishing cue from one of the three dimensions: sender, grammar or urgency. This also allows participants to spot phishing emails, as without these cues the phishing emails would not differ much from the genuine emails. It is also of importance that the experiment will seem as natural as possible when measuring human behaviour in order to get the best results (King et al., 2013).

3.3.1. Spear phishing emails

Both groups of email type contained seven spear phishing emails and seven genuine emails. A total of 14 emails with a equal ratio is in line with prior research about this topic (Parsons et al., 2019). The reason for this ratio is that it would not be possible to use the real average ratio, as this would lead to such a small amount of spear phishing emails that it becomes impossible to measure the consumer vulnerability without creating a burden to participants (Canfield et al., 2016). Every email was put into a newly created fake email application, to make sure that this was equally unfamiliar for all the participants. This was meant to prevent certain biases, while also keeping it realistic as it seemed like a normal email inbox.

To create the AI made spear phishing emails the latest accessible model of Chat gpt was used: GPT-4o (*ChatGPT*, z.d.). The AI was first fed with all the information about the fictional personal to assure that the spear phishing email was personalized. After that a series of prompts was given to create the emails, each with a different cue. An example of a translated used prompt with the corresponding email can be seen below and in figure 3.

Example prompt used: *Make a new spear phishing email with the sender being XXL nutrition. Make it that the content contains approximately 100 words. The only phishing cue that is meant to be present in this email is a typographical error in the content of the email, and not in the subject or the sender of the email. These are supposed to be spelled correctly.*

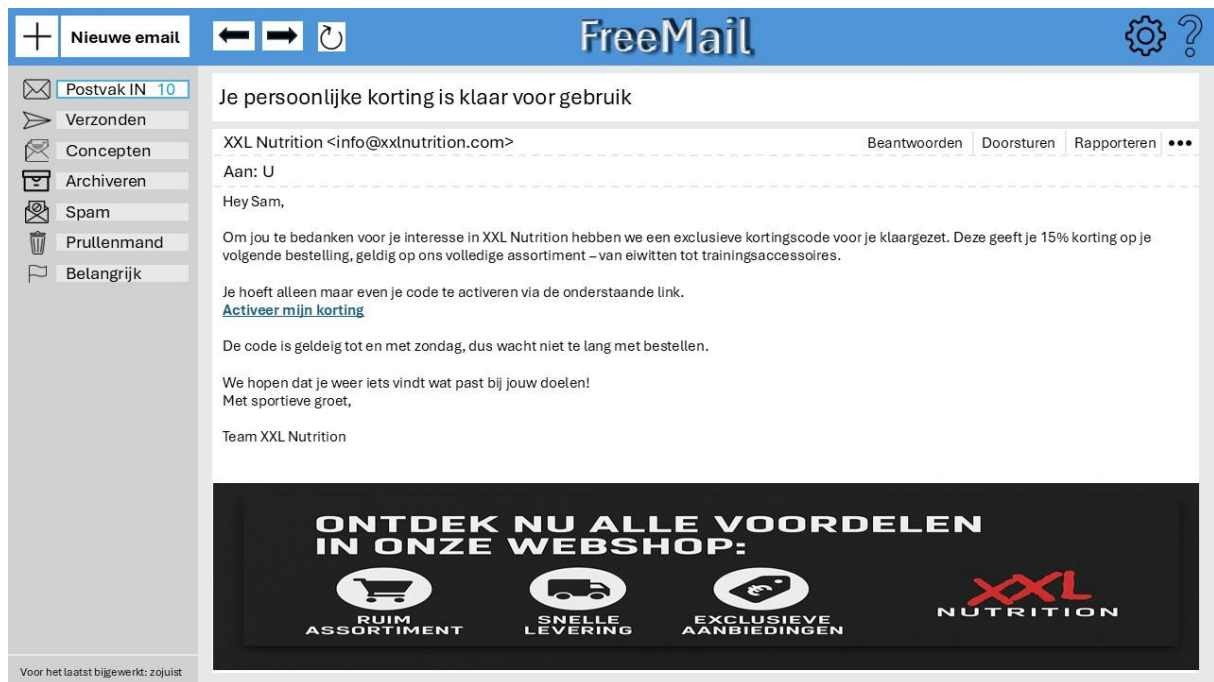


Figure 3: Example of a GenAI made email used in the experiment

The human made spear phishing emails were created using the V-trait model in line with the research of (Heiding et al., 2024). The V-trait model consists of three pillars that are used to decrease the suspicion to humans: credibility, compatibility and customizability. These pillars have been used with the information about the fictional persona to create the spear phishing emails. An example of a human made spear phishing email used in the experiment is depicted in figure 4.

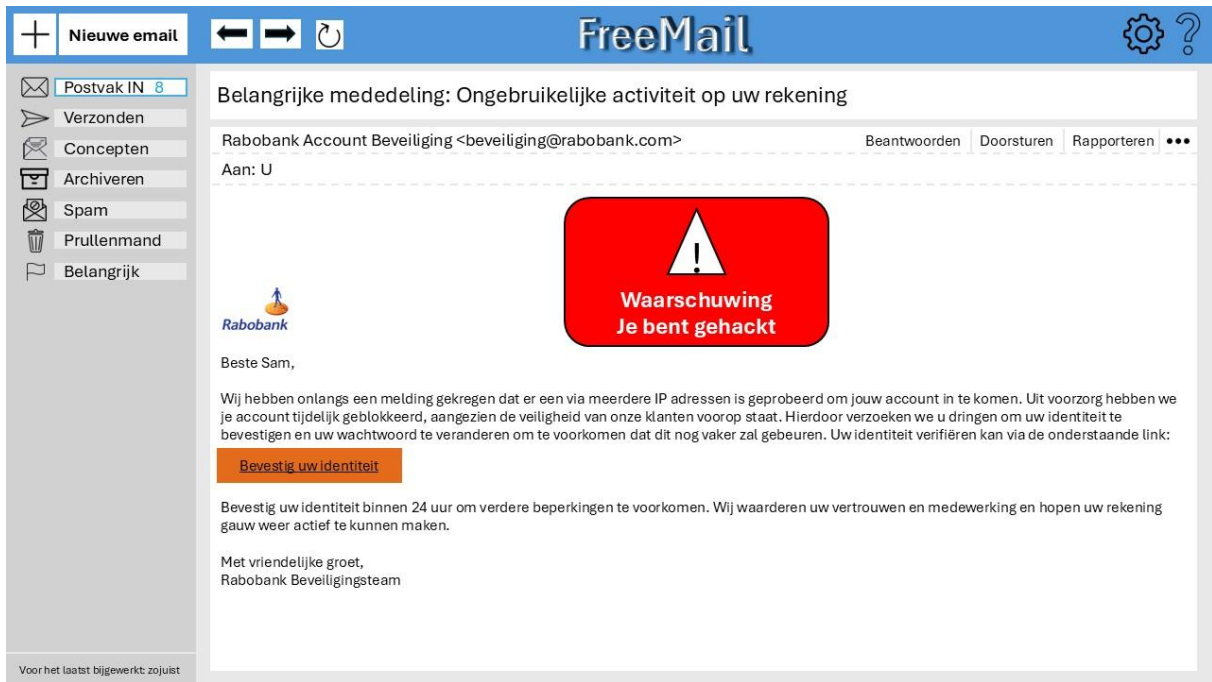


Figure 4: Example of a Human made email used in the experiment

The genuine emails were all based of actual genuine emails received by the authors. This is in line with the research of (Parsons et al., 2019). An example is seen in figure 5.

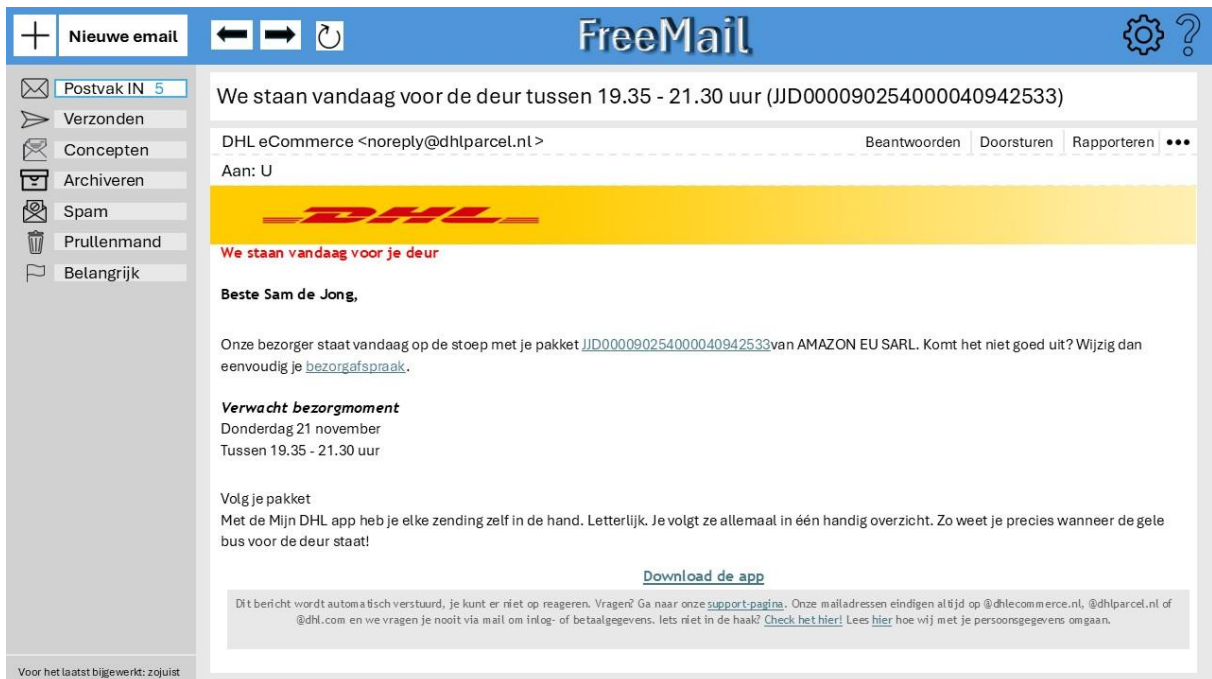


Figure 5: Example of a genuine email used in the experiment

3.3.2. Measuring consumer vulnerability

To measure consumer vulnerability, participants got seven answer options after each email they were shown: “reply”, “download attachment”, “click on link”, “investigate further”, “report”, “delete” and “ignore”. These options are derived from prior research about phishing and consumer vulnerability (Sarno et al., 2023). To determine the consumer vulnerability the phishing detection accuracy is calculated by dividing the amount of correctly classified phishing emails by the amount of total phishing emails, which was seven. This ratio represents the phishing detection accuracy derived from prior research (Lawson et al., 2020).

3.3.3. Measuring the independent variables

The independent variables are measured using a survey at the end of the experiment. In order to measure phishing cue knowledge, eight items are used that are all adapted from the study by Vishwanath et al. (2011). The items are fit to the context of this research, and they are made measurable on a 7-point Likert scale

To measure the control variable fear of identity theft the scale used in the research by Guedes et al. (2022) will be adapted to the context of this research. This scale consists of three items which will be measured on a 7-point Likert scale.

The control variable conscientiousness will be measured using the Mini-IPIP Scale from Donnellan et al. (2006), which consists of four items that will be measured on a 7-point Likert scale. The second and fourth item of this scale are reversed to give them the same direction as the other questions in the survey. This is done to prevent confusion to the participants and to increase the chance of getting better data.

All items measured on a 7-point Likert scale use the same rating where the scores 1-7 go from “I completely disagree” to ‘I completely agree’.

To measure the control variable age participants have to fill in their age in numbers. All the items that belong to the scales can be found in appendix A.

Main model	Measurement	Measurement level	Supportive literature
Consumer vulnerability	One item after every email containing the seven options	Nominal	(Sarno et al., 2023)

Phishing cue knowledge	8 items on a 7-point Likert scale	Interval	(Vishwanath et al., 2011)
Control variables			
Age	Participant age in number	Interval	-
Fear of online identity theft	3 items on a 7-point Likert scale	Interval	(Guedes et al., 2022)
Conscientiousness	4 items on a 7-point Likert scale	Interval	(Donnellan et al., 2006)

Table 1: Operationalization of the variables.

3.4. Procedure

The process which the participants went through during the experiment was as follows: first the participants got onto the online platform where they got equally divided into one of the two email type groups. They then had to give consent into participating and they received general instructions about what is being expected from them. They also had to fill in their age. After this they got information about the persona which they had to pretend to be. Next was the set of emails, where below every email there was question about what action they take after reading that email. After the last email a survey was presented which they had to fill in. At the end participants were consulted on the actual intention of this experiment, which was testing their spear phishing vulnerability. This was followed by a second time of asking for consent and a question about saving their answers to be used for the purposes of this research.

3.5. Data analysis

Given that the dependent variable is measured on a metric scale, the independent variable on a categorical scale (with two categories) and the other predicting variables also on a metric scale the best suited statistical test is a regression analysis (Field, 2017; Hair et al., 2019). In terms of the sample size more is always better (Field, 2017). It would be enough however to get a minimum of 15 respondents for every predicting variable (Field, 2017).

First the data was cleaned and prepared in order to be used in the analysis. After that a missing data analysis was conducted to test if the missing data was completely at random (MCAR). This is all done in SPSS Statistics (IBM SPSS Statistics 27, n.d.). After that the measurement model is examined. To examine the measurement model, a confirmatory factor analysis (CFA) was conducted. This is done to test to what extent a prespecified measurement

theory existing of measured variables and items fits with reality as captured by the data (Hair et al., 2019). The software used for this is ADANCO (ADANCO, n.d.). Following the CFA a reliability analysis was performed to test the multi-item scales for their reliability.

After that the data was tested for any violations of the assumptions relevant to multiple regression analyses. These include: outliers, multicollinearity, linearity of the phenomenon measured, constant variance of the error terms, normality of the error term distribution and independence of the error terms (Hair et al., 2019; Pallant, 2001).

Because this research examines a moderating effect, PROCESS model 1 version 4.2 (Hayes, 2022) is used to analyse the data. PROCESS (Hayes, 2022) is a macro for SPSS Statistics (IBM SPSS Statistics 27, n.d.) that has some advantages over a normal regression analysis because it centres predictors automatically, it can correct for heteroscedastic data and it computes the interaction term automatically (Field, 2017).

3.7. Ethics

Within this experimental research there are some ethical considerations that have to be taken into account. The Radboud University has two forms of assessing research on ethics. There is a light track and a full track (*Ethical Review Committee for Law and Management Sciences (ETRM) / Radboud University, n.d.*). This research will fall into the light track which requires some conditions to be met (*Radboud University, n.d.-a*). These are the following conditions:

1. Participants are healthy, capable, older than 16, do not belong to a vulnerable group and participate voluntarily in the research.
2. The participants are informed by means of an informed consent.
3. The privacy of the participants is guaranteed.
4. The research is not invasive, intensive and has minimal risks.
5. The research takes place within Europe or in an online environment.

To ensure that all of these conditions are met the following actions have been taken. First of, participants had to be older than 18 in order to participate in the experiment, and the very first question they had to fill in was to give permission for their participation. They were informed beforehand what the estimated time would be to finish the experiment, alongside with the fact that they could quit at any given moment. The privacy was guaranteed by not collecting any personal data other than age, education and gender. The data was anonymized and stored securely according to the AVG law by storing it in an environment from the Radboud University that is protected. This is needed to follow the AVG law (*Privacy &*

Informatieveiligheid / Radboud Universiteit, n.d.; Personal Data Protection Regulation / Radboud University, 2024).

Additionally, the data is only used for the purpose of this research and is therefore also not shared with external parties. The experiment itself did not cause any harm to participants in any way and the used phishing emails were fake and could not cause any data breaches. To further minimize the burden for participants, the experiment is conducted online. When the experiment was finished participants received a debrief with the actual intentions of the research and a final question about giving consent one more time. This is necessary since the actual purpose of the experiment is not revealed before starting the experiment.

As a researcher ethical standards have also been taken into account. All information gathered from external sources has been accurately represented while referring to the author. This is done to ensure transparency towards the information presented and give credibility to the original author(s). The data collected has also been presented accurately without manipulating results or including biases in order to represent the researched sample objectively. This is done by indicating every step taken while preparing and analyzing the data.

4. Results

4.1. Data preparation and cleaning

After the sampling a total of 205 responses were collected in a timeframe of two weeks. Three replies came from the preview and are therefore deleted. Four respondents answered the first question by filling in that they did not want to participate in the experiment and are therefore also deleted. At the end of the experiment after explaining to the respondents that the research was actually about spear phishing two respondents indicated that they no longer wanted to be part of the research, and therefore their data was also deleted. Five respondent failed to fill in any of the items that belonged a construct, and are therefore also deleted to increase the validity. According to Hair et al. (2019) this is missing data at the construct-level, and not addressing this would be impactful on the results through its actions at the construct level.

4.1.1. Sample description

Cleaning the data lead to a total of 191 respondents, of which 94 were in the human made email group and 97 in the AI made email group. The average age was 33.6, with most participants being 26 or younger. This was expected due to the sampling method. 91 of the participants were male, 98 female and 1 participant preferred not to share their gender. The most frequent educational level is HBO-, WO bachelor (the Dutch equivalents of higher professional education bachelors degree and university education bachelors degree) with 79 cases. This makes up for 41.4% and was also expected to be high.

4.1.2. Attention check

After deleting the cases that were invalid, the attention checks need to be taken into account. During the experiment three attention checks were performed to test whether participants got manipulated correctly and actively paid attention to the questions in the experiment. This was necessary to test the spear phishing concept using a fictional persona. After looking at the results, 157 (82.8%) respondents got all three manipulation checks right. Since the sample size after deleting all the cases with one or more incorrect attention check is still sufficient to perform the analysis ($n=157$), the decision is made to delete those cases to increase both the validity and the reliability.

4.1.3. Missing data analysis

After this a missing data analysis was performed. This had to be done once for both the groups of email types because both groups have ignorable missing data that is part of the research design. In both groups the missing data is less than 2% for every variable, with almost all of the variables having no missing data. This is generally acceptable since it is <10%, and therefore the data is amenable to any imputation strategy (Hair et al., 2019). To test whether the missing values are completely random (MCAR), the Little's MCAR test has been conducted for both groups. Both groups have a nonsignificant result for the Little's MCAR test with group 1 and group 2 scoring respectively $\chi^2(56) = 48.166$; $p = .762$ and $\chi^2(28) = 40.339$; $p = .062$. This is an indication that the missing data is MCAR.

The imputation strategy used for the independent metric variables is Mean substitution, replacing the missing values with the best single replacement value which is the mean of the other items in that same scale (Hair et al., 2019). The missing item on the scale

for the dependent categorical variable was deleted. After all of these changes the data set is left with a total of 156 cases, of which 74 in group 1 and 82 in group 2.

4.2. Confirmatory factor analysis

To examine the measurement model, a CFA was conducted for the three multi item variables: phishing cue knowledge, conscientiousness and fear of online identity theft. After this the structural model can be assessed using multiple regression analysis. More results of the CFA can be found in appendix C.

First the overall model fit was assessed using the standardized root mean square residual (SRMR). A SRMR value less than 0.05 indicates a good model fit, but the cut-off value is 0.08 (Henseler et al., 2016). Initially the SRMR score is 0.0882, which is not sufficient and indicates that the measurement model needed to be improved.

After that the construct reliability was assessed for all three constructs using Dijkstra-Henseler's rho (ρ_A), Jöreskog's rho (ρ_c) and Cronbach's alpha (α) which all have a threshold of 0.7 (Henseler et al., 2016). This was met by all constructs by having a value of > 0.7 on all three measures.

Next the convergent validity was tested using the Average variance extracted (AVE). An AVE of 0.5 or higher is regarded as acceptable and shows that the construct is unidimensional (Henseler et al., 2016). The AVE for both phishing cue knowledge and conscientiousness is not sufficient with values of 0.3200 and 0.4494 respectively. Fear of online identity theft had a sufficient AVE with a value of 0.6604.

After several iterations of deleting items to increase the model fit and the AVE, the items PCK_1, PCK_3, PCK_6, PCK_7 and PCK_8 from the scale of phishing cue knowledge have been deleted due to their low loadings and low indicator reliability. This significantly increases the AVE of phishing cue knowledge to 0.5695. The construct conscientiousness could not be improved with the deletion of an item.

Phishing cue knowledge has now been sufficiently improved in its convergent validity. The model fit has also been improved with the SRMR being 0.0583, which is below the threshold of 0.08 (table 2). After the deletion of these items the construct reliability is good, with all constructs having a value of > 0.7 on all three measures. Then the discriminant validity was tested to see if each factor that measures a concept that is theoretically different, is also statistically different (Henseler et al., 2016). This is first assessed by the Fornell-Larcker criterion which says that the AVE should be higher than the squared correlations with all the

other factors in the model, and the HTMT which should be smaller than one (Henseler et al., 2016). This was the case for all constructs. Discriminant validity also includes that individual items should only represent one latent construct (Hair et al., 2019). This means that there can be no cross-loadings. This is not the case.

At the end, after deleting five items from the scale of phishing cue knowledge the measurement model is significantly improved. The measurement model now meets the criteria and has increased in validity. Conscientiousness however still has an insufficient convergent validity, but due to the AVE just being below the threshold and the construct reliability being good, the decision is made to keep this as the final measurement model. A summary of the CFA on the final measurement model can be seen in table 2. The loadings are displayed in table 3.

Assessment	Construct	Result
Model fit (saturated model)	-	SRMR = 0.0583 / < 95% bootstrap quantile (HI95 of SRMR) $d_{ULS} < 95\%$ bootstrap quantile $d_G < 99\%$ bootstrap quantile
Construct reliability	Conscientiousness	> 0.7 on all three measures
	Fear of online identity theft	> 0.7 on all three measures
	Phishing cue knowledge	> 0.7 on all three measures
Convergent validity	Conscientiousness	AVE = 0.4494
	Fear of online identity theft	AVE = 0.6604
	Phishing cue knowledge	AVE = 0.5695
HTMT	-	All > 1
Fornell-Larcker criterion	-	All < corresponding AVE
Cross-loaders	-	No cross-loaders spotted

Table 2: Summary of the final measurement model

Construct	Item	Loadings
Conscientiousness	1	0.6196
	2	0.7298
	3	0.6750
	4	0.6522
Fear of online identity theft	1	0.8436
	2	0.8523
	3	0.7370
Phishing cue knowledge	2	0.5762
	4	0.8344
	5	0.8247

Table 3: Item loadings

4.3. Reliability analysis

To assess the reliability the Cronbach's Alpha will be used, where a score of 0.8 or higher is good but 0.7 is enough (Field, 2017). The scale for phishing cue knowledge shows a sufficient Cronbach's Alpha ($\alpha = .78$) and is therefore reliable. When deleting the item PCK_2 the Cronbach's Alpha would increase ($\alpha = .91$), but this would lead to the scale only having two items and also losing an important theoretical meaning of the scale. Because of this and the fact that the scale is already considered reliable with this Cronbach's Alpha (Pallant, 2001), PCK_2 is not deleted.

The scales of the control variables have also been tested for their reliability. Conscientiousness showed a sufficient reliability ($\alpha = .76$). Fear of online identity theft showed a good reliability ($\alpha = .85$). These results can all be seen in appendix B.

Now that the scales are validated, the total scores for each of the multi-item variables was calculated with summated scales. For the dependent variable consumer vulnerability the detection accuracy was determined.

4.4. Assumptions

When looking at the box plots the variables phishing cue knowledge and detection accuracy have potential outliers. However, when comparing the mean values with the 5% trimmed mean values the differences are very small, which can be seen in table 4. This indicates that these potential outliers do not exert a big influence on the mean scores (Pallant, 2001). When looking at Cook's distance there is no case with a value greater than 1, and therefore no case has too much overall influence on the model (Field, 2017).

The multicollinearity is assessed by looking at the VIF and tolerance statistics for every independent variable. The Tolerance should not be below 0.2 and the VIF should not be greater than 10 (Field, 2017). The tolerance is very close to 1.0 for every variable, while the VIF is below 1.1 for every variable. This indicates that the assumption of multicollinearity is not violated. The results are depicted in table 5.

To test for violations of linearity of the phenomenon measured, the residual plot was studied. This plot does not show a clear violation of the linearity. Therefore this assumption is not violated.

Constant variance of the error term, or homoscedasticity, is the opposite of heteroscedasticity. When looking at the variance plot from before the data seems to be slightly heteroscedastic. This can be seen by the funnel like shape in the plot. To counter this, PROCESS model 1 (Hayes, 2022) has a build in feature to deal with heteroscedastic data: HC3.0. By using this feature the violation of this assumption can be mitigated.

Normality of the error terms is checked by looking at the normal P-P plot. If the distribution is normal, the standardized residuals line should closely follow the normal distribution line (Hair et al., 2019). This is the case for the data and therefore this assumption is not violated.

To assess whether the assumption independence of error terms is violated, the residual plots are assessed once again. This shows no reason to suspect that this assumption is violated. When looking at the individual plots from each variable, email type seems to be violating this. This pattern shows when basic model conditions change which are not included into the model (Hair et al., 2019). This is to be expected since the respondents got different sets of emails, depending on which group they were in. To further assess this assumption the Durbin-Watson test is used for detecting autocorrelation. The value was 1.5, indicating that there was a positive correlation, but no cause for concern since the value is between 1 and 3 (Field, 2017). Therefore residuals were independent and the assumption was met.

Construct	Mean	5% trimmed mean
Detection accuracy	0.71	0.72
Phishing cue knowledge	6.09	6.19
Fear of online identity theft	3.91	3.92
Conscientiousness	4.51	4.52

Table 4: Compared means

Predictor	Tolerance	VIF
Email type	.982	1.018
Phishing cue knowledge	.927	1.079
Fear of online identity theft	.982	1.018
Conscientiousness	.949	1.054
Age	.904	1.106

Table 5: Tolerance and VIF

4.5. Hypothesis testing

H1 and H2 were tested using PROCESS model 1 (Hayes, 2022) to test the effect of email type on consumer vulnerability. Email type was dummy-coded with 0 = Human made and 1 = AI made. For the analysis a confidence level of 95% is maintained as a threshold.

The overall model was statistically significant with $R^2 = .112$, $F(6,149) = 2.44$, $p = .028$. This indicates that 11.2% of the variance in consumer vulnerability was explained in this model.

To test H1 the effect of email type on detection accuracy was tested. This effect was statistically significant with $b = -.067$, $p = .049$. Email type therefore significantly predicted consumer vulnerability in this sample, supporting H1.

H2 was tested by assessing the interaction effect of email type and phishing cue knowledge on detection accuracy. This interaction effect was not significant, $b = .016$, $p = .721$. This indicates that phishing cue knowledge does not statistically significant moderate the effect of email type on consumer vulnerability and therefore H2 is not supported.

The direct effect of phishing cue knowledge on detection accuracy was also tested and showed to be nonsignificant: $b = .036$, $p = .261$. These results are found in table 6.

4.5.1. Control variables

As mentioned before the control variables have been incorporated into the models to test their influence. The results can be found in table 6. The effect of conscientiousness was not significant with $b = -.014$, $p = .352$. Fear of online identity theft also did not have a significant effect on detection accuracy with $b = .011$, $p = .362$. The only control variable with a statistically significant effect in this model was age with the following score: $b = .0028$, $p = .0231$. This means that with the increase of age, the detection accuracy increases slightly, and thus older people turned out to be slightly less vulnerable to spear phishing in this sample.

Predictor	b	SE	t	p
Email type	-.6783	.0338	-1.9841	.0491
Phishing cue knowledge	.0358	.0317	1.1283	.2610
Interaction effect	.0156	.0437	.3577	.7211
Age	.0028	.0012	2.2952	.0231
Fear of online identity theft	.0113	.0123	.9147	.3618
Conscientiousness	-.0143	.0153	-.9338	.3519

Table 6: Results main analysis

4.6. Post hoc analyses

To further explore the data post hoc analyses were conducted. Even though the moderating effect of phishing cue knowledge on detection accuracy was not significant, a chart has been made to visualize the interaction between phishing cue knowledge and email type. This can be seen in figure 6. In this figure it is shown that GenAI made emails lead to a lower detection accuracy compared to human made emails, and that a higher level of phishing cue knowledge makes the detection accuracy go up for both email type groups. This can however not be interpreted since this effect was not significant.

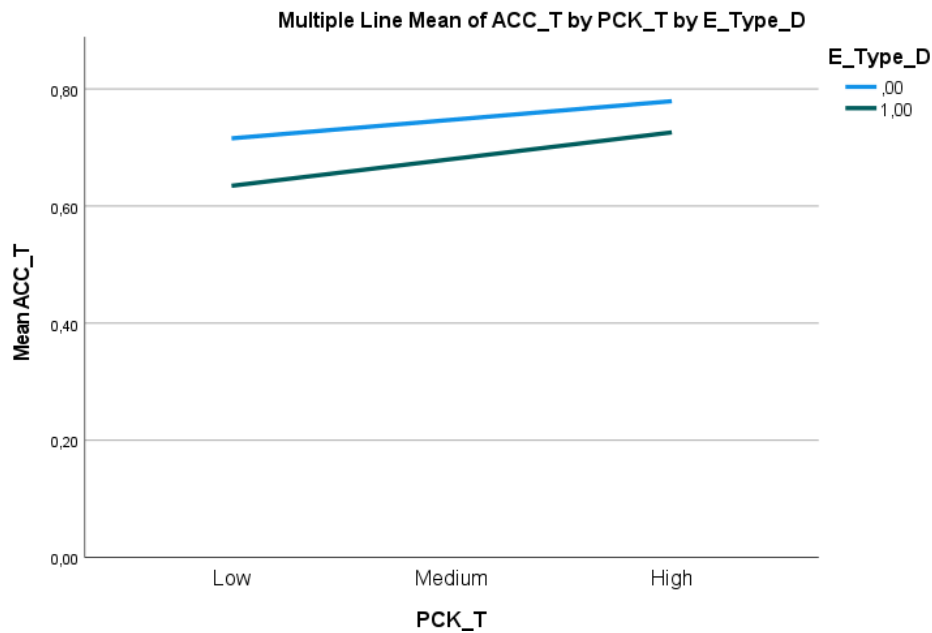


Figure 6: Visualization of the interaction term

After that PROCESS model 1 (Hayes, 2022) was used to test if age moderates the relationship between email type and consumer vulnerability while controlling for phishing cue knowledge, conscientiousness and fear of online identity theft. The overall model was statistically significant: $R^2 = .112$, $F(6,149) = 2.57$, $p = .021$. In this model email type significantly predicted detection accuracy, $b = -.067$, $p = .048$. When using age as a moderator the interaction effect was not significant, $b = .0013$, $p = .614$. The main effect of age on detection accuracy was also not significant: $b = .0022$, $p = .233$.

Interestingly, in this model phishing cue knowledge had a statistically significant effect as a predictor on detection accuracy: $b = .044$, $p = .041$. This analysis showed that both phishing cue knowledge and age can act as a predictor for detection accuracy, but not as a moderator. The results are shown in table 7 below.

Predictor	b	SE	t	p
Email type	-.0672	.0337	-1.9913	.0483
Age	.0022	.0018	1.1987	.2326
Interaction effect	.0013	.0025	.5060	.6136
Fear of online identity theft	.0106	.0125	.8467	.3985
Conscientiousness	-.0138	.0154	-.8985	.3704
Phishing cue knowledge	.0438	.0212	2.0637	.0408

Table 7: Results post hoc analysis with age as moderator

To further assess the relationship between phishing cue knowledge and detection accuracy, a simple regression analysis has been performed with email type as the independent variable and phishing cue knowledge, conscientiousness, fear of online identity theft and age as control variables. The overall model was statistically significant, $R^2 = .111$, $F(5,150) = 3.73$, $p = .003$. In this model without moderation 11.1% of the variance of detection accuracy is explained, and email type significantly predicted detection accuracy: $b = -.067$, $p = .044$. Next to email type, both phishing cue knowledge and age had a significant effect on detection accuracy with the scores $b = .043$, $p = .026$ and $b = .003$, $p = .032$ respectively. All together, H1 being accepted is supported over multiple models while phishing cue knowledge is only found to be significant as a main effect instead of a moderator. Age was also consistently significant as a covariate.

Predictor	b	SE	t	p
Email type	-.067	.033	-2.027	.044
Phishing cue knowledge	.043	.019	2.245	.026
Age	.003	.001	2.162	.032
Fear of online identity theft	.011	.011	.982	.328
Conscientiousness	-.014	.015	-.923	.358

Table 8: Results post hoc simple regression analysis

After testing the hypotheses the results showed that only H1 was accepted. A summary of these results is shown in table 9 below.

Hypothesis	Accepted	p value
H1	Yes	.049
H2	No	.721

Table 9: Summary results analysis

5. Discussion

This research has developed and tested a theory to discover the influence of GenAI on consumer vulnerability to spear phishing emails, compared to human made spear phishing emails. The expectations of this research were that GenAI made emails would lead to an increase in vulnerability compared to human made emails, and that phishing cue knowledge would moderate this relationship. This was tested using an in between subjects experiment, conducted online. The results showed two main conclusions: (1) email type did have an effect on consumer vulnerability. It showed that consumers were more vulnerable to GenAI made spear phishing emails compared to human made spear phishing emails in this sample. (2) In this sample it could not be proven that phishing cue knowledge moderates the relationship between email type and consumer vulnerability due to nonsignificant results. The data therefore only partially supports the predefined hypotheses.

5.1. Theoretical contributions

This study makes several contributions to the literature by being among the first to discover the impact of GenAI made spear phishing emails on consumer vulnerability.

First, H1 was accepted and participants showed to be more vulnerable to GenAI made spear phishing emails compared to human made spear phishing emails. This effect was robust as it stayed significant during the post hoc analyses with different models using the same variables. This is in line with the expectations in existing theory, that expected GenAI to enhance spear phishing campaigns by making them more realistic and personalised and thus more effective (Eze & Shamir, 2024; Pastor-Galindo et al., 2021; Schmitt & Flechais, 2024). The acceptance of H1 therefore contributes to theory by empirically testing this expectation and finding this effect in the setting of this research.

Second, the findings of this study contradict prior findings by Heiding et al. (2024), where the findings indicated that human made emails and GenAI made emails achieved the same click-through rate. These different findings could be explained by the difference in operationalizing consumer vulnerability and thus a different way of measuring this. This study uses detection accuracy to measure consumer vulnerability compared to the click-through rate used by Heiding et al. (2024), showing the impact of the measurement method used.

H2 was not accepted and therefore it could not be proven that phishing cue knowledge moderates the relationship between email type and consumer vulnerability in this study. The

third contribution is therefore adding insights into the relationship between technical knowledge and vulnerability which is still evolving and not yet completely understood in the literature (Althobaiti, 2021). Because no results were found for H2, post hoc analyses have been performed. The interaction figure showed that phishing cue knowledge slightly moderates the main effect of email type on consumer vulnerability, suggesting a potential moderation effect under alternative conditions. This requires more research with a different design.

Fourth, phishing cue knowledge has a direct effect on consumer vulnerability. In further post hoc analyses the relationship between phishing cue knowledge, only as a direct effect, and consumer vulnerability showed to be significant and thus it was found that higher levels of phishing cue knowledge lead to lower consumer vulnerability by increasing the detection accuracy. This is in line with existing literature indicating that general knowledge and experience with phishing is related to lower consumer vulnerability and a higher detection accuracy for human generated phishing emails (Downs et al., 2006; Yang et al., 2022). This study contributes to this theory by looking at the relationship between the specific knowledge about the phishing cues that consumers use to recognize phishing emails, and consumer vulnerability. Unlike prior research focusing solely on human made emails (Sturman et al., 2023), GenAI made emails are also taken into the context of this study. This contribution also supports theory about cue utilization, which stated that consumers with higher cue utilization should be able to more accurately classify phishing emails by recognizing certain features better (Bayl-Smith et al., 2020; Williams et al., 2023).

The final contribution to theory is the incorporation of the factor age in a study about the influence of GenAI on consumer vulnerability. It was found that older people are less vulnerable to spear phishing emails compared to younger people, which is in line with existing research (Darwish et al., 2012). In further post hoc analysis age was not found to be a moderator and thus age was not found to make a difference in consumer vulnerability between two email type groups. This is a new insight about demographics in GenAI made phishing emails and consumer vulnerability which remains underexplored in the literature.

5.2. Practical contributions

Next to the theoretical contributions, there are also some practical contributions linked to the findings of this study. From a practical perspective, these results show that GenAI is a growing threat in online fraud and specifically spear phishing. GenAI made spear phishing

emails are shown to cause an increase in consumer vulnerability. This likely has to do with the fact that GenAI has also been proven to be capable of creating very realistic content (Schmitt & Flechais, 2024; Neupane et al., 2023). It is therefore of importance for managers to understand the dangers of this new technology.

The first practical contribution is that given the increased danger of these GenAI made emails, managers should look to update their training programs and phishing detection software. Managers need to understand that GenAI made emails can look different and contain different cues. As the literature also suggests, using GenAI for the email creation is a way to get around traditional spam detection security measures (Eze & Shamir, 2024). This combined with the increased effectiveness of GenAI made emails highlights the need for the adoption of updated detection software. Managers should look into newer and more sophisticated security measures like AI technologies. These have shown to be able to detect phishing emails with good accuracy (Schmitt & Flechais, 2024), and are also very effective against GenAI made phishing emails (Eze & Shamir, 2024).

Given that phishing cue knowledge has been found to decrease consumer vulnerability, this remains an important and effective countermeasure against phishing. Having the technical knowledge about the features to look for in an email can help consumers to detect spear phishing emails. The second practical contribution is therefore that managers should implement trainings programs for their employees that focusses on cue utilization and gaining more knowledge and experience about phishing emails. By increasing the specific phishing knowledge of cues, employees can better detect phishing emails (Yang et al., 2022). However, in line with the first contribution it is required to update these training programs to accommodate for GenAI made phishing emails that may use different cues. To train the experience of employees cue based training can be used to improve detection accuracy for employees (Sturman et al., 2023). This makes employees more familiar with the features present in these GenAI made phishing emails, and helps them build better mental models to deal with these situations in the future, which is in line with cue utilization theory (Morrison et al., 2025; Williams et al., 2023).

At last managers should take into account that age is a significant predictor of consumer vulnerability. Younger employees appear to be at an increased risk of falling for spear phishing attacks. The final contribution to practice is therefore that managers should consider prioritizing the use of training recourses for young employees first, if there is a limited capacity. To minimize the chances of employees falling victim to spear phishing

attacks in the process of taking countermeasures, it is recommended to start the training program with the most vulnerable consumers.

5.3. Limitations

This study shed light on online fraud involving GenAI, however several limitations should be noted. First the design of the experiment may not have fully replicated a real-world scenario, which would cause respondents to answer differently than which they would have done in a real context. The decision was made to create a new email application design to make sure that it was equally unfamiliar for all respondents and thus giving the most reliable results, however this could have also contributed to the experiment not feeling real enough. Also contributing to this limitation is the same problem that Bayl-Smith et al. (2020) described, which is that participants assess images of spear phishing emails instead of responding to real spear phishing emails. This takes place in a controlled environment to ensure the safety of the participants. However, people might act different in a real setting where they can interact with the email. Another limitation about the research design is that phishing cue knowledge was measured using self-report, which may not represent the participants' actual utilization of phishing cues as they could be biased. This method was chosen due to the feasibility of the experiment and to make it more accessible to respondents in order to receive more data. Other research about phishing cues used EXPERTise 2.0 to overcome this limitation (Bayl-Smith et al., 2020; Morrison et al., 2025; Sturman et al., 2023, 2024; Williams et al., 2023).

Another limitation is that this study included one phishing cue in each phishing email, with the same cues for both GenAI made emails and human made emails. The amount of emails was limited to limit the effects of respondents fatigue, in line with the research of Parsons et al. (2019). But this also leads to a limited amount of phishing cues that can be tested, and the inability to test combinations. Using only a small number of emails is a common weakness among phishing studies (Martin et al., 2021), and this research is no exception.

The next limitation is the sampling technique. Because of the convenience sampling the biggest portion of the sample consists of students. Even though students are not representable for the average consumer, they are very relevant in the context of online fraud since they engage more in online activities and conduct more online transactions than the average consumer (Vishwanath et al., 2011).

Other limitations are found in the measurement model. In order to increase the internal validity of the scale for phishing cue knowledge, five out of the eight items had to be removed from this scale following the confirmatory factor analysis. Because of this the scale is less comprehensive and might not fully capture the role of phishing cue knowledge as a moderator. Next to this the variable conscientiousness did not have the desired validity, because of the convergent validity which was just below the threshold. This could have caused a lack in explanatory power in the structural model.

5.4. Future research

While this research provides valuable insights into the relationship between GenAI made spear phishing emails, phishing cue knowledge and consumer vulnerability, it also highlights some opportunities for future research. First of all, to properly test the moderating role of phishing cue knowledge it is necessary to measure this concepts using EXPERTise 2.0 in order to properly measure the participants usage of cues when assessing emails. EXPERTise 2.0 has demonstrated construct reliability, predictive validity and reliability (Sturman et al., 2023). In order to better understand the direct relationship between phishing cue knowledge and GenAI made emails, researchers can also test the cue utilization for both groups, and add a control group to the experiment.

Future research should also consider using more emails in the experiment, this helps to incorporate more cues in the experiment which could give a more comprehensive insight into this concept. In line with past research that also employed an email sorting task (Williams et al., 2023), future research should consider putting a time limit on every email that participants get to see. This can make participants act closer to how they would in a real situation, because it prevents participants from carefully reading every email.

Apart from changing the research design, future research could also focus on exploring other potential moderators, for example age or education level. Investigating different factors can show if certain individuals are at a higher risk of new and rising forms of online fraud. Instead of focusing on GenAI made emails, future research could also focus on GenAI with human-in-the-loop in combination with phishing cues. These are emails made by GenAI and then improved and personalized by humans to make them appear more genuine (Heiding et al., 2024). Heiding et al. (2024) found that these GenAI made emails with human-in-the-loop have a higher click through rate than both human made and GenAI made, thus proving that they are dangerous and require more research.

Finally, given that AI technologies are still rapidly evolving (Cho et al., 2025; Schmitt & Flechais, 2024), future research should focus on developing advanced techniques to detect and defend against these new GenAI phishing emails. An example of this in line with existing literature (Heiding et al., 2024; Schmitt & Flechais, 2024) is employing AI systems to detect fraudulent emails. This still requires more research.

5.5. Conclusion

In conclusion, this study explored the emerging threat of GenAI made spear phishing emails, showing that they are even more effective at deceiving consumers compared to the traditional human made spear phishing emails. While phishing cue knowledge is generally important to protect individuals from falling victim to these online frauds, it has not been proven to make an impactful difference when exposed to GenAI made emails compared to human made emails. Given that the problem of GenAI in combination with online frauds will only increase, more research and new solutions are essential.

References

- Abdulai, M. A. (2020). *Examining the Effect of Victimization Experience on Fear of Cybercrime: University Students' Experience of Credit/Debit Card Fraud*.
<https://doi.org/10.5281/ZENODO.3749468>
- ADANCO. (n.d.). *Equation Modeling - ADANCO by Composite Modeling*. Retrieved May 25, 2025, from <https://www.composite-modeling.com/>
- Akkermans, M., Arends, J., Derksen, E., & Reep, C. (2023, mei 10). *1. Inleiding* [Webpagina]. Centraal Bureau voor de Statistiek. <https://www.cbs.nl/nl-nl/longread/rapportages/2023/online-veiligheid-en-criminaliteit-2022/1-inleiding>
- Alharbi, T., & Tassaddiq, A. (2021). Assessment of Cybersecurity Awareness among Students of Majmaah University. *Big Data and Cognitive Computing*, 5(2), 23.
<https://doi.org/10.3390/bdcc5020023>
- Althobaiti, M. (2021). Assessing User's Susceptibility and Awareness of Cybersecurity Threats. *Intelligent Automation & Soft Computing*, 28(1), 167-177.
<https://doi.org/10.32604/iasc.2021.016660>
- Bayl-Smith, P., Sturman, D., & Wiggins, M. (2020). Cue Utilization, Phishing Feature and Phishing Email Detection. In M. Bernhard, A. Bracciali, L. J. Camp, S. Matsuo, A. Maurushat, P. B. Rønne, & M. Sala (Red.), *Financial Cryptography and Data Security* (pp. 56-70). Springer International Publishing. https://doi.org/10.1007/978-3-030-54455-3_5
- Burnes, D., DeLiema, M., & Langton, L. (2020). Risk and protective factors of identity theft victimization in the United States. *Preventive Medicine Reports*, 17, 101058.
<https://doi.org/10.1016/j.pmedr.2020.101058>
- Burns, A. J., Johnson, M. E., & Caputo, D. D. (2019). Spear phishing in a barrel: Insights from a targeted phishing campaign. *Journal of Organizational Computing and Electronic Commerce*, 29(1), 24-39. <https://doi.org/10.1080/10919392.2019.1552745>
- Canfield, C. I., Fischhoff, B., & Davis, A. (2016). Quantifying Phishing Susceptibility for Detection and Behavior Decisions. *Human Factors*, 58(8), 1158-1172.
<https://doi.org/10.1177/0018720816665025>

- Cho, K., Park, Y., Kim, J., Kim, B., & Jeong, D. (2025). Conversational AI forensics: A case study on ChatGPT, Gemini, Copilot, and Claude. *Forensic Science International: Digital Investigation*, 52, 301855. <https://doi.org/10.1016/j.fsidi.2024.301855>
- Ciuchita, R., Heller, J., Köcher, S., Köcher, S., Leclercq, T., Sidaoui, K., & Stead, S. (2023). It is Really Not a Game: An Integrative Review of Gamification for Service Research. *Journal of Service Research*, 26(1), 3-20. <https://doi.org/10.1177/10946705221076272>
- Clavariate (2020). *Journal Citation Reports*. Accessed February 2, 2025. [Journal Citation Reports - Home](#)
- Conner, M., & Abraham, C. (2001). Conscientiousness and the Theory of Planned Behavior: Toward a more Complete Model of the Antecedents of Intentions and Behavior. *Personality and Social Psychology Bulletin*, 27(11), 1547-1561. <https://doi.org/10.1177/01461672012711014>
- Darwish, A., Zarka, A. E., & Aloul, F. (2012). Towards understanding phishing victims' profile. *2012 International Conference on Computer Systems and Industrial Informatics*, 1-5. <https://doi.org/10.1109/ICCSII.2012.6454454>
- Donnellan, M. B., Oswald, F. L., Baird, B. M., & Lucas, R. E. (2006). The Mini-IPIP Scales: Tiny-yet-effective measures of the Big Five Factors of Personality. *Psychological Assessment*, 18(2), 192-203. <https://doi.org/10.1037/1040-3590.18.2.192>
- Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006). Decision strategies and susceptibility to phishing. *Proceedings of the Second Symposium on Usable Privacy and Security - SOUPS '06*, 79. <https://doi.org/10.1145/1143120.1143131>
- Ethical Review Committee for Law and Management Sciences (ETRM) | Radboud University*. (n.d.). <https://www.ru.nl/over-ons/organisatie/faculteiten/rechtsgeleerdheid/onderzoek/ethische-toetsingscommissie>
- Eze, C. S., & Shamir, L. (2024). Analysis and Prevention of AI-Based Phishing Email Attacks. *Electronics*, 13(10), Article 10. <https://doi.org/10.3390/electronics13101839>
- Field, A. (2017). *Discovering statistics using IBM SPSS statistics* (5th edition). SAGE Publications.
- Gan, C. L., Lee, Y. Y., & Liew, T. W. (2024). Fishing for phishy messages: Predicting phishing susceptibility through the lens of cyber-routine activities theory and heuristic-systematic model. *Humanities and Social Sciences Communications*, 11(1), 1-17. <https://doi.org/10.1057/s41599-024-04083-1>

- Guedes, I., Martins, M., & Cardoso, C. S. (2022). Exploring the determinants of victimization and fear of online identity theft: An empirical study. *Security Journal*, 36(3), 472-497. <https://doi.org/10.1057/s41284-022-00350-5>
- Gupta, B. B., Arachchilage, N. A. G., & Psannis, K. E. (2018). Defending against phishing attacks: Taxonomy of methods, current issues and future directions. *Telecommunication Systems*, 67(2), 247-267. <https://doi.org/10.1007/s11235-017-0334-z>
- Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate data analysis* (Eighth edition). Cengage.
- Hayes, A. F. (2022). Introduction to mediation, moderation, and conditional process analysis: A regression-based approach (3rd ed.). The Guilford Press.
- Heiding, F., Lermen, S., Kao, A., Schneier, B., & Vishwanath, A. (2024). *Evaluating Large Language Models' Capability to Launch Fully Automated Spear Phishing Campaigns: Validated on Human Subjects* (arXiv:2412.00586). arXiv. <https://doi.org/10.48550/arXiv.2412.00586>
- Heiding, F., Schneier, B., Vishwanath, A., Bernstein, J., & Park, P. S. (2024). Devising and Detecting Phishing Emails Using Large Language Models. *IEEE Access*, 12, 42131-42146. <https://doi.org/10.1109/ACCESS.2024.3375882>
- Henseler, J., Hubona, G., & Ray, P. A. (2016). Using PLS path modeling in new technology research: Updated guidelines. *Industrial Management & Data Systems*, 116(1), 2-20. <https://doi.org/10.1108/IMDS-09-2015-0382>
- Herley, C. (2010). The Plight of the Targeted Attacker in a World of Scale. In *WEIS*.
- IBM SPSS Statistics 27*. (n.d.). Retrieved May 12, 2025, from <https://www.ibm.com/support/pages/downloading-ibm-spss-statistics-26>
- Iuga, C., Nurse, J. R. C., & Erola, A. (2016). Baiting the hook: Factors impacting susceptibility to phishing attacks. *Human-Centric Computing and Information Sciences*, 6(1), 8. <https://doi.org/10.1186/s13673-016-0065-2>
- Kävrestad, J., Hagberg, A., Nohlberg, M., Rambusch, J., Roos, R., & Furnell, S. (2022). Evaluation of Contextual and Game-Based Training for Phishing Detection. *Future Internet*, 14(4), Article 4. <https://doi.org/10.3390/fi14040104>

- Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing Detection: A Literature Survey. *IEEE Communications Surveys & Tutorials*, 15(4), 2091-2121. IEEE Communications Surveys & Tutorials. <https://doi.org/10.1109/SURV.2013.032213.00009>
- King, E. B., Hebl, M. R., Botsford Morgan, W., & Ahmad, A. S. (2013). Field Experiments on Sensitive Organizational Topics. *Organizational Research Methods*, 16(4), 501-521. <https://doi.org/10.1177/1094428112462608>
- 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>
- Martin, S. R., Lee, J. J., & Parmar, B. L. (2021). Social distance, trust and getting “hooked”: A phishing expedition. *Organizational Behavior and Human Decision Processes*, 166, 39-48. <https://doi.org/10.1016/j.obhdp.2019.08.001>
- Mishra, V., & Mishra, M. P. (2023). PRISMA for Review of Management Literature – Method, Merits, and Limitations – An Academic Review. In S. Rana, J. Singh, & S. Kathuria (Red.), *Review of Management Literature* (pp. 125-136). Emerald Publishing Limited. <https://doi.org/10.1108/S2754-586520230000002007>
- Morrison, B. W., Graf, E., Bayl-Smith, P., & Wiggins, M. W. (2025). Like Shooting Phish in a Barrel: Cue Utilization and Cognitive Reflection Aid Performance in Controlled, but Not Naturalistic Phishing Tasks. *Journal of Cognitive Engineering and Decision Making*, 19(1), 32-53. <https://doi.org/10.1177/15553434241296170>
- Neupane, S., Fernandez, I. A., Mittal, S., & Rahimi, S. (2023). *Impacts and Risk of Generative AI Technology on Cyber Defense* (arXiv:2306.13033). arXiv. <https://doi.org/10.48550/arXiv.2306.13033>
- OpenAI. (2025). ChatGPT (v. GPT-4, 2025, 5 april) [Large language model]. <https://chat.openai.com/>
- Pallant, J. (2001). *SPSS survival manual: A step-by-step guide to data analysis using SPSS for Windows (Versions 10 and 11); [applies to SPSS for windows up to version 11]* (Repr). Open Univ. Press.

- 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>
- Parsons, K., Butavicius, M., Pattinson, M., Calic, D., McCormac, A., & Jerram, C. (2016). *Do Users Focus on the Correct Cues to Differentiate Between Phishing and Genuine Emails?* (arXiv:1605.04717). arXiv. <https://doi.org/10.48550/arXiv.1605.04717>
- Pastor-Galindo, J., Mármol, F. G., & Pérez, G. M. (2021). Nothing to Hide? On the Security and Privacy Threats Beyond Open Data. *IEEE Internet Computing*, 25(4), 58-66. *IEEE Internet Computing*. <https://doi.org/10.1109/MIC.2021.3088335>
- Personal Data Protection Regulation | Radboud Universiteit*. (2024, 1 November). <https://www.ru.nl/regelingen/regeling-bescherming-persoonsgegevens>
- Privacy & informatieveiligheid | Radboud Universiteit*. (n.d.). <https://www.ru.nl/over-ons/beleid-en-regelingen/privacy-en-informatieveiligheid>
- Qualtrics XM - Experience Management Software*. (n.d.). Qualtrics. Retrieved 22 March 2025, from <https://www.qualtrics.com/nl/>
- Radboud University. (n.d.-a). *Procedure Ethics Assessment Committee*. Radboud University. Retrieved March 22, 2025, from <https://www.radboudnet.nl/rechten/onderzoek/ethics-assessment-committee/procedure/>
- Sarno, D. M., Harris, M. W., & Black, J. (2023). Which phish is captured in the net? Understanding phishing susceptibility and individual differences. *Applied Cognitive Psychology*, 37(4), 789-803. <https://doi.org/10.1002/acp.4075>
- Schmitt, M., & Flechais, I. (2024). Digital deception: Generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review*, 57(12), 324. <https://doi.org/10.1007/s10462-024-10973-2>
- Sturman, D., Bell, E. A., Auton, J. C., Breakey, G. R., & Wiggins, M. W. (2024). The roles of phishing knowledge, cue utilization, and decision styles in phishing email detection. *Applied Ergonomics*, 119, 104309. <https://doi.org/10.1016/j.apergo.2024.104309>

- Sturman, D., Valenzuela, C., Plate, O., Tanvir, T., Auton, J. C., Bayl-Smith, P., & Wiggins, M. W. (2023). The role of cue utilization in the detection of phishing emails. *Applied Ergonomics*, *106*, 103887. <https://doi.org/10.1016/j.apergo.2022.103887>
- Vennix, J. A. (2019). *Research methodology: an introduction to scientific thinking and practice*. Pearson [Benelux].
- Virtanen, S. M. (2017). Fear of Cybercrime in Europe: Examining the Effects of Victimization and Vulnerabilities. *Psychiatry, Psychology, and Law*, *24*(3), 323-338. <https://doi.org/10.1080/13218719.2017.1315785>
- Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, *51*(3), 576-586. <https://doi.org/10.1016/j.dss.2011.03.002>
- Williams, R., Morrison, Ben W., Wiggins, Mark W., & Bayl-Smith, P. (2023). The role of conscientiousness and cue utilisation in the detection of phishing emails in controlled and naturalistic settings. *Behaviour & Information Technology*, *43*(9), 1842-1858. <https://doi.org/10.1080/0144929X.2023.2230307>
- Wilson-Lopez, A., Minichiello, A., & Green, T. (2019). An Inquiry Into the Use of Intercoder Reliability Measures in Qualitative Research. *2019 ASEE Annual Conference & Exposition Proceedings*, 32067. <https://doi.org/10.18260/1-2--32067>
- Xu, T., Singh, K., & Rajivan, P. (2023). Personalized persuasion: Quantifying susceptibility to information exploitation in spear-phishing attacks. *Applied Ergonomics*, *108*, 103908. <https://doi.org/10.1016/j.apergo.2022.103908>
- Yang, R., Zheng, K., Wu, B., Li, D., Wang, Z., & Wang, X. (2022). Predicting User Susceptibility to Phishing Based on Multidimensional Features. *Computational Intelligence and Neuroscience*, *2022*(1), 7058972. <https://doi.org/10.1155/2022/7058972>
- Zhou, Y., Cui, X., Qu, W., & Ge, Y. (2022). The effect of automation trust tendency, system reliability and feedback on users' phishing detection. *Applied Ergonomics*, *102*, 103754. <https://doi.org/10.1016/j.apergo.2022.103754>

Appendix A: Item list

The following table includes the items that belong to the scales used to measure the variables.

Variable	Item number	Item
Phishing cue knowledge	1	Wanneer ik een e-mail verdacht vind, let ik altijd extra goed op de naam van de afzender
	2	Wanneer ik een e-mail verdacht vind, let ik altijd extra goed op het e-mailadres van de afzender
	3	Wanneer ik een e-mail verdacht vind, let ik altijd extra goed op het e-mail adres wat er komt te staan als ik de e-mail beantwoord
	4	Wanneer ik een e-mail verdacht vind, let ik altijd extra goed op grammaticale en spelling fouten in de onderwerpregel en bij de afzender
	5	Wanneer ik een e-mail verdacht vind, let ik altijd extra goed op grammaticale en spelling fouten in de inhoud van de e-mail
	6	Wanneer ik een e-mail verdacht vind, let ik altijd extra goed op waarschuwingen in het bericht van de e-mail
	7	Wanneer ik een e-mail verdacht vind, let ik altijd extra goed op uitspraken die urgentie aanduiden
	8	Wanneer ik een e-mail verdacht vind, let ik altijd extra goed op uitspraken over tijdsdruk of tijdsgebonden zaken
Fear of online identity theft	1	Ik ben bang dat iemand mijn persoonlijke en financiële gegevens online kan stelen
	2	Ik maak me zorgen dat iemand mijn persoonlijke en financiële gegevens online kan gebruiken zonder mijn toestemming

	3	Ik maak me zorgen dat mijn reputatie kan worden beschadigd door misbruik van mijn persoonlijke en financiële gegevens online
Conscientiousness	1	Ik voer klusjes meteen uit
	2	Ik leg dingen meestal terug op hun plek
	3	Ik houd van orde
	4	Ik maak nooit ergens een rommeltje van
Age	-	-Age in numbers-
Phishing vulnerability	-	Na het lezen van deze e-mail, welke actie zou u nemen als u Sam zou zijn? A. E-mail beantwoorden B. Bijlage downloaden C. Op de link klikken D. Verder onderzoeken (op internet zoeken, contact opnemen met de betreffende instantie) E. Rapporteren F. Verwijderen G. Negeren

Table A1: List of items.

Appendix B: Persona

Below is the information about the fictional persona which was shown to the participants before the experiment started.

Om dit onderzoek zo realistisch mogelijk te maken is het van belang dat je jezelf kunt verplaatsen in de situatie van de persoon die in de verschillende e-mails voorkomt. Hierdoor introduceren we Sam de Jong, een fictieve persona die zal worden gebruikt in deze studie. Probeer de onderstaande informatie goed te onthouden.

Over Sam

Algemene informatie

Naam: Sam de Jong

Leeftijd: 25 jaar (geboren op 30 september 1999)

Woonplaats: Zonnewijzerlaan 123. 1234AB, Nijmegen

Opleiding: HBO en WO in communicatie en digitale marketing

Woonsituatie: Woont samen met twee vrienden in een appartement in Nijmegen

Bankzaken: Een bankrekening bij Rabobank

Professioneel

Werkzaam bij: Bol.com

Functie: Junior online marketeer

Collega's: Daan, Thomas, Lars, Emma, Julia en Anna

Interesses en online gedrag

Hobbies: Sport, festivals, vintage shoppen, podcasts

Social media gebruik: Actief en geïnteresseerd in digitale tools en sociale media

Waarom Sam?

Het onderzoek bevat de taak om e-mails zo goed mogelijk te kunnen classificeren. Omdat persoonlijkheidsvariabelen voor dit onderzoek van belang zijn, zullen een aantal e-mails ook gepersonaliseerd zijn op basis van e-mails die gestuurd kunnen zijn naar Sam de Jong. Sam vertegenwoordigd een 25-jarige professional uit Nijmegen. Voor e-mail classificatie taak is het hierbij belangrijk je zo veel mogelijk in te leven in het leven van Sam en de e-mails te beantwoorden op de manier hoe Sam dit zou doen.

Appendix C: Analyses

		Statistics			
		Wat is uw leeftijd? (vul een getal in in jaren)	Wat is uw hoogst behaalde opleidingsniveau?	Wat is uw geslacht?	Email_Type
N	Valid	191	191	190	191
	Missing	0	0	1	0
Mean		33,64	5,64	1,53	1,5079
Std. Deviation		15,321	,871	,531	,50125

Table C1: Mean values demographics

		Email_Type			
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1,00	94	49,2	49,2	49,2
	2,00	97	50,8	50,8	100,0
Total		191	100,0	100,0	

Table C2: Frequencies email type groups

EM Estimated Statistics														
EM Means ^a														
H7	H6	G3.0	G6.0	H3	G7.0	H2	H5	G4.0	G1.0	H4	G5.0	G2.0	H1	
5,47	3,85	5,22	3,14	4,53	4,39	2,82	3,47	4,27	5,65	4,77	4,29	4,43	5,05	
Consistentiousnes s_1	Consistentiousnes s_2	Consistentiousnes s_3	Consistentiousnes s_4	fear_of_identity_the _1	fear_of_identity_the _2	fear_of_identity_the _3	POK_1	POK_2	POK_3	POK_4	POK_5	POK_6	POK_7	POK_8
4,28	5,09	5,65	3,47	4,26	4,16	3,49	6,15	6,38	4,61	5,93	5,86	5,65	5,57	5,54

a. Little's MCAR test: Chi-Square = 48,166, DF = 56, Sig. = ,762

Table C3: Little's MCAR test – group 1

EM Estimated Statistics

EM Means ^a													
A5	G4	A11	G3	A13	A12	A17	G5	G6	A4	G7	A16	G1	G2
4,70	4,19	3,45	5,10	5,28	4,68	2,77	4,31	2,86	5,96	4,63	3,35	5,63	4,59

a. Little's MCAR test: Chi-Square = 40,339, DF = 28, Sig. = ,062

Conscientiousness_s_1	Conscientiousness_s_2	Conscientiousness_s_3	Conscientiousness_s_4	fear_of_identity_the_1	fear_of_identity_the_2	fear_of_identity_the_3	POK_1	POK_2	POK_3	POK_4	POK_5	POK_6	POK_7	POK_8
4,08	4,88	5,42	3,29	3,95	3,80	3,77	6,34	6,39	4,72	6,02	5,99	5,72	5,67	5,78

Table C4: Little's MCAR test – group 2

Overall Model

Goodness of model fit (saturated model)

	Value	HI95	HI99
SRMR	0.0583	0.0664	0.0737
d _{ULS}	0.1868	0.2423	0.2991
d _G	0.1138	0.1123	0.1327

Goodness of .model fit (estimated model)

	Value	HI95	HI99
SRMR	0.0583	0.0664	0.0737
d _{ULS}	0.1868	0.2423	0.2991
d _G	0.1138	0.1123	0.1327

Table C5: CFA overall model fit

Construct Reliability

Construct	Dijkstra-Henseler's rho (ρ _A)	Jöreskog's rho (ρ _c)	Cronbach's alpha(α)
Conscientiousness_T	0.7677	0.7649	0.7624
fear_of_identity_the_T	0.8576	0.8532	0.8486
phishing cue knowledge	0.8177	0.7946	0.7702

Table C6: CFA construct reliability

Reliability Statistics

Cronbach's Alpha	N of Items
,757	4

Table C7: Cronbach's Alpha – Conscientiousness

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Beantwoord de volgende stellingen: - Ik voer klusjes meteen uit	13,87	12,156	,501	,730
Beantwoord de volgende stellingen: - Ik leg dingen meestal terug op hun plek	13,05	10,746	,638	,652
Beantwoord de volgende stellingen: - Ik houd van orde	12,50	13,426	,562	,706
Beantwoord de volgende stellingen: - Ik maak nooit ergens een rommeltje van	14,66	11,400	,543	,709

Table C8: Cronbach's Alpha if item deleted – Conscientiousness

Reliability Statistics

Cronbach's Alpha	N of Items
,781	3

Table C9: Cronbach's Alpha – Phishing cue knowledge

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Wanneer ik een e-mail verdacht vind, let ik altijd extra goed op: - het e-mailadres van de afzender	11,89	5,182	,396	,905
Wanneer ik een e-mail verdacht vind, let ik altijd extra goed op: - grammaticale en spelling fouten in de onderwerpregel en bij de afzender	12,29	2,648	,791	,491
Wanneer ik een e-mail verdacht vind, let ik altijd extra goed op: - grammaticale en spelling fouten in de inhoud van de e-mail	12,37	2,659	,766	,526

Table C10: Cronbach's Alpha if item deleted – Phishing cue knowledge

Reliability Statistics

Cronbach's Alpha	N of Items
,848	3

Table C11: Cronbach's Alpha – Fear of online identity theft

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Beantwoord de volgende stellingen: - Ik ben bang dat iemand mijn persoonlijke en financiële gegevens online kan stelen	7,63	8,803	,771	,736
Beantwoord de volgende stellingen: - Ik maak me zorgen dat iemand mijn persoonlijke en financiële gegevens online kan gebruiken zonder mijn toestemming	7,76	8,766	,792	,715
Beantwoord de volgende stellingen: - Ik maak me zorgen dat mijn reputatie kan worden beschadigd door misbruik van mijn persoonlijke en financiële gegevens online	8,09	10,121	,598	,898

Table C12: Cronbach's Alpha if item deleted – Fear of online identity theft

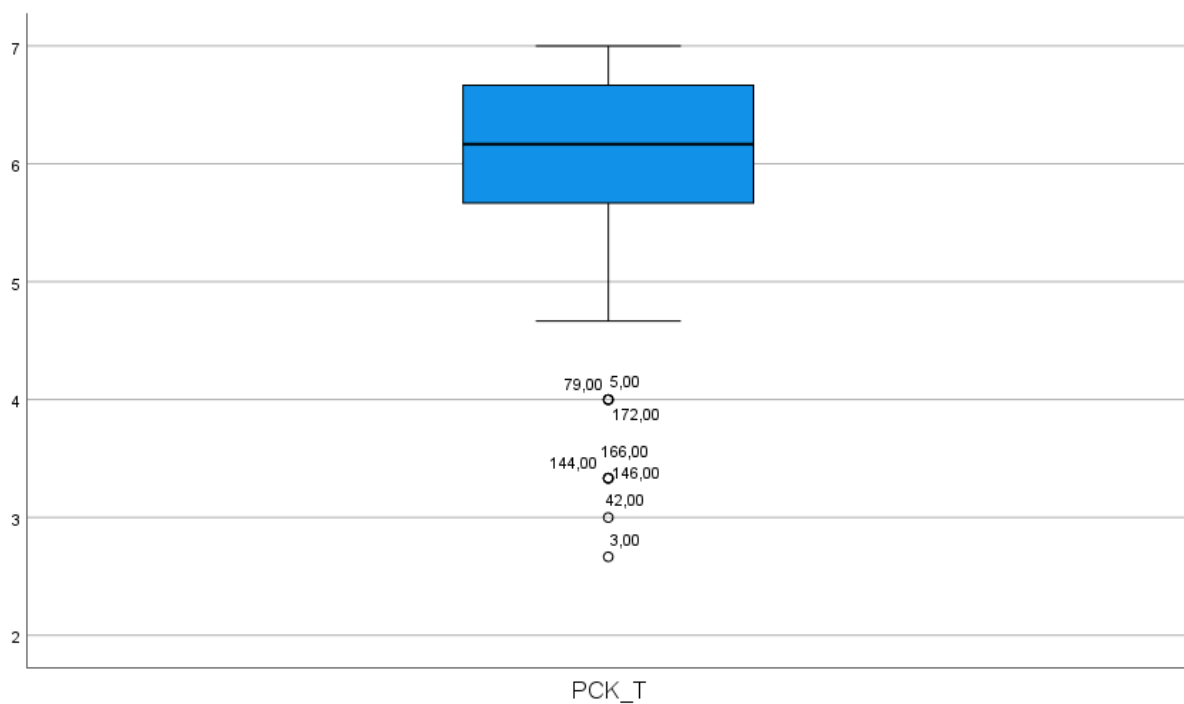


Figure C1: Example of a box plot used to assess outliers

OUTCOME VARIABLE:

ACC_T

Model Summary

R	R-sq	MSE	F(HC3)	df1	df2	p
,3341	,1116	,0421	2,4434	6,0000	149,0000	,0278

Model

	coeff	se (HC3)	t	p	LLCI	ULCI
constant	,6783	,0860	7,8855	,0000	,5083	,8482
E_Type_D	-,0671	,0338	-1,9841	,0491	-,1340	-,0003
PCK_T	,0358	,0317	1,1283	,2610	-,0269	,0985
Int_1	,0156	,0437	,3577	,7211	-,0706	,1019
Age	,0028	,0012	2,2952	,0231	,0004	,0053
Fear_T	,0113	,0123	,9147	,3618	-,0131	,0356
Con_T	-,0143	,0153	-,9338	,3519	-,0446	,0160

Product terms key:

Int_1 : E_Type_D x PCK_T

Table C13: Results main analysis PROCESS model 1

OUTCOME VARIABLE:

ACC_T

Model Summary

R	R-sq	MSE	F(HC3)	df1	df2	p
,3349	,1121	,0421	2,5701	6,0000	149,0000	,0213

Model

	coeff	se (HC3)	t	p	LLCI	ULCI
constant	,5025	,1550	3,2430	,0015	,1963	,8088
E_Type_D	-,0672	,0337	-1,9913	,0483	-,1339	-,0005
Age	,0022	,0018	1,1987	,2326	-,0014	,0058
Int_1	,0013	,0025	,5060	,6136	-,0037	,0062
Fear_T	,0106	,0125	,8467	,3985	-,0141	,0352
Con_T	-,0138	,0154	-,8985	,3704	-,0442	,0166
PCK_T	,0438	,0212	2,0637	,0408	,0019	,0857

Product terms key:

Int_1 : E_Type_D x Age

Table C14: Results post hoc analysis wit age as moderator

Model Summary ^b									
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	R Square Change	Change Statistics			Sig. F Change
						F Change	df1	df2	
1	,333 ^a	,111	,081	,20461	,111	3,731	5	150	,003

a. Predictors: (Constant), Age, E_Type_D, Fear_T, Con_T, PCK_T

b. Dependent Variable: ACC_T

Table C15: Post hoc simple regression analysis model fit

Coefficients^a

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	,416	,132		3,147	,002
	E_Type_D	-,067	,033	-,158	-2,027	,044
	Fear_T	,011	,011	,076	,982	,328
	PCK_T	,043	,019	,180	2,245	,026
	Con_T	-,014	,015	-,073	-,923	,358
	Age	,003	,001	,175	2,162	,032

a. Dependent Variable: ACC_T

Table C16: Post hoc simple regression analysis results