

Radboud Universiteit



The effect of different spear phishing e-mails on consumer vulnerability
moderated by self-efficacy

Abstract

This thesis investigates whether AI-generated spear phishing e-mails lead to higher consumer vulnerability than human-crafted ones and whether self-efficacy moderates this relationship. Through a between-subjects online experiment participants were exposed to either GenAI or human-generated phishing e-mails and asked to respond as if they were the e-mail recipient. Results showed no significant differences in vulnerability between the two types of messages, nor a significant moderating effect of self-efficacy. However, phishing cue knowledge (PCK) significantly predicted lower vulnerability suggesting that recognizing phishing indicators remains a key protective factor. Although GenAI e-mails appeared more polished, this did not automatically translate to higher deception. These findings contribute to a growing body of literature exploring how emerging technologies and psychological traits shape cyber risk, and highlight the need to focus training efforts on practical cue recognition rather than just confidence-building.

Keywords: spear phishing, Generative AI, phishing vulnerability, self-efficacy, cybersecurity, ai-generated deception, online fraud detection, experimental design.

Table of contents

1. Introduction	4
2. Theoretical Background	7
2.1 Spear phishing and consumer vulnerability	8
2.2 GenAI in spear phishing	9
2.3 The moderating role of Self-efficacy	10
2.4 Control variables	12
2.5 Conceptual model and hypothesis	14
3. Methodology	15
3.1 Research strategy	15
3.2 Sampling	15
3.3 Operationalization	17
3.3.1 Spear phishing vulnerability	17
3.3.2 Moderator	17
3.3.3 Independent variable	17
3.3.4 Control variables	19
3.4 procedure	20
3.5 Data analysis	21
3.6 Ethical considerations	22
4. Analysis	23
4.1 Descriptives & data cleaning	23
4.2 Confirmatory factor analysis	25
4.3 Assumption testing	26
4.3.1 Linearity	26
4.3.2 Normality	27
4.3.3 Homoscedasticity	27
4.3.4 Multicollinearity	27
4.3.5 Independence of error terms	27
4.4 Hypothesis testing	27
4.4.1 Main effect of type of spear phishing message on vulnerability	27
4.4.2 Moderating effect of self-efficacy	28
4.4.3 Control variables	29
5. Discussion	30
5.1 Discussion of the findings	30
5.2 Theoretical and practical implications	32
5.3 Limitations & recommendations for future research	33

5.4 Conclusion	34
References	36
Appendix	44

1. Introduction

Artificial Intelligence (AI) refers to systems that can perform tasks typically requiring human intelligence such as recognizing patterns, making decisions and understanding language (Russell & Norvig, 2020). In recent years AI has become increasingly common in society offering new possibilities in areas like customer service, automation and data analysis (Choudhury et al., 2025). At the same time these same developments also bring new risks, especially in the field of cybersecurity.

One example where this risk becomes clear is spear phishing. These are phishing e-mails that are targeted and personalized often pretending to come from a trustworthy source (Eftimie et al., 2022). In the past, these e-mails were written by humans and often contained spelling or grammar mistakes that made them easier to recognize (Heiding et al., 2024). This has changed rapidly with the rise of generative AI (GenAI) tools like ChatGPT, which allow attackers to craft well written and convincing phishing e-mails within seconds (Bezzi, 2024; Schmitt & Flechais, 2024).

As these e-mails become more professional and realistic it becomes more important to understand why some people are more vulnerable than others. Previous studies have looked into differences in phishing vulnerability based on things like knowledge, digital habits or risk perception (Goel et al., 2017; Vishwanath et al., 2011). Despite growing attention to phishing in general there is still little research that focuses specifically on AI-generated phishing e-mails and how psychological traits like self-efficacy may influence the way people respond to them.

Self-efficacy refers to someone's belief in their own ability to perform certain tasks (Bandura, 1977; Ribeiro et al., 2023). In the context of phishing previous research has found that both high and low levels of self-efficacy can be risky. For example people with high self-efficacy may be overconfident and miss warnings signs, especially when the message looks polished (Wright & Marett, 2010; Wang et al., 2016). On the other hand, people with low self-efficacy may doubt themselves and click too quickly out of uncertainty (Lee et al., 2023). Even though previous studies have looked at self-efficacy in phishing, no research has yet examined how it interacts with AI-generated versus human spear phishing e-mails. This indicates that a gap still exists in the current literature. While phishing has been widely examined, little attention has been given to how self-efficacy moderates the effect of different spear phishing e-mail types such as GenAI versus human-written e-mails. This study focuses on that specific link.

The goal of this study is to examine whether the type of spear phishing e-mail (GenAI versus human) influences vulnerability and whether self-efficacy moderates this relationship. This leads to the following research question: “To what extent do different types of spear phishing (GenAI vs. Human) e-mails influence spear phishing vulnerability, and to what extent does self-efficacy moderate this relationship?”

This study contributes to the academic literature by combining insights from phishing research, AI-generated deception and psychological moderators such as self-efficacy. While previous studies have explored how users detect traditional phishing messages (Goel et al., 2017; Vishwanath et al., 2011), little is known about how generative AI influences detection behavior and how individual traits affect this process. By examining self-efficacy as a moderator, this study provides a more nuanced understanding of how the effect of message type depends on an individual's perceived ability to detect phishing. This adds depth to existing models that explain phishing vulnerability (Vishwanath et al., 2011) and helps update theoretical frameworks in light of emerging technologies such as large language models (LLMs) (Choudhury et al., 2025).

In practice, this study offers valuable insights for organizations that aim to reduce phishing vulnerability among employees or consumers. As phishing attacks become more realistic and personalized through the use of AI, it becomes increasingly important to understand how psychological traits influence vulnerability. Research shows that factors such as self-efficacy, personality traits and habitual online behavior play a critical role in determining vulnerability to phishing (Frauenstein et al., 2023; Kavvadias & Kotsilieris, 2025). Identifying self-efficacy as a moderating factor can help tailor training programs to better match users' cognitive profiles and risk perception (Wang et al., 2012; Vishwanath et al., 2011). For example, users with high self-efficacy may benefit more from exposure to polished, realistic phishing simulations while those with low self-efficacy may need more guided support to increase their awareness and detection confidence (Wright & Marett, 2010; Parsons et al., 2014).

This topic is relevant for many sectors such as education, government and healthcare, where phishing attacks have led to serious problems in recent years (Frauenstein et al., 2023). By increasing awareness of the psychological factors that influence how people react to phishing, policymakers can create more focused and effective cybersecurity campaigns. In addition, this study adds to existing research that stresses the need to look beyond technical solutions and

also consider human behavior when dealing with cyber risks. Many cyber incidents are caused by how people act or respond rather than by system errors, which is why it is important to combine psychological, organizational and technical strategies in cybersecurity (Smith et al., 2025). As cyber attackers keep using more advanced tools, it becomes even more important to understand how different people react to these threats in order to create flexible and human-focused security systems.

The upcoming chapters are structured as follows:

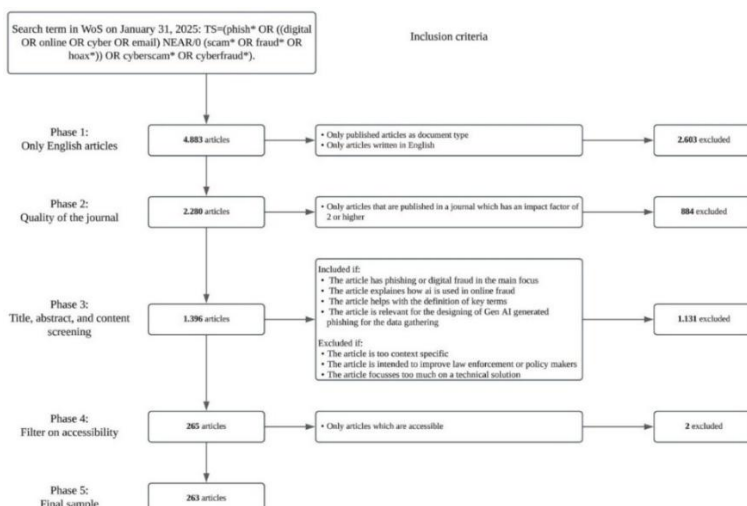
- Chapter 2 introduces the theoretical background and hypotheses.
- Chapter 3 outlines the methodological approach used in this study.
- Chapter 4 presents the results of the data analysis.
- Chapter 5 provides a discussion, including limitations and recommendations for future research and the overall conclusion

2. Theoretical Background

Within this chapter the literature that is used in this thesis will be presented. The literature is gathered via a systematic literature review (Ciuchita et al., 2022). The purpose of the literature review is to gather good quality articles that are specified towards the topic in question. This literature review was performed with the help of five other students that are researching the same main relationship. All the steps of the selection process, following the PRISMA framework (Moher et al., 2009) are presented in Figure 1.

The first step was to determine a search term that was fitting for our main relationship. We included factors that were attached to our independent variable and dependent variable and tried to keep it broad into the cybersecurity domain. In phases one and two the main part of the filtering was done by general inclusion criteria like only English articles and quality had to be a minimal impact factor of two. An impact factor of 2 was chosen to ensure the academic quality of the articles (Hiebl, 2021). In the third phase the articles that remained were divided amongst pairs of two people. The pairs of two were constructed in order to have a better intercoder reliability for our whole project (Belur et al., 2018). The intercoder reliability for the literature review is calculated as 0.93, which is an acceptable score looking at the minimal value of 0.80 that needed to be reached (Wilson-Lopez et al., 2019). This calculation was made by dividing the times that both coders came to the same conclusion by the total of articles (Wilson-Lopez et al., 2019). During this process inclusion and exclusion criteria were used as a guideline for the filtering. In phase four the articles were filtered on accessibility of the article. In the last phase the final sample remained.

Figure 1
Systematic literature review.



2.1 Spear phishing and consumer vulnerability

Spear phishing is a form of phishing in which an attacker poses as a trustworthy source and uses personal information to deceive an individual, organization or group (Eftimie et al., 2022). The spear phishing process typically consists of five stages. It begins with the preparation phase, during which the attacker collects personal data to craft a convincing e-mail. In the filter phase, this e-mail is tested against security systems. If not flagged, the e-mail reaches the recipient, who then opens it in the third phase. The fourth phase involves the victim performing a risky action such as clicking a link or downloading an attachment. This may lead to malware infection or redirection to a malicious website. In the final phase the attacker gains access to sensitive information through the infected system or website (Eftimie et al., 2022).

Understanding how individuals become victims of such attacks involves exploring the concept of vulnerability. Spear phishing vulnerability refers to the extent to which someone is likely to fall for a targeted phishing attempt (Hassandoust et al., 2020). This vulnerability is influenced by personal factors such as habits, motivation and cognitive biases that may be exploited by attackers (Hassandoust et al., 2020).

To better understand the psychological processes behind such vulnerability, the Elaboration Likelihood Model (ELM) is often applied. According to this model, there are two main ways of processing information: the central route which relies on careful consideration and logical evaluation, and the peripheral route which is driven by heuristics and superficial cues (Petty & Cacioppo, 1986). Processing via the central route requires motivation and cognitive capacity while the peripheral route involves minimal cognitive effort and is more common in everyday decision making.

In the context of spear phishing it is essential to identify which processing route is most frequently used when individuals evaluate suspicious messages. Research by Goel et al. (2017) shows that people often rely on the peripheral route, judging e-mails based on surface-level characteristics such as formatting, logos or tone. This highlights a potential weak spot in digital awareness, as superficial processing increases the risk of falling for deceptive content. At the same time this knowledge is useful for attackers as it helps them craft messages that appear legitimate and bypass critical thinking (Goel et al., 2017).

This theoretical foundation underlines the importance of understanding not only the characteristics of phishing e-mails but also the psychological processes that influence how people interpret and respond to them.

2.2 GenAI in spear phishing

Generative Artificial Intelligence (GenAI) refers to a form of artificial intelligence that can autonomously generate new content by learning patterns from existing data (Choudhury et al., 2025). In the context of spear phishing, GenAI is used to create highly realistic and personalized e-mails that mimic the tone, structure and writing style of legitimate senders (Schmitt & Flechais, 2024). These AI-generated spear phishing e-mails are crafted to deceive recipients more effectively than traditional, human-written ones (Heiding et al., 2024).

A key technology behind this development is the use of large language models (LLMs) which are trained on datasets to produce coherent and contextually appropriate text (Heiding et al., 2024). Through techniques such as prompt engineering where targeted instructions are used to guide the output of the model, attackers can instruct LLMs to generate messages tailored to specific individuals or scenarios (Trad & Chehab, 2024). This personalization is further enhanced by integrating publicly available data such as job roles or social media activity allowing for highly credible and targeted messages (Schmitt & Flechais, 2024).

LLMs do not only imitate human language but can also adjust for tone, grammar and persuasive cues making the message appear more authentic and trustworthy (Bezzi, 2024). Some models are even capable of maintaining ongoing dialogues, strengthening the illusion of trust and increasing the likelihood of deception (Heiding et al., 2024). In addition GenAI can be combined with other AI technologies such as image generation tools to create fake identities with profile pictures or forged documents (Bezzi, 2024).

In contrast human-generated spear phishing e-mails are often based on intuition or manual research and may contain linguistic errors or inconsistent formatting (Schmitt & Flechais, 2024). According to Heiding et al. (2024) all of this makes them easier to detect and less successful in deceiving recipients.

Because GenAI e-mails appear more professional and personalized, they may elicit greater trust which in turn can increase vulnerability to spear phishing (Heiding et al., 2024; Bezzi, 2024). Research shows that users often rely on surface-level cues such as tone, structure and

spelling to assess whether a message is legitimate (Goel et al., 2017). Since GenAI messages tend to contain fewer linguistic errors and more closely mimic professional communication, they may avoid suspicion more easily than human-made phishing attempts which often contain linguistic inconsistencies (Schmitt & Flechais, 2024).

In addition, AI tools can generate highly specific messages at scale through techniques such as prompt engineering, allowing for highly personalized phishing content that matches the recipient's context (Trad & Chehab, 2024). This increases the chance of bypassing individual detection strategies and leads to higher engagement, as reflected in higher click-through rates for GenAI-generated e-mails (Heiding et al., 2024).

GenAI messages frequently mirror real communication in tone and layout which can make them appear more credible to recipients (Bezzi, 2024). This means that recipients might perceive them as trustworthy, even when they contain harmful content (Bezzi, 2024). This perceived credibility can lower users alertness and make them more likely to respond (Bezzi, 2024). These elements combined may help clarify why GenAI phishing messages tend to be more convincing than those created by humans.

This leads to the first hypothesis of the study:

H1: "GenAI spear phishing e-mails lead to higher vulnerability compared to human made spear phishing e-mails".

2.3 The moderating role of Self-efficacy

The concept of self-efficacy refers to the broad belief individuals have in their ability to perform specific tasks (Bandura, 1977; Ribeiro et al., 2023). In the context of this research self-efficacy is used as a moderator in the relationship between the type of spear phishing e-mail (GenAI vs. human) and spear phishing vulnerability.

Several studies have shown that self-efficacy affects how people respond to phishing attempts, what elements they focus on and which cues they trust depending on the message type (Wang et al., 2016; Vishwanath et al., 2011). Ribeiro et al. (2023) for instance suggests that individuals with high levels of self-efficacy can become overly confident in their ability to detect phishing attempts, leading them to overlook potential warning signs. In particular when GenAI-generated messages are used (often more refined and professional), this

overconfidence may result in increased vulnerability (Bandura, 1997; Ribeiro et al., 2023; Wright & Marett, 2010).

While self-efficacy is often seen as a protective factor in online settings (Vishwanath et al., 2011), it may also lead to overconfidence, especially when messages appear sophisticated or trustworthy (Wang et al., 2016). This becomes particularly relevant in the context of GenAI-generated phishing e-mails which often look more realistic, professional and emotionally persuasive than their human written counterparts (Bezzi, 2024; Heiding et al., 2024).

Previous studies show that individuals with high levels of self-efficacy are more likely to rely on their own judgement rather than external cues when evaluating suspicious content (Harrison et al., 2016). Wang et al. (2016) found that overconfidence among high self-efficacy individuals can reduce their attention to subtle signs of deception, especially when the phishing message appears polished and legitimate. Similarly, Harrison et al. (2016) explained that these individuals often use peripheral (heuristic) processing routes which can be risky when messages lack obvious red flags, as is often the case with GenAI output.

In contrast, individuals with lower self-efficacy may lack confidence in their ability to detect phishing which could lead them to either avoid acting or rely more heavily on external cues (Vishwanath et al., 2011). In some cases, this uncertainty may lead to more cautious behaviour such as avoiding clicking or reporting suspicious e-mails. In contrast, GenAI phishing e-mails are generally more grammatically correct and professionally written which may make human-generated e-mails that are often less polished easier to detect for individuals with high self-efficacy (Bezzi, 2024; Heiding et al., 2024). This suggests that the interaction between e-mail type and self-efficacy is particularly relevant in this study. That is, GenAI messages may disproportionately affect those with higher self-efficacy due to their reliance on internal confidence rather than critical scrutiny (Wang et al., 2016; Harrison et al., 2016).

In contrast other research points out that low self-efficacy can also be risky. When people doubt their ability to detect phishing attempts they may feel overwhelmed or unsure which can lead to impulsive decisions or excessive trust (Lee et al., 2023). On the other hand some individuals with low confidence may become more cautious which can lower their vulnerability (Workman, 2007; Vishwanath et al., 2011).

In addition Wright and Marett (2010) found that people with high self-efficacy often feel safer online which might lower their level of attention and lead to riskier behavior. Previous studies have shown mixed effects of self-efficacy suggesting that both high and low levels may

increase vulnerability under certain circumstances. However, recent literature offers stronger evidence that high self-efficacy can lead to overconfidence which in turn increases vulnerability to more refined phishing attacks. Based on this, the current study hypothesizes that self-efficacy moderates the relationship between e-mail type and phishing vulnerability, with higher self-efficacy increasing vulnerability to GenAI-generated e-mails compared to human ones.

These insights form the following hypothesis:

H2: “Self-efficacy moderates the relationship between spear phishing e-mail type (GenAI vs. human) and phishing vulnerability, with individuals high in self-efficacy expected to show increased vulnerability to GenAI-generated e-mails compared to those low in self-efficacy”.

2.4 Control variables

Fear of identity theft

Fear of Online Identity Theft (FOIT) refers to the fear people experience when thinking about the misuse of their personal or financial information online (Guedes et al., 2022). This fear usually consists of two parts: fear of financial loss and fear of reputational damage (Hille et al., 2015). Financial loss can involve situations like someone stealing money or accessing accounts without permission. Reputational damage happens when someone misuses another person’s identity in ways that could be embarrassing or harmful to their reputation.

Previous research has shown that FOIT can influence how people behave online, especially when it comes to trust and risk perception (Jordan et al., 2018). People who are more afraid of identity theft might be more cautious or suspicious when interacting with potentially harmful online content, like phishing e-mails (Guedes et al., 2022; Jordan et al., 2018).

In this study, FOIT is included as a control variable because it may affect how vulnerable someone feels or behaves when confronted with phishing attempts (Guedes et al., 2022; Hassandoust et al., 2020). Previous studies have shown that individuals who experience higher levels of fear of identity theft are more likely to engage in cautious or avoidant online behavior, which can influence their ability to detect or respond to phishing cues (Guedes et al., 2022). By controlling for FOIT, this research can better isolate the effects of the e-mail type and self-efficacy on phishing vulnerability without the results being skewed by someone’s general fear of being targeted online.

Phishing cue knowledge

Phishing Cue Knowledge (PCK) refers to an individual's ability to recognize typical signs of phishing attempts in e-mails such as generic greetings, urgent language, suspicious URLs or spelling and grammar errors (Vishwanath et al., 2011). This kind of domain-specific knowledge helps users interpret e-mails more critically by comparing message features to their existing mental models of legitimate communication (Sturman et al., 2024; Vishwanath et al., 2011).

Previous research has shown that people with higher PCK are better at identifying deceptive e-mails, as they tend to focus more on structural cues like sender details, message tone or linguistic inconsistencies (Jakobsson, 2007; Vishwanath et al., 2011). This knowledge allows them to engage in more elaborate processing which reduces the risk of falling for phishing scams, especially those relying on superficial trust cues or urgency (Eveland et al., 2001; Petty & Cacioppo, 1986). In contrast, individuals with low PCK are more likely to rely on peripheral processing, increasing their susceptibility to deception (Petty & Cacioppo, 1986).

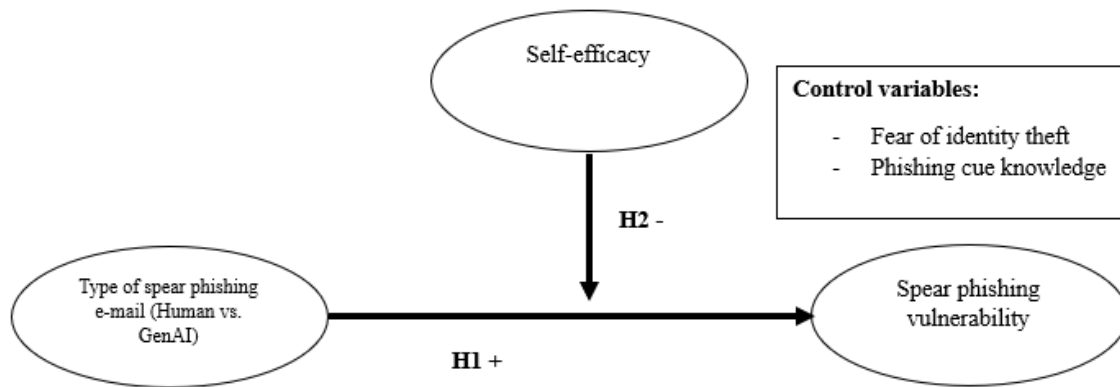
In this study PCK is included as a control variable because prior familiarity with phishing indicators may influence how participants interpret and respond to both GenAI and human-written phishing e-mails (Vishwanath et al., 2011; Sturman et al., 2024). Without controlling for this, differences in knowledge might wrongly influence the results for message type or self-efficacy. By controlling for PCK, this research aims to isolate the psychological mechanisms under investigation and increase the validity of the results (Vishwanath et al., 2011).

2.5 Conceptual model and hypothesis

Based in the previous literature study the following conceptual model is created for this study:

Figure 2

Conceptual model.



3. Methodology

The focus of this study is on researching to what extent vulnerability is being influenced by different kind of spear phishing messages and to what extent self-efficacy has an impact on this relationship. The methodology for this research is discussed in the paragraphs below. The research is conducted by six students in total with all different moderating effects.

3.1 Research strategy

This study used a between-subjects online experiment to examine whether there were differences in spear phishing vulnerability between human and GenAI generated e-mails. This experimental design was chosen because it allows manipulation of a single independent variable (e-mail type) while minimalizing learning or fatigue effects that may arise in within-subject designs (Canfield et al., 2016). Previous studies in phishing research have successfully used similar experimental setups (Zhou et al., 2022; Williams et al., 2023).

The online nature of the experiment enables broad and efficient data collection in a controlled environment which enhances ecological validity and practical feasibility (Williams et al., 2023). Participants were exposed to realistic e-mails and had to respond as if they were the persona itself. The persona used in this study is presented in appendix 8.

A quantitative approach was applied to objectively measure phishing detection accuracy following prior studies in this domain (Xu et al., 2022; Williams et al., 2019; Lawson et al., 2020; Parsons et al., 2019). Phishing detection accuracy is used as a behavioral indicator of spear phishing vulnerability as it shows how well participants are able to recognize malicious e-mails. A lower score means that someone is less accurate in spotting phishing which suggests they are more vulnerable to such attacks (Sarno et al., 2023; Xu et al., 2022).

3.2 Sampling

The target population for this study consisted of individuals aged 18 and older who have experience using e-mail. This age limit was based on the ethical research guidelines of Radboud University which allow participants from age 18 to provide informed consent independently, without the involvement of legal guardians (Radboud University, n.d.-c). This

ensured that no vulnerable groups were included and that all participants could give voluntary and informed consent (Ethical Review Committee for the Humanities, 2019).

Spear phishing is a form of cybercrime that can potentially affect a broad range of people, regardless of demographic characteristics (Xu et al., 2022). However, in practice the sample for this study primarily consisted of university students and young adults within the researchers personal networks. As a result of this the findings are most applicable to this specific population and caution should be taken when generalizing results to the wider population.

Participants were recruited using a convenience sampling method via personal social media platforms such as Instagram and WhatsApp. This method was selected because of its practical benefits for online experiments and its successful use in previous phishing research (Heiding et al., 2024; Xu et al., 2022; Stratton, 2021). Although the researchers initially shared the survey link themselves, it is likely that the post was also seen or reshared by individuals outside of their direct networks. This means that the full reach of the survey cannot be fully controlled, but access and distribution were still largely manageable.

The goal was to obtain a minimum sample size of 100 participants. This is in line with recommendations for linear regression analysis which suggest that a sample of 100 is sufficient when the number of predictors is below six (Field, 2017). In this study, the predictors included the independent variable (e-mail type), the moderator (self-efficacy) and two control variables, all within this limit. After data cleaning the final dataset included 156 valid responses which met the required sample size (Field, 2017).

To ensure the constructs were measured reliably and validly, a confirmatory factor analysis (CFA) was conducted before testing the hypotheses. Since CFA falls under structural equation modeling, a rule of thumb is to include at least 10 respondents per indicator item (Hair et al., 2019). The CFA included three latent variables: self-efficacy (3 items), fear of identity theft (3 items), and phishing cue knowledge (8 items), resulting in a total of 14 items. Based on this, a minimum of 140 participants was required. This threshold was met with a final sample of 156 respondents included in the analysis. Problematic items were removed in later iterations to improve model fit.

3.3 Operationalization

Within this research different variables are measured: Spear phishing vulnerability, type of message and self-efficacy. There are also some control variables measured for this specific study, these are mentioned in the text below and can also be found in appendix 3.

3.3.1 Spear phishing vulnerability

In this research spear phishing vulnerability is measured through participants behavioral responses to e-mail scenarios, which simulate real-life decisions. Following the approach of Sarno et al. (2023) and Xu et al. (2022), participants were presented with multiple response options for each e-mail including: (reply, download attachment, click on link, search online, report, delete or ignore). These responses were categorized as high (reply, download attachment, click on link) and low (investigate, report, delete, ignore) vulnerability based on the classification of Xu et al. (2022). In order to measure spear phishing vulnerability within the dataset phishing detection accuracy was used measuring the percentage of correctly identified spear phishing e-mails (number of correctly identified spear phishing e-mails / total number of phishing e-mails presented) (Sarno et al., 2023; Xu et al., 2022).

3.3.2 Moderator

The moderator in this study self-efficacy is measured by a 7-point Likert scale ranging from 1 (I completely disagree) to 7 (I completely agree). For this measure a developed scale from Chen et al. (2020) is used that consists of three items. This scale is developed for the phishing context specifically based on previous work from Wang et al. (2009) that measured self-efficacy in the e-mail identification setting.

In this study, the validated phishing self-efficacy scale from Chen et al. (2020) was used. To make sure the items matched the specific context of spear phishing, the word “spear” was added to the original phishing-related statements. The adjusted items used to measure spear phishing self-efficacy can be found in Appendix 3. This small wording change helped improve content validity without changing the meaning or structure of the original scale (Diamantopoulos & Winklhofer, 2001).

3.3.3 Independent variable

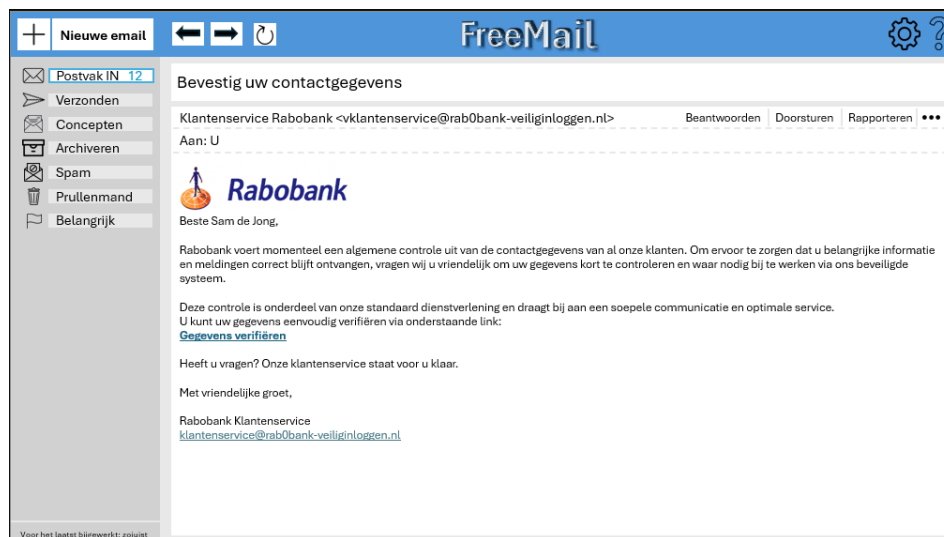
The independent variable in this study is the type of spear phishing e-mail, which includes two categories: human-generated spear phishing e-mails and AI-generated spear phishing e-mails.

This variable is categorical in nature and was dummy coded for analysis (0 = human, 1 = GenAI) (Field, 2017).

AI-generated spear phishing e-mails were created using the most recent accessible version of ChatGPT (GPT-4o). To tailor these messages to the fictional persona used in the experiment, the persona's profile (see Appendix 8) was first provided in the prompt to create personalized content. Example prompts included: “Write a phishing e-mail impersonating a manager urgently asking for login credentials” or “Pretend to be a delivery service requesting a click on a suspicious tracking link.” Although ChatGPT may restrict direct requests for “spear phishing e-mails” due to ethical guidelines, this was avoided by simply prompting the model to “write an e-mail” in a specific context (Heiding et al., 2024). In practice, the model had no problem generating convincing spear phishing e-mails. To create variation the AI was instructed to produce different e-mails, each targeting a different phishing tactic until a sufficient set was reached.

Figure 3

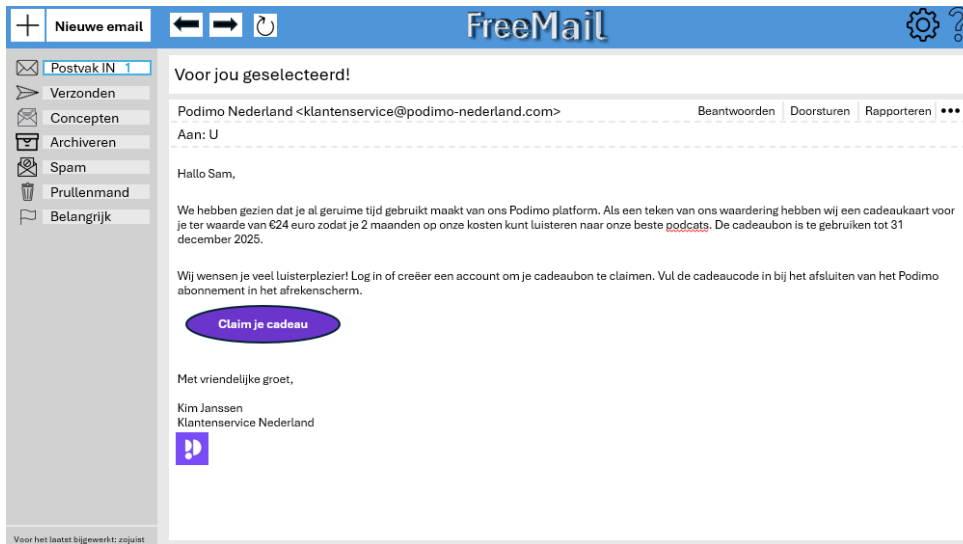
AI-generated spear phishing e-mail.



Human-generated spear phishing e-mails were created based on the V-Triad model (Heiding et al., 2024), which manipulates messages along three pillars: credibility, compatibility and customizability. These messages were crafted manually by the researchers using contextual information from the fictional persona. Each message was written to closely mimic real-life phishing tactics that would bypass suspicion filters by adjusting content, tone and sender details such as creating urgency, impersonating authority figures or including misleading URLs (Heiding et al., 2024).

Figure 4

Human-generated spear phishing e-mail.



Genuine e-mails were also used as part of the experiment. These messages followed the cues described by Parsons et al. (2016), including: higher consistency, personalization, presence of links and credibility of sender. Genuine e-mails were collected from the researchers actual inboxes and were sent by well-known organizations such as Rabobank or bol.com in line with methods from Parsons et al. (2016). All selected e-mails were carefully checked to ensure they met the criteria for authentic communication and did not trigger suspicion (Parsons et al., 2016).

3.3.4 Control variables

Fear of Identity Theft (FOIT) is included as a control variable to account for individual differences in how cautious people behave when exposed to phishing threats. It reflects people's concern about the misuse of their personal or financial information in online environments (Guedes et al., 2022). In this study, FOIT was measured using a 7-point Likert scale based on validated items from previous research that capture concerns related to both financial loss and reputational damage (Guedes et al., 2022). This variable was included to control for fear-related reactions that could influence how participants respond to phishing e-mails (Guedes et al., 2022).

The second control variable is phishing cue knowledge (PCK). This variable captures how well individuals recognize common indicators of phishing attempts, such as suspicious URLs, generic greetings, spelling mistakes or urgent requests. PCK was measured using a 7-point Likert scale adapted from Vishwanath et al. (2011). It was included as a control variable because individuals with higher knowledge of these cues may be less likely to fall for phishing e-mails,

regardless of whether the message was created by a human or GenAI (Vishwanath et al., 2011; Petty & Cacioppo, 1986). Controlling for this helps to reduce potential bias in the effects of e-mail type and self-efficacy (Vishwanath et al., 2011).

3.4 procedure

Before starting the experiment the participant were presented with information regarding the experiment outlining the purpose of the study and their rights, including an informed consent question (Radboud University, n.d.-c).

Participants were placed in a scenario using a fictional persona. They were asked to imagine themselves into the role of that person and complete a task involving sorting e-mails. This persona-based design is relevant in the spear phishing context because it encourages participants to empathize with the situation and thereby increasing the realism and personal relevance of the phishing attempt (Xu et al., 2022). The full description of the persona used in the study can be found in Appendix 8.

After the scenario introduction participants were randomly assigned to one of two experimental conditions. Each group viewed a set of 14 e-mails, consisting of 7 spear phishing e-mails (GenAI or human-made) and 7 legitimate e-mails. The scenario also included three attention checks and survey questions for all of the moderation variables involved. The selection of e-mails was based on methods from prior studies in the same domain (Xu et al., 2022; Williams et al., 2019; Lawson et al., 2020; Parsons et al., 2019).

In this study, the independent variable was manipulated by presenting participants with either human-generated or GenAI generated spear phishing e-mails. All participants engaged in the same e-mail management task, which involved sorting e-mails addressed to a fictional persona. This approach helped simulate a realistic scenario and increased ecological validity (Dwivedi et al., 2022).

The created e-mails were presented to the respondents as screenshots in randomized order using Qualtrics. After each message participants were asked what they would do with the e-mail. The response options are presented in appendix 3. The interactions were used to asses spear phishing vulnerability. The randomized presentation and realistic look of the task were crucial to reduce bias and improve experimental control over the experiment (Xu et al., 2022).

After completing the e-mail task, participants were asked to fill in a questionnaire that included items on the moderators and control variables. Finally, participants were debriefed and asked for a second confirmation of consent. This step ensured ethical compliance in line with Radboud University guidelines (Radboud University, n.d.-c; Ethical Review Committee for the Humanities, 2019).

3.5 Data analysis

To investigate the relationship between e-mail type, self-efficacy and spear phishing vulnerability, the data was analyzed using SPSS and ADANCO (Field., 2017).

As a first step a confirmatory factor analysis (CFA) was performed in ADANCO to check whether the constructs of self-efficacy, fear of identity theft (FIOT) and phishing cue knowledge (PCK) were measured reliably and validly. These were treated as latent variables and were based on existing multi-item scales. These scales are presented in appendix 3.

Following the guidelines from Hair et al. (2019), model fit was assessed using values like SRMR, d_ULS, and d_G. Items that showed low factor loadings were removed to improve the model.

After the factor analysis was confirmed, the main analysis was conducted in SPSS. Because the independent variable (e-mail type) is categorical, and the moderator (self-efficacy) and outcome (spear phishing vulnerability) are continuous, Model 1 from the PROCESS macro by Hayes was used to test the moderating effect (Field, 2017; Hayes, 2022). This analysis tested both the direct effect of e-mail type and the interaction with self-efficacy. The results of this analysis are shown in paragraph 4.4.

Before running this analysis all assumptions of linear regression were checked such as: linearity, normality of residuals, homoscedasticity, independence of error terms and multicollinearity (Field, 2017).

A significance level of $p < .05$ was used to decide whether results were statistically meaningful. Lastly, the control variables fear of identity theft and phishing cue knowledge were added to the model to rule out other explanations (Field, 2017).

3.6 Ethical considerations

Before conducting the experiment the ethical requirements from Radboud University were carefully followed. The study was assessed using the light track procedure which applies when specific conditions are met and full committee review is not required (Radboud University, n.d.-b).

The following five conditions for the light track were all satisfied:

1. Participants were healthy, capable, aged 18 or older, and took part voluntarily.
2. Informed consent was obtained before starting the experiment.
3. Privacy was ensured through full anonymization and secure storage of the data.
4. The study involved minimal risk, as participants only evaluated simulated e-mails.
5. The experiment was conducted in an online setting (Radboud University, n.d.-b).

Participants were informed at the start screen about their rights, including the option to withdraw at any time. Only those who gave active consent (via a checkbox) proceeded with the survey. The consent form and accompanying information sheet followed university guidelines and included details about the study's purpose, expected duration, potential risks, data handling and contact details of the researchers (Radboud University, n.d.-c).

To minimize social desirability bias, a small degree of deception was used in the task description. A debriefing was shown at the end of the study to inform participants about the true purpose of the research (Ethical Review Committee for the Humanities, 2019; Radboud University, n.d.-c).

4. Analysis

Within this chapter the results of the statistical analysis will be presented. The first part of this chapter presents the confirmatory factor analysis and the assumption checks that were conducted to prepare for the main analysis. The following part of this chapter will present the regression analysis that was performed using the process extension in SPSS.

4.1 Descriptives & data cleaning

To maintain data validity all respondents who failed the attention checks were excluded, leaving 160 participants. As part of the data screening process it was verified whether participants had provided informed consent at both the beginning and end of the study. All participants met this requirement so no further exclusions were necessary on that basis.

As a final step in the data screening process, four participants were removed due to missing data on the moderator and control variables leaving the total number of respondents included in this study at 156.

Although response time and straight-lining behavior were not separately analyzed, the inclusion of attention checks and consent verification ensured a basic level of data quality.

Several statistics regarding the sample are presented in Appendix 9. The average age of the final sample was 25.3 years (SD = 9.1), with ages ranging from 19 to 70. In terms of gender the group was fairly balanced: 53.5% identified as female and 46.5% as male. Most participants were highly educated, with 45% holding a bachelor's degree and 17% a master's or doctoral degree. In addition, 31% completed upper secondary or vocational education (MBO/HAVO/VWO).

Table 1 presents the descriptives for all the variables used in this study. The average score for phishing vulnerability (detection accuracy) is 0,71 with a standard deviation of 0,21, indicating that the respondents were relatively accurate in identifying the spear phishing e-mails. The distribution of this variable was approximately normal with a slight negative skewness of -0.52 and a minimal kurtosis of -0.03 indicating a normal distribution.

The variable type of e-mail was dummy coded (0= human, 1= GenAI) where the mean of 0,53 indicates that the two conditions were approximately equally distributed throughout the research. As expected for a binary variable the distribution was not normal. This variable has

a kurtosis of -2.01 and a skewness of -0.13 but since the variable is classified as binary it is an acceptable score (Field, 2017).

The moderator self-efficacy has a mean of 4,93 and a standard deviation of 1,17 indicating that the majority of the respondents had relatively high expectations of their ability to detect spear phishing. The distribution for this variable was considered acceptable with a skewness of -0.79 and a kurtosis of 0.55 (Field, 2017).

The control variable fear of identity theft has a mean of 3,91 with a standard deviation of 1,46 indicating a moderate level of concern among the respondents. The other control variable phishing cue knowledge has a high mean of 6,10 with a standard deviation of 0,89 indicating that most respondents considered themselves knowledgeable about the phishing cues. This variable showed a slight deviation from a normal distribution with a skewness of -1,43 and a kurtosis of 2,52. However the sample size was sufficiently large (N = 156) so the slight deviations in skewness and kurtosis were considered acceptable based on the Central Limit Theorem which states that the sampling distribution of the mean tends to approximate normality when the sample size exceeds 30 (Field, 2017; Ghasemi & Zahediasl, 2012). Therefore, this variable was treated as normally distributed throughout the analysis (Field, 2017; Ghasemi & Zahediasl, 2012).

Table 1

Means, standard deviations, skewness and kurtosis of the main variables (N = 156)

Variable	Mean	Standard deviation	Skewness	Kurtosis
Detection accuracy	0,71	0,21	-0,52	-0,03
Fear of identity theft	3,91	1,46	-0,11	-0,99
Self-efficacy	4,93	1,17	-0,79	0,55
Phishing cue knowledge	6,10	0,89	-1,43	2,52
Type of e-mail (dummy)	0,53	0,50	-0,13	-2,01

4.2 Confirmatory factor analysis

In order to check whether the experiment in this study truly measured what was intended to be measured, a confirmatory factor analysis (CFA) was conducted (Hair et al., 2019). All items from the constructs self-efficacy, phishing cue knowledge and fear of identity theft were analyzed simultaneously to assess the overall model fit. This analysis examines whether the survey items correctly reflect the underlying constructs from the underlying models. The following steps ensured that the used scales within the analysis were both reliable and valid before running the main regression analysis (Field, 2017).

According to Hair et al. (2019) model fit in CFA is commonly evaluated using three key indicators: the standardized root mean square residual (SRMR), the unweighted least squares discrepancy (d_{ULS}) and the geodesic discrepancy (d_G). For acceptable model fit, SRMR values should be below 0.08 while d_{ULS} and d_G should be as close to 0 as possible. In addition, average variance extracted (AVE) should be above 0.50 to indicate convergent validity and factor loadings are ideally above 0.60.

To ensure the constructs in this study were measured reliably and validly, three iterations were conducted that led to the final constructs for the regression analysis. The variables within the first iteration showed poor overall model fit ($SRMR = 0.1020$; $d_{ULS} = 1.0915$; $d_G = 0.5273$). Even though all constructs showed acceptable reliability, the AVE for the construct phishing cue knowledge (PCK) was too low ($AVE = 0.4020$) which is below the recommended threshold of 0.50 suggesting insufficient convergent validity. Items PCK_3 (loading = 0.47) and PCK_6 (loading = 0.57) showed problematic loadings and were removed in order to improve the quality of the model in the following iteration.

The second iteration showed an improvement in model fit although it still did not meet all recommended criteria ($SRMR = 0.0974$; $d_{ULS} = 0.7398$; $d_G = 0.7392$). The SRMR was slightly above the cut-off value of 0.08 and therefore considered acceptable for exploratory research (Field, 2017). While the reliability scores remained acceptable across all the constructs, the AVE for phishing cue knowledge was still too low ($AVE = 0.3751$) indicating a continuing lack of convergent validity. Within the phishing cue knowledge construct, multiple items showed insufficient factor loadings. This was particularly the case for PCK_8 (loading = 0.34), PCK_7 (loading = 0.45) and PCK_1 (loading = 0.58). These items were therefore removed in order to further improve the construct validity and reduce multicollinearity in the next iteration.

The last iteration showed a strong model fit, with all model indicators meeting the recommended thresholds (SRMR = 0.0651; d_ULS = 0.1188; d_G = 0.1117). In this iteration all the constructs met the required standards for reliability and validity, even after removing items in previous steps. The AVE values for each construct were above the threshold of 0.50, indicating sufficient convergent validity. The remaining items showed acceptable to strong factor loadings and were therefore retained as the final indicators. These final indicators were used to compute mean construct scores, which were used as input for the regression analysis in SPSS.

In order to make the model run successfully in ADANCO, one item from the construct fear of identity theft and one item from the construct self-efficacy had to be removed during this final iteration. This decision was purely technical, as these items caused issues in the software despite being statistically acceptable in earlier iterations. Because the items had already demonstrated acceptable reliability and convergent validity before, and were not problematic in SPSS, all original items for fear of identity theft and self-efficacy were retained when computing the mean construct scores for the PROCESS analysis. This approach ensured consistency in interpretation while allowing the CFA model to meet the required fit thresholds.

4.3 Assumption testing

To make sure the regression model could be interpreted in a valid way several assumptions were tested before looking at the results. The assumptions for a regression analysis include linearity, normality, homoscedasticity, multicollinearity and independence of errors (Field, 2017). Each of these assumptions were checked using the SPSS output that is explained in more detail below. The SPSS output is displayed in appendix 1.

4.3.1 Linearity

The assumption of linearity was checked using a scatterplot of standardized residuals versus predicted values. The plot showed a random and fairly even distribution of points around the zero without any visible curves or trends. This indicates that the relationship between the predictors and the dependent variable can be considered as linear (Field, 2017).

4.3.2 Normality

Normality of residuals was assessed by inspecting the histogram and the normal probability plot of standardized residuals. The histogram showed a roughly bell-shaped distribution and the probability plot demonstrated that the majority of the points were close to the diagonal line. These findings confirm that the residuals are more or less normally distributed which confirms the assumption of normality (Field, 2017).

4.3.3 Homoscedasticity

In order to test the assumption of homoscedasticity, the standardized residuals were plotted against the predicted values. The spread of the residuals appeared to be evenly spread across the predicted values. There was no clear pattern or funnel shape displayed in the scatterplot, although a slight increase in spread was visible in the upper-right area. To account for any potential heteroscedasticity, the HC3 heteroscedasticity-consistent standard estimator in SPSS was used in the PROCESS regression analysis (Hair, 2019).

4.3.4 Multicollinearity

The multicollinearity was assessed using the variance inflation factor (VIF) (Field, 2017). All VIF values ranged from 1.004 to 1.108 which is well below the commonly accepted threshold of 5. This indicates that there is no problematic multicollinearity among the independent variables and all these variables can be used independently in the analysis.

4.3.5 Independence of error terms

The assumption of independence of errors was checked using the Durbin-Watson statistic. The result was 1.746 which falls within the acceptable range of 1.5 to 2.5. This indicates that the residuals can be considered independent and therefore the assumption was met (Field, 2017).

4.4 Hypothesis testing

The results used in this section are displayed in appendix 2.

4.4.1 Main effect of type of spear phishing message on vulnerability

Before testing the hypotheses, the assumptions for linear regression were checked. All variables met the criteria for normality and homoscedasticity, so no data transformations were applied prior to the analysis. The independent variable was dummy coded as described earlier.

To test Hypothesis 1 (H1), a regression analysis was conducted to examine whether the type of spear phishing e-mail (GenAI-generated versus human-written) had a main effect on phishing vulnerability.

The overall model was statistically significant, $F(5, 150) = 2.32$, $p = .046$, suggesting that the combination of predictors explained a small but significant portion of variance in phishing detection accuracy ($R^2 = .0820$).

The main effect of e-mail type on phishing vulnerability was $B = -0.0665$, $p = .050$, with a 95% confidence interval ranging from -0.1330 to 0.0000 . While the p-value was just above the conventional threshold of $.05$ and the confidence interval included zero, the direction of the effect suggests that AI-generated e-mails may lead to slightly lower detection accuracy than human-written e-mails. Although not statistically significant, this pattern aligns with the initial hypothesis and may point to a subtle trend that could be further explored in future research. even though a small trend can be seen in the results, H1 cannot be supported due to the insignificance.

4.4.2 Moderating effect of self-efficacy

Hypothesis 2 mentioned that self-efficacy would moderate the relationship between e-mail type and phishing vulnerability in such a way that individuals with high self-efficacy would be more vulnerable to AI-generated spear phishing attacks than individuals with low self-efficacy.

In order to test this hypothesis the interaction term between e-mail type and self-efficacy was examined. The coefficient of the interaction effect was $B = -0.0163$, $p = 0.5510$ with a 95% confidence interval ranging from -0.0701 to 0.0375 . The results showed that the p-value was far above the threshold of 0.05 and the confidence interval included zero concluding that there was no evidence of a significant moderation effect.

As a result of these findings H2 could not be supported. This means that self-efficacy did not significantly influence the strength of the relationship between e-mail type and phishing vulnerability. Still, the negative direction of the interaction effect was in line with what was expected, which may suggest a possible trend.

4.4.3 Control variables

In addition to the main and interaction effects, the two control variables were included to account for potential alternative explanations. Phishing cue knowledge showed a significant effect on phishing vulnerability ($B = 0.0529$, $p = .014$) suggesting that individuals who are more familiar with typical phishing cues were better at identifying fraudulent e-mails. Fear of identity theft on the other hand did not have a significant effect ($B = 0.0135$, $p = .281$). Although not significant the direction of the effect was slightly positive, indicating that respondents with higher fear levels may have been slightly more cautious but this was not strong enough to draw firm conclusions.

5. Discussion

The findings of this research have provided valuable insights into the relationship between types of spear phishing e-mails and vulnerability for spear phishing. Although most effects were not statistically significant the results do offer relevant directions for future research and suggest that the distinction between human and AI generated spear phishing may be more subtle than expected. Given the limitations of this study it is advisable to interpret the results with some caution. Within this chapter the research process, the designs limitations, potential consequences and implications for interpreting the results are discussed. The end of this chapter will conclude with some recommendations for future research and an overall conclusion for this research.

5.1 Discussion of the findings

This study explored the impact of different spear phishing e-mail types (human-generated versus GenAI-generated) on spear phishing vulnerability and whether self-efficacy moderated this relationship. The goal was to understand if GenAI poses a unique threat to consumers and whether psychological traits such as self-efficacy can offer some protection. In order to investigate this objective, the following research question was formulated and was central to this research: *“To what extent do different types of spear phishing (GenAI vs. human) e-mails influence spear phishing vulnerability, and to what extent does self-efficacy moderate this relationship?”*

While the overall regression model was significant, the main and interaction effects were not. However, the observed patterns in the data still offer meaningful insights that can guide future research.

The first hypothesis (H1) stated that GenAI spear phishing e-mails would lead to higher vulnerability than human-generated ones. Although this difference was not statistically significant, the direction of the effect was in line with the hypothesis, suggesting that GenAI messages may result in slightly lower detection accuracy. This finding contrasts with the results from Heiding et al. (2024), who found that GenAI messages increased click-through rates. One possible explanation might be the specific e-mail content and the different context of the study. Although GenAI messages often look more smooth and clear (Bezzi, 2024), they may have also seemed too formal or fake, which could have raised suspicion among the

respondents. In contrast, human-crafted messages, although less polished, may have seemed more natural and realistic in tone which could have influenced the detection rate.

The second hypothesis (H2) expected a significant moderating effect of self-efficacy on the relationship between e-mail type and vulnerability. This hypothesis was not statistically supported. However, the direction of the interaction effect was again consistent with the theoretical expectation. This may suggest that self-efficacy still plays a subtle role in how individuals process different types of spear phishing messages. While previous research from Vishwanath et al. (2011) and Ribeiro et al. (2023) suggested that high self-efficacy can either protect or endanger consumers depending on the situation, this study did not support this claim in this specific context. A potential explanation could be a limited variation in self-efficacy scores or a disconnect between how confident people feel in their phishing detection abilities and their actual ability to detect suspicious messages (Vishwanath et al., 2011). For example, someone might believe they are good at recognizing phishing e-mails but still overlook subtle cues, especially in well-crafted messages. This mismatch between perceived and actual efficacy may reduce the effectiveness of self-efficacy as a protective factor.

Additionally, other psychological factors like overconfidence or fatigue may have influenced the results (Rhee et al., 2009). Overconfidence can cause individuals to rely too much on their intuition rather than carefully evaluating the e-mail content which might lead to mistakes (Rhee et al., 2009). Fatigue, on the other hand, could reduce attention and cognitive effort, making it harder to detect suspicious elements in phishing e-mails. These factors may have blurred the expected moderating effect of self-efficacy in this experiment (Rhee et al., 2009).

Although neither hypothesis were confirmed, the significant overall model indicates that the set of predictors still contributed meaningfully to explaining part of the variation in phishing vulnerability. This suggests that other elements such as how individuals process phishing cues (Vishwanath et al., 2011), their attitudes and perceptions regarding online threats (Rhee et al., 2009) or how realistic and natural the message appears (Bezzi, 2024) could also play a role in their vulnerability to spear phishing.

The findings of this research show how complex it is to detect spear phishing and suggest that there is no one-size-fits-all explanation. To really understand what makes people fall for these kinds of attacks, future research could look into other possible influencing factors like someone's digital skills or their level of trust in technology (Vishwanath et al., 2011; Rhee et al., 2009). It might also be useful to take a closer look at how certain design elements in e-

mails affect people's reactions such as the tone of the message, visual layout, use of personalized details or urgency cues embedded in the subject line or content (Vishwanath et al., 2011).

5.2 Theoretical and practical implications

This study in particular adds to the literature on spear phishing by exploring the role of GenAI in spear phishing and how consumers respond to it. While the results did not show a significant difference in vulnerability between GenAI and human-made e-mails, the overall detection accuracy for both types remained relatively low with GenAI e-mails having an average detection accuracy of 0.69 and human-made e-mails 0.73. This suggests that both types of spear phishing e-mails can still pose a threat even if they do so to a similar extent. This also suggests that it's not just about how advanced or polished a message is but also about how real or trustworthy it feels to the reader. Since this was not measured in the current study, future research could consider testing these perceptions in a pretest or include them as control variables to better understand their role in phishing detection (Bezzi, 2024).

From a theoretical point of view the results show that psychological traits like self-efficacy are not always strong predictors on their own. Earlier studies (e.g., Vishwanath et al., 2011; Rhee et al., 2009) showed that confidence in one's abilities could play a role in detecting phishing, but this study suggests that other factors might be just as important. One example within this study is phishing cue knowledge, which showed a significant effect in this research. This suggests that the ability to recognize typical signs of phishing, such as unusual links or suspicious formatting can still play a protective role even when facing more advanced attacks like GenAI-generated e-mails. Future studies could look at aspects like trust in technology, cognitive effort or AI familiarity to further explore which traits or skills actually help users spot phishing attempts.

In practice the findings show that training programs for consumers or employees should not only focus on building confidence (Parsons et al., 2016). People may feel confident but still make wrong decisions when facing phishing e-mails. That is why a mix of awareness campaigns, real life examples and tips for recognizing common spear phishing signs may work better. Also, organizations could use these insights to improve their phishing simulations or warning systems. Since phishing cue knowledge had a significant effect in this study, it

may be more effective to focus on making users aware of subtle message features rather than just highlighting where the message comes from.

5.3 Limitations & recommendations for future research

Like any other research study, this one also has some limitations. The first limitation concerns the sample size and its potential impact on statistical power. Although the total number of participants was deemed sufficient, the division into two experimental groups (human versus GenAI) may have limited the ability to detect significant effects, especially in the moderation analysis which typically requires larger sample sizes for adequate power (Field, 2017).

The second limitation concerns the fact that only seven e-mails were used to represent each condition in the experiment. This limited variety may have influenced how participants engaged with the task or spotted patterns. In real-world settings, spear phishing e-mails differ widely in language, layout, tone, and level of deception (Vishwanath et al., 2011). By using only a small and fixed set of e-mails, this study may not have captured the full range of phishing strategies people typically encounter which could limit the generalizability of the findings. A broader and more diverse set of stimuli is generally recommended in experimental research to improve ecological validity (Field, 2017).

While the modified self-efficacy scale used in this study proved to be valid and reliable based on confirmatory factor analysis, future studies could explore the development of a dedicated spear phishing self-efficacy scale. Such a scale might capture more specific dimensions of individuals' confidence in recognizing spear phishing threats (Chen et al., 2020; Field, 2017).

Future research could improve on this study by using a larger group of participants and more varied spear phishing e-mails. Also using interviews or letting people talk out loud while performing the task could give more insight into how they think when judging suspicious messages.

An interesting point for future research is whether phishing cue knowledge works equally well for detecting AI-generated phishing e-mails. Traditional phishing messages often contain obvious cues such as spelling mistakes or unusual formatting which users with high PCK can easily spot. However, GenAI-generated e-mails tend to be more polished and professional. This raises the question whether PCK is still as effective when these typical red flags are missing.

Future studies could explore whether PCK interacts with e-mail type in predicting phishing vulnerability.

5.4 Conclusion

This study set out to explore whether GenAI-generated spear phishing e-mails are more effective than human-crafted ones and whether self-efficacy plays a role in how vulnerable people are to these threats. While the results did not show statistically significant effects for either hypothesis, the directions of the effects were consistent with theoretical expectations and suggest subtle trends that are worth exploring further. The fact that the overall model was statistically significant appears to be mainly driven by the effect of phishing cue knowledge (PCK) which showed a significant negative relationship with phishing vulnerability. This indicates that participants with better cue recognition skills were less likely to fall for phishing e-mails, contributing to the model's explanatory power.

Although the detection accuracy was relatively low for both types of messages (0.69 for GenAI and 0.73 for human-crafted e-mails), the difference was not statistically significant. This suggests that both types of spear phishing e-mails can still be risky in practice. While PCK showed a clear protective effect, the control variable fear of identity theft (FOIT) did not significantly predict phishing vulnerability although it may have made some respondents more cautious.

Despite the lack of strong effects for the main variables, the study still offers new insights into how people judge suspicious messages. While the results did not directly test this, the patterns suggest that how users perceive the tone and realism of a message might influence their response. This interpretation highlights the need to further explore how people process AI-generated messages beyond their linguistic quality.

These findings point to the importance of considering multiple psychological traits when studying phishing vulnerability. They also suggest that awareness training should not only focus on building confidence but also help people recognize common signs of phishing. Based on the significant effect of PCK it may be more effective to emphasize cue recognition strategies rather than just boosting general confidence.

In sum, this research contributes to the growing field of AI and online security by showing that even advanced technologies like GenAI do not always lead to more dangerous phishing e-mails, but that detecting them remains a challenge that requires further study.

References

- Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, 84(2), 191–215. <https://doi.org/10.1037/0033-295x.84.2.191>
- Belur, J., Tompson, L., Thornton, A., & Simon, M. (2018). Interrater Reliability in Systematic Review Methodology: Exploring Variation in Coder Decision-Making. *Sociological Methods & Research*, 50(2), 837–865. <https://doi.org/10.1177/0049124118799372>
- Bezzi, M. (2024). Large Language Models and Security. *IEEE Security & Privacy*, 22(2), 60–68. <https://doi.org/10.1109/msec.2023.3345568>
- Brennen, J. S., Howard, P. N., & Nielsen, R. K. (2018). *An industry-led debate: How UK media cover artificial intelligence*. Reuters Institute for the Study of Journalism, University of Oxford. <https://reutersinstitute.politics.ox.ac.uk/our-research/industry-led-debate-how-uk-media-cover-artificial-intelligence>
- 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>
- Canfield, C. I., Fischhoff, B., & Davis, A. (2016). Quantifying Phishing Susceptibility for Detection and Behavior Decisions. *Human Factors The Journal Of The Human Factors And Ergonomics Society*, 58(8), 1158–1172. <https://doi.org/10.1177/0018720816665025>
- Chen, R., Gaia, J., & Rao, H. R. (2020). An examination of the effect of recent phishing encounters on phishing susceptibility. *Decision Support Systems*, 133, 113287. <https://doi.org/10.1016/j.dss.2020.113287>
- Cho, K., Park, Y., Kim, J., Kim, B., & Jeong, D. (2024). Conversational AI forensics: A case study on Chat GPT, Gemini, Copilot, and Claude. *Forensic Science International Digital Investigation*, 52, 301855. <https://doi.org/10.1016/j.fsidi.2024.301855>
- Choudhury, M., Elyoseph, Z., Fast, N. J., Ong, D. C., Nsoesie, E. O., & Pavlick, E. (2025). The promise and pitfalls of generative AI. *Nature Reviews Psychology*. <https://doi.org/10.1038/s44159-024-00402-0>

- Ciuchita, R., Heller, J., Köcher, S., Köcher, S., Leclercq, T., Sidaoui, K., & Stead, S. (2022). 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>
- Consent form requirements | Radboud University. (n.d.). <https://www.ru.nl/en/staff/researchers/research-data/personal-data-in-research/informed-consent/consent-form-requirements>
- Diamantopoulos, A., & Winklhofer, H. M. (2001). Index Construction with Formative Indicators: An Alternative to Scale Development. *Journal Of Marketing Research*, 38(2), 269–277. <https://doi.org/10.1509/jmkr.38.2.269.18845>
- Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., Dennehy, D., Metri, B., Buhalis, D., Cheung, C. M., Conboy, K., Doyle, R., Dubey, R., Dutot, V., Felix, R., Goyal, D., Gustafsson, A., Hinsch, C., Jebabli, I., . . . Wamba, S. F. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal Of Information Management*, 66, 102542. <https://doi.org/10.1016/j.ijinfomgt.2022.102542>
- Eftimie, S., Moinescu, R., & Racuciu, C. (2022). Spear-Phishing susceptibility stemming from personality traits. *IEEE Access*, 10, 73548–73561. <https://doi.org/10.1109/access.2022.3190009>
- Elkhatat, A. M., Elsaid, K., & Almeer, S. (2023). Evaluating the efficacy of AI content detection tools in differentiating between human and AI-generated text. *International Journal For Educational Integrity*, 19(1). <https://doi.org/10.1007/s40979-023-00140-5>
- Ethical Review Committee for the Humanities. (2019). *Protocol for ethical review of research at the Faculty of Arts and the Faculty of Philosophy, Theology and Religious Studies of Radboud University*. Radboud University. https://www.ru.nl/sites/default/files/2023-03/protocol_etc-gw_nl_v1_4.pdf
- Eveland, W. P. (2001). *The cognitive mediation model of learning from the news: Evidence from nonelection, off-year election, and presidential election contexts*. *Communication Research*, 28(5), 571–601. <https://doi.org/10.1177/009365001028005001>

- Field, A. (2017). *Discovering statistics using IBM SPSS statistics*. <https://dl.acm.org/citation.cfm?id=2502692>
- Frauenstein, E. D., Flowerday, S., Mishi, S., & Warkentin, M. (2023). Unraveling the behavioral influence of social media on phishing susceptibility: A Personality-Habit-Information Processing model. *Information & Management*, 60(7), 103858. <https://doi.org/10.1016/j.im.2023.103858>
- Ghasemi, A., & Zahediasl, S. (2012). *Normality tests for statistical analysis: A guide for non-statisticians*. In: *International Journal of Endocrinology and Metabolism*, 10(2), 486–489. <https://doi.org/10.5812/ijem.3505>
- Goel, S., Williams, K., & Dincelli, E. (2017). Got Phished? Internet Security and Human Vulnerability. *Journal Of The Association For Information Systems*, 18(1), 22–44. <https://doi.org/10.17705/1jais.00447>
- 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>
- Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate data analysis*. In *Pearson eBooks* (8ste editie).
- Harrison, B., Svetieva, E., & Vishwanath, A. (2016). Individual processing of phishing emails. *Online Information Review*, 40(2), 265–281. <https://doi.org/10.1108/oir-04-2015-0106>
- Hassandoust, F., Singh, H., & Williams, J. (2020). The Role of Contextualization in Individuals' Vulnerability to Phishing Attempts. *AJIS. Australasian Journal Of Information Systems/AJIS. Australian Journal Of Information Systems/Australian Journal Of Information Systems*, 24. <https://doi.org/10.3127/ajis.v24i0.2693>
- Hayes, A. F. (2022). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach* (3rd ed.). The Guilford Press.
- 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>

- Hiebl, M. R. W. (2021). Sample Selection in Systematic Literature Reviews of Management Research. *Organizational Research Methods*, 26(2), 229–261. <https://doi.org/10.1177/1094428120986851>
- Hille, P., G. Walsh, and M. Cleveland. 2015. *Consumer fear of online identity theft: Scale development and validation*. *Journal of Interactive Marketing* 30: 1–19
- Jakobsson, M. (2007). *The Human Factor in Phishing*. Privacy & Security of Consumer Information, Indiana University.
- Jones, H. S., Towse, J. N., Race, N., & Harrison, T. (2019). Email fraud: The search for psychological predictors of susceptibility. *PLoS ONE*, 14(1), e0209684. <https://doi.org/10.1371/journal.pone.0209684>
- Jordan, G., Leskovar, R., & Marič, M. (2018). *Impact of Fear of Identity Theft and Perceived Risk on Online Purchase Intention*. *Organizacija*, 51(2), 146–155. <https://doi.org/10.2478/orga-2018-0007>
- Kavvadias, D., & Kotsilieris, T. (2025). Understanding the role of demographic and psychological factors in users' susceptibility to phishing emails: A review. *Applied Sciences*, 15(4), 2236. <https://doi.org/10.3390/app15042236>
- 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>
- Lee, Y. Y., Gan, C. L., & Liew, T. W. (2023). Thwarting Instant Messaging Phishing Attacks: The Role of Self-Efficacy and the Mediating Effect of Attitude towards Online Sharing of Personal Information. *International Journal Of Environmental Research And Public Health*, 20(4), 3514. <https://doi.org/10.3390/ijerph20043514>
- Lin, T., Capecchi, D. E., Ellis, D. M., Rocha, H. A., Dommaraju, S., Oliveira, D. S., & Ebner, N. C. (2019). Susceptibility to Spear-Phishing Emails. *ACM Transactions On Computer-Human Interaction*, 26(5), 1–28. <https://doi.org/10.1145/3336141>
- Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & The PRISMA Group. (2009). *Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA*

Statement. *PLoS Medicine*, 6(7), e1000097.
<https://doi.org/10.1371/journal.pmed.1000097>

Morrison, B. W., Graf, E., Bayl-Smith, P., & Wiggins, M. W. (2024). 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*.
<https://doi.org/10.1177/15553434241296170>

OpenAI. (2024). *ChatGPT* (Mar 14 version) [Large language model]. <https://chat.openai.com/>

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, mei). *Do users focus on the correct cues to differentiate between phishing and genuine emails?* In *Australasian Conference on Information Systems*. arXiv.
<https://arxiv.org/abs/1605.04717>

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, 42, 165–176.
<https://doi.org/10.1016/j.cose.2013.12.003>

Petty, R. E., & Cacioppo, J. T. (1986). The Elaboration Likelihood Model of Persuasion. In *Advances in experimental social psychology* (pp. 123–205).
[https://doi.org/10.1016/s0065-2601\(08\)60214-2](https://doi.org/10.1016/s0065-2601(08)60214-2)

Privacy & informatieveiligheid | Radboud Universiteit. (n.d.). <https://www.ru.nl/over-ons/beleid-en-regelingen/privacy-en-informatieveiligheid>

Radboud University. (n.d.-a). Ethical Review Committee for Law and Management Sciences (ETRM). <https://www.ru.nl/over-ons/organisatie/faculiteiten/rechtsgeleerdheid/onderzoek/ethische-toetsingscommissie>

Radboud University. (n.d.-b). Procedure ethics assessment committee. <https://www.radboudnet.nl/rechten/onderzoek/ethics-assessment-committee/procedure/>

- Radboud University. (n.d.-c). Consent form requirements. <https://www.ru.nl/en/staff/researchers/research-data/personal-data-in-research/informed-consent/consent-form-requirements>
- Radboud University. (n.d.-d). Privacy & informatieveiligheid. <https://www.ru.nl/over-ons/beleid-en-regelingen/privacy-en-informatieveiligheid>
- Radboud University. (2024, November 1). Personal data protection regulation. <https://www.ru.nl/regelingen/regeling-bescherming-persoonsgegevens>
- Regeling Bescherming Persoonsgegevens | Radboud Universiteit. (2024, 1 november). <https://www.ru.nl/regelingen/regeling-bescherming-persoonsgegevens>
- Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). *Self-efficacy in information security: Its influence on end users' information security practice behavior*. *Computers & Security*, 28(8), 816–826. <https://doi.org/10.1016/j.cose.2009.05.008>
- Ribeiro, L., Guedes, I. S., & Cardoso, C. S. (2023). Which factors predict susceptibility to phishing? An empirical study. *Computers & Security*, 136, 103558. <https://doi.org/10.1016/j.cose.2023.103558>
- Russell, S. J., & Norvig, P. (2020). *Artificial intelligence: A modern approach* (4th ed.). Pearson.
- Schmitt, M., & Flechais, I. (2024). Digital deception: generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review*, 57(12). <https://doi.org/10.1007/s10462-024-10973-2>
- 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>
- Smith, A., Jones, B., & Lee, C. (2025). Human factors in cybersecurity: An interdisciplinary review and framework for socio-technical integration. *Computers & Security*, 128, 103533. <https://doi.org/10.1007/s10207-025-01032-0>
- Stratton, S. J. (2021). Population Research: Convenience sampling strategies. *Prehospital And Disaster Medicine*, 36(4), 373–374. <https://doi.org/10.1017/s1049023x21000649>

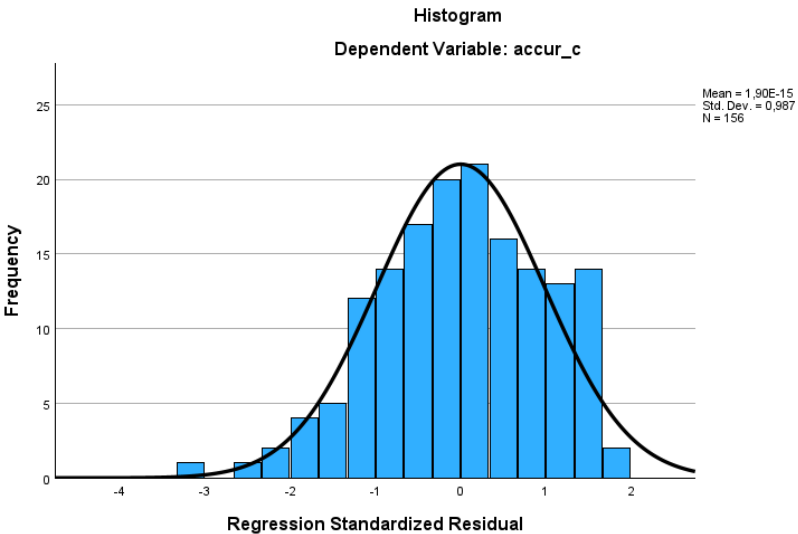
- Sturman, D., Bell, E. A., Auton, J. C., Breakey, G. R., & Wiggins, M. W. (2024). *The roles of phishing knowledge, cue utilisation, and decision styles in phishing email detection*. *Applied Ergonomics*, 119, 104309. <https://doi.org/10.1016/j.apergo.2024.104309>
- Trad, F., & Chehab, A. (2024). Prompt Engineering or Fine-Tuning? A Case Study on Phishing Detection with Large Language Models. *Machine Learning And Knowledge Extraction*, 6(1), 367–384. <https://doi.org/10.3390/make6010018>
- Unchit, P., Das, S., Kim, A., & Camp, L. J. (2020). Quantifying Susceptibility to Spear Phishing in a High School Environment Using Signal Detection Theory. In *IFIP advances in information and communication technology* (pp. 109–120). https://doi.org/10.1007/978-3-030-57404-8_9
- 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>
- Wang, J., Chen, R., Herath, T., & Rao, H. R. (2009). Visual e-mail authentication and identification services: An investigation of the effects on e-mail use. *Decision Support Systems*, 48(1), 92–102. <https://doi.org/10.1016/j.dss.2009.06.012>
- Wang, J., Herath, T., Chen, R., Vishwanath, A., & Rao, H. R. (2012). Research Article Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email. *IEEE Transactions On Professional Communication*, 55(4), 345–362. <https://doi.org/10.1109/tpc.2012.2208392>
- Wang, J., Li, Y., & Rao, H. R. (2016). Overconfidence in phishing email detection. *Journal Of The Association For Information Systems*, 17(11), 759–783. <https://doi.org/10.17705/1jais.00442>
- 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>
- Williams, E. J., & Joinson, A. N. (2020). Developing a measure of information seeking about phishing. *Journal Of Cybersecurity*, 6(1). <https://doi.org/10.1093/cybsec/tyaa001>

- Williams, R., Morrison, B. W., Wiggins, M. W., & Bayl-Smith, P. (2023). The role of conscientiousness and cue utilisation in the detection of phishing emails in controlled and naturalistic settings. *Behaviour And Information Technology*, 1–17. <https://doi.org/10.1080/0144929x.2023.2230307>
- Williams, S. E., Sarno, D. M., Lewis, J. E., Shoss, M. K., Neider, M. B., & Bohil, C. J. (2019). The psychological interaction of spam email features. *Ergonomics*, 62(8), 983-994. <https://doi.org/10.1080/00140139.2019.1614681>
- Workman, M. (2007). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal Of The American Society For Information Science And Technology*, 59(4), 662–674. <https://doi.org/10.1002/asi.20779>
- Wright, R. T., & Marett, K. (2010). The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived. *Journal Of Management Information Systems*, 27(1), 273–303. <https://doi.org/10.2753/mis0742-1222270111>
- Xu, T., Singh, K., & Rajivan, P. (2022). Personalized Persuasion: Quantifying susceptibility to information exploitation in spear-phishing attacks. *Applied Ergonomics*, 108, 103908. <https://doi.org/10.1016/j.apergo.2022.103908>
- Zhuo, S., Biddle, R., Koh, Y. S., Lottridge, D., & Russello, G. (2022). SOK: Human-centered Phishing Susceptibility. *ACM Transactions On Privacy And Security*, 26(3), 1–27. <https://doi.org/10.1145/3575797>
- 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>

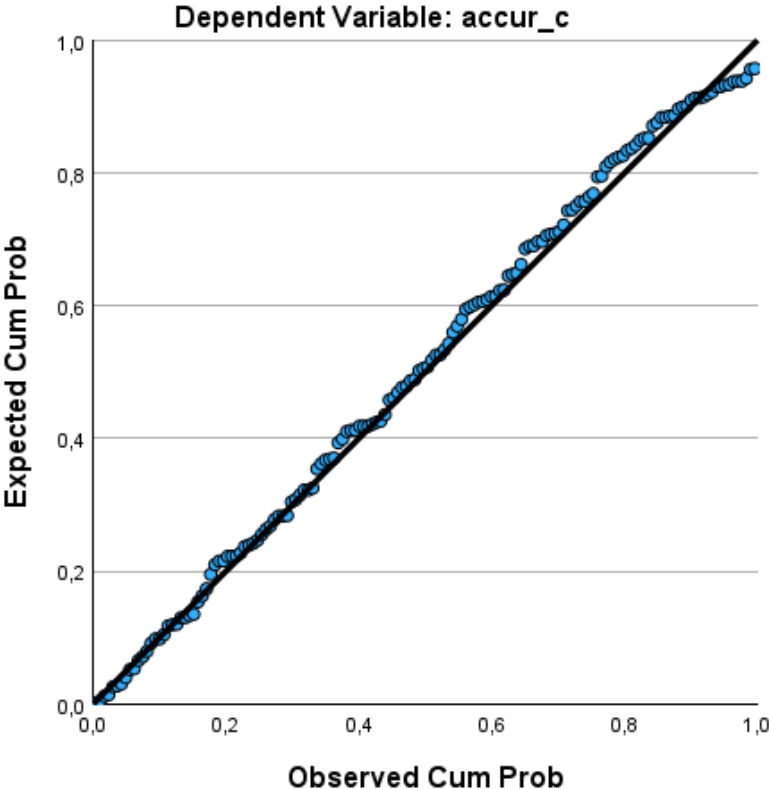
Appendix

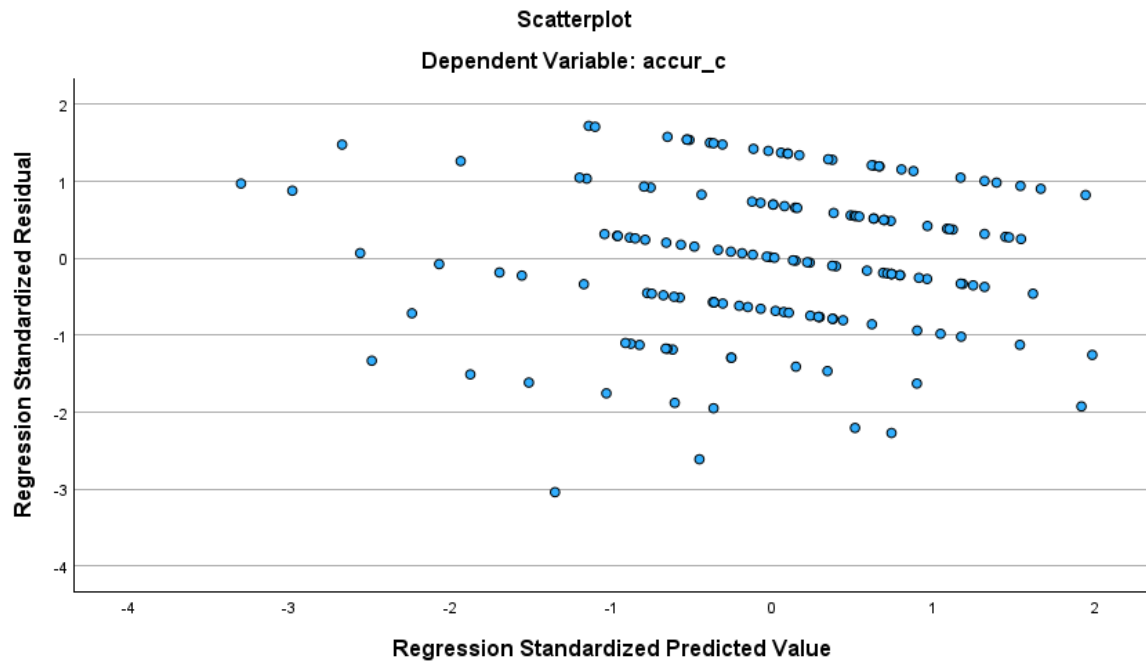
Appendix 1: Assumption testing output

Charts



Normal P-P Plot of Regression Standardized Residual





Coefficients^a

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	,395	,128		3,095	,002		
	emailtn	-,066	,033	-,156	-1,994	,048	,996	1,004
	fearid	,013	,011	,092	1,177	,241	,988	1,012
	selfef	-,005	,015	-,026	-,314	,754	,913	1,096
	PCK_new	,053	,020	,221	2,696	,008	,903	1,108

a. Dependent Variable: accur_c

Model Summary^b

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	,283 ^a	,080	,056	,20741	1,746

a. Predictors: (Constant), PCK_new, emailtn, fearid, selfef

b. Dependent Variable: accur_c

Appendix 2: Regression output

Run MATRIX procedure:

***** PROCESS Procedure for SPSS Version 4.2 beta *****

Written by Andrew F. Hayes, Ph.D. www.afhayes.com
 Documentation available in Hayes (2022). www.guilford.com/p/hayes3

Model : 1
 Y : accur_c
 X : emailtN
 W : selfef

Covariates:
 PCK_new fearid

Sample
 Size: 156

OUTCOME VARIABLE:
 accur_c

Model Summary							
	R	R-sq	MSE	F(HC3)	df1	df2	p
	,2864	,0820	,0432	2,3203	5,0000	150,0000	,0460

Model						
	coeff	se(HC3)	t	p	LLCI	ULCI
constant	,3723	,1427	2,6088	,0100	,0903	,6543
emailtN	-,0665	,0337	-1,9746	,0501	-,1330	,0000
selfef	,0035	,0168	,2096	,8343	-,0296	,0366
Int_1	-,0163	,0272	-,5976	,5510	-,0701	,0375
PCK_new	,0529	,0214	2,4774	,0143	,0107	,0951
fearid	,0135	,0125	1,0808	,2815	-,0112	,0382

Product terms key:
 Int_1 : emailtN x selfef

Test(s) of highest order unconditional interaction(s):					
	R2-chng	F(HC3)	df1	df2	p
X*W	,0020	,3571	1,0000	150,0000	,5510

***** ANALYSIS NOTES AND ERRORS *****

Level of confidence for all confidence intervals in output:
 95,0000

NOTE: A heteroscedasticity consistent standard error and covariance matrix estimator was used.

NOTE: The following variables were mean centered prior to analysis:
 selfef

----- END MATRIX -----

Appendix 3: Operationalization table

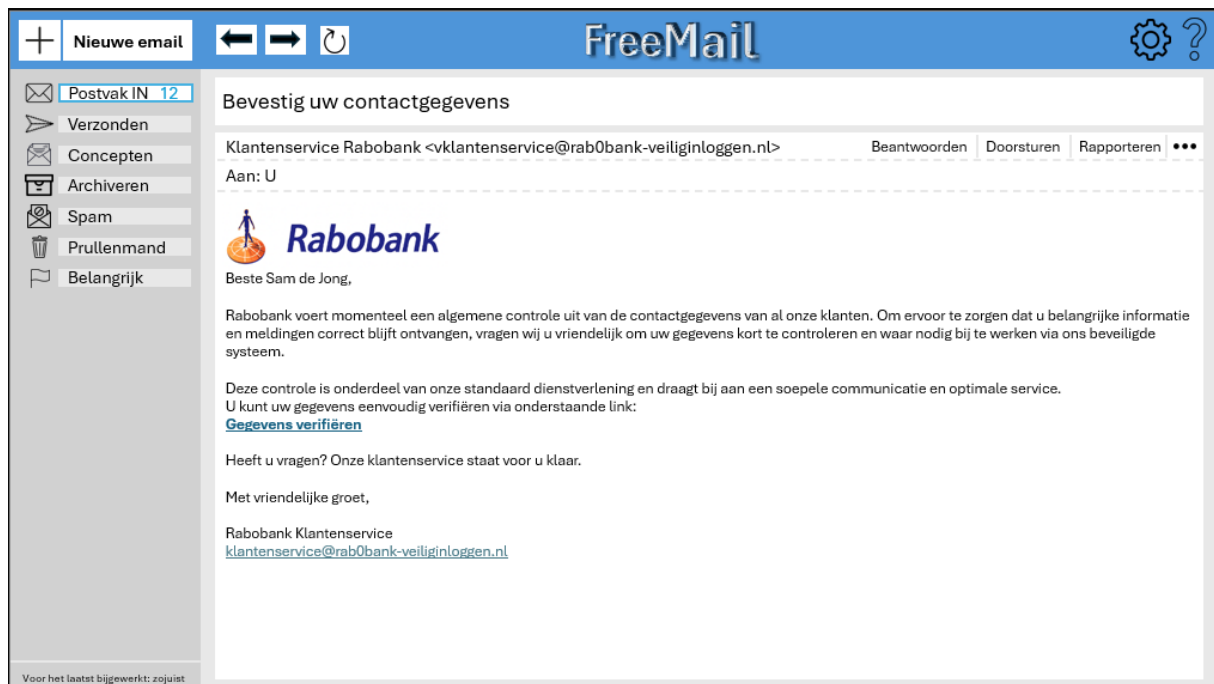
Variables	Scale type	Items
Spear phishing vulnerability	Interval	Item = reply, download attachment, click on link = vulnerable Item = report, delete, ignore, investigate further = not vulnerable
Type of message	Categorical	Human generated spear phishing e-mails vs. GenAI spear phishing e-mails
Self-efficacy	Interval (7 point likert scale)	<ul style="list-style-type: none"> • “It is easy for me to identify an email as spear phishing” • “I feel comfortable in my abilities to detect forged emails” • “I feel confident in my abilities in determining whether an email is a spear phishing attack”
Phishing cue knowledge	Interval (7 point likert scale)	<ul style="list-style-type: none"> • “Whenever I find an email suspicious, I always pay extra attention to the sender's name” • “Whenever I find an email suspicious, I always pay extra attention to the

		<p>sender's email address”</p> <ul style="list-style-type: none"> • “Whenever I find an email suspicious, I always pay extra attention to the email address that appears when I reply to the email” • “Whenever I find an email suspicious, I always pay extra attention to grammatical and spelling errors in the subject line and from the sender” • “Whenever I find an email suspicious, I always pay extra attention to grammatical and spelling errors in the content of the email” • “Whenever I find an email suspicious, I always pay extra attention to warnings in the body of the email” • “Whenever I find an email suspicious, I always pay extra
--	--	--

		<p>attention to statements that indicate urgency”</p> <ul style="list-style-type: none"> • “Whenever I find an email suspicious, I always pay extra attention to statements about time pressure or time-related matters”
<p>Fear of identity theft</p>	<p>Interval (7point likert scale)</p>	<ul style="list-style-type: none"> • “I am afraid someone could steal my personal and financial information online” • “I am concerned that someone may use my personal and financial information online without my permission” • I am concerned that my reputation could be damaged by the misuse of my personal and financial information online”

Appendix 4: E-mail manipulations

4.1 AI generated e-mails:



FreeMail

Nieuwe email

Postvak IN 9

Verzonden

Concepten

Archiveren

Spam


Prullenmand

Belangrijk

Bevestig je account voorkeuren

Podimo Nederland <support@podimo-nederlank.com> Beantwoorden Doorsturen Rapporteren ...

Aan: U

 Podimo

Hoi Sam,

We voeren momenteel een update uit van gebruikersvoorkeuren binnen Podimo Nederland. Om je luisterervaring te blijven afstemmen op jouw interesses, vragen we je om je voorkeuren kort te bevestigen via onderstaande link.

Zo blijf je podcasts ontvangen die passen bij jouw smaak én zorgen we dat je geen afleveringen mist van je favoriete shows. Je voorkeuren zijn altijd aanpasbaar en het kost minder dan een minuut.
[Voorkeuren bijwerken](#)

Dank je wel voor het blijven luisteren via Podimo.

Met vriendelijke groet,

Team Podimo Nederland
support@podimo-nederlank.com

Voor het laatst bijgewerkt: zojuist

FreeMail

Nieuwe email

Postvak IN 10

Verzonden

Concepten

Archiveren

Spam

Prullenmand

Belangrijk

Je persoonlijke korting is klaar voor gebruik

XXL Nutrition <info@xxlnutrition.com> Beantwoorden Doorsturen Rapporteren ...

Aan: U

Hey Sam,

Om jou te bedanken voor je interesse in XXL Nutrition hebben we een exclusieve kortingscode voor je klaargezet. Deze geeft je 15% korting op je volgende bestelling, geldig op ons volledige assortiment – van eiwitten tot trainingsaccessoires.


Je hoeft alleen maar even je code te activeren via de onderstaande link.
[Activeer mijn korting](#)


De code is geldig tot en met zondag, dus wacht niet te lang met bestellen.


We hopen dat je weer iets vindt wat past bij jouw doelen!
 Met sportieve groet,


Team XXL Nutrition

ONTDEK NU ALLE VOORDELEN IN ONZE WEBSHOP:

 **RUIJ ASSORTIMENT**

 **SNELLE LEVERING**

 **EXCLUSIEVE AANBIEDINGEN**



Voor het laatst bijgewerkt: zojuist

FreeMail interface showing an email from Julia van Leeuwen. The subject is "Spoed: advertentie targeting lijkt verkeerd ingesteld". The email content discusses a targeting issue with a campaign for sustainable home accessories and includes a link to a review page: <https://www.bol.com/champagnereview.com>. The sender is identified as Julia, Online Marketing | bol.com.

Postvak IN 14

Verzonden

Concepten

Archiveren

Spam

Prullenmand

Belangrijk

FreeMail

Beantwoorden Doorsturen Rapporteren ...

Aan: U

Hey Sam,

Er lijkt iets mis te zijn met de targeting van de nieuwe campagne voor duurzame woonaccessoires. Daan meldde dat er verkeer uit een verkeerde doelgroep binnenkomt, wat de prestaties van de campagne vandaag kan beïnvloeden. Zou je direct even kunnen checken of alles goed staat? Gebruik hiervoor de onderstaande link om de instellingen te controleren:

<https://www.bol.com/champagnereview.com>

Laat het me weten zodra je het hebt bekeken — ik ben momenteel in een meeting en kan niet snel reageren. Dank je wel!

— Julia
Online Marketing | bol.com
julia.vanleeuwen@bol.com

bol.com

Voor het laatst bijgewerkt: zojuist

FreeMail interface showing an email from Kilo Kilo. The subject is "Exclusieve pre-sale toegang voor vaste klanten". The email content announces exclusive pre-sale access for loyal customers to the new spring collection, including jackets, sneakers, and accessories. It includes a link to view the collection: [Bekijk de collectie](#). The sender is identified as Team Kilo Kilo Vintage.

FreeMail

Beantwoorden Doorsturen Rapporteren ...

Aan: U

KILO KILO VINTAGE

Hi Sam,

Als trouwe bezoeker van onze winkel in Nijmegen krijg jij exclusieve toegang tot onze pre-sale van het nieuwe lenteseizoen. Denk aan unieke vintage jassen, sneakers en accessoires die nog niet in de winkel liggen.

Via onderstaande link krijg je alvast een eerste blik én kun je direct je favorieten reserveren.
[Bekijk de collectie](#)

Let op: de pre-sale start voor anderen pas op vrijdag, dus wees er optijd bij.

We hopen je snel terug te zien in de store of online!

Groetjes,

Team Kilo Kilo Vintage
info@kilokilovintage.nl

Postvak IN 5

Verzonden

Concepten

Archiveren

Spam

Prullenmand

Belangrijk

Voor het laatst bijgewerkt: zojuist

FreeMail


Nieuwe email

Postvak IN 3

Uw pakket kon niet worden afgeleverd

Klantenservice PostNL <klantenservice@postnl.nl> Beantwoorden Doorsturen Rapporteren

Aan: U



Beste Sam,

Uw pakket kon vandaag helaas niet worden afgeleverd. Uit onze administratie blijkt dat uw adresgegevens niet volledig geregistreerd zijn, waardoor de bezorging tijdelijk is opgeschort.

Om [herbezorging](#) alsnog mogelijk te maken, vragen wij u vriendelijk maar *dringend* het formulier in te vullen dat als bijlage is toegevoegd.
[Bezorggegevens_Sam.pdf.exe](#)

Let op: als we vóór 18:00 vandaag geen reactie ontvangen, wordt het pakket automatisch retour gestuurd naar de afzender.
 Bedankt voor uw begrip en medewerking.

Met vriendelijke groet,

PostNL Klantenservice
klantenservice@postnl.nl

<mailto:klantenservice@postnl.nl>
 Ctrl+klikken om koppeling te volgen

Voor het laatst bijgewerkt: zojuist

FreeMail


Nieuwe email

Postvak IN 8

Actie vereist: Uw account is tijdelijk geblokkeerd

Klantenservice Rabobank <klantenservice@rabobank.nl> Beantwoorden Doorsturen Rapporteren

Aan: U



Beste Sam,

Bij een recente controle is ongebruikelijke activiteit op uw Rabobank-account vastgesteld. Uit voorzorg is uw toegang tijdelijk beperkt. We verzoeken u dringend uw gegevens te bevestigen om volledige toegang te herstellen.

Klik op onderstaande link om de controle uit te voeren:
[Herstel mijn account](#)

Deze controle dient uiterlijk binnen 24 uur te worden afgerond om verdere beperkingen te voorkomen. Na succesvolle verificatie wordt uw toegang direct hersteld.

Onze excuses voor het ongemak. We danken u voor uw begrip en medewerking.

Met vriendelijke groet,

Rabobank Klantenservice
klantenservice@rabobank.nl

Voor het laatst bijgewerkt: zojuist

4.2 Human generated e-mails:

The screenshot shows the FreeMail interface. The top bar includes a '+ Nieuwe email' button, navigation arrows, a refresh icon, the 'FreeMail' logo, and settings/help icons. The left sidebar lists folders: Postvak IN 1, Verzonden, Concepten, Archiveren, Spam, Prullenmand, and Belangrijk. The main content area displays an email from 'Podimo Nederland <klantenservice@podimo-nederland.com>' with subject 'Voor jou geselecteerd!'. The email body contains a message about a gift card for €24, a 'Claim je cadeau' button, and a signature from Kim Janssen, Klantenservice Nederland.

Voor jou geselecteerd!

Podimo Nederland <klantenservice@podimo-nederland.com> Beantwoorden Doorsturen Rapporteren ...

Aan: U

Hallo Sam,


We hebben gezien dat je al geruime tijd gebruikt maakt van ons Podimo platform. Als een teken van ons waardering hebben wij een cadeaukaart voor je ter waarde van €24 euro zodat je 2 maanden op onze kosten kunt luisteren naar onze beste podcasts. De cadeaubon is te gebruiken tot 31 december 2025.

Wij wensen je veel luisterplezier! Log in of creëer een account om je cadeaubon te claimen. Vul de cadeaucode in bij het afsluiten van het Podimo abonnement in het afreken scherm.

[Claim je cadeau](#)

Met vriendelijke groet,

Kim Janssen
Klantenservice Nederland




Voor het laatst bijgewerkt: zojuist

The screenshot shows the FreeMail interface. The top bar includes a '+ Nieuwe email' button, navigation arrows, a refresh icon, the 'FreeMail' logo, and settings/help icons. The left sidebar lists folders: Postvak IN 8, Verzonden, Concepten, Archiveren, Spam, Prullenmand, and Belangrijk. The main content area displays an email from 'Rabobank Account Beveiliging <beveiliging@rabobank.com>' with subject 'Belangrijke mededeling: Ongebruikelijke activiteit op uw rekening'. The email body features a red warning box with a white exclamation mark and the text 'Waarschuwing Je bent gehackt', followed by a message from the Rabobank security team and a 'Bevestig uw identiteit' button.

Belangrijke mededeling: Ongebruikelijke activiteit op uw rekening

Rabobank Account Beveiliging <beveiliging@rabobank.com> Beantwoorden Doorsturen Rapporteren ...

Aan: U



**Waarschuwing
Je bent gehackt**

Beste Sam,

Wij hebben onlangs een melding gekregen dat er een via meerdere IP adressen is geprobeerd om jouw account in te komen. Uit voorzorg hebben we je account tijdelijk geblokkeerd, aangezien de veiligheid van onze klanten voorop staat. Hierdoor verzoeken we u dringen om uw identiteit te bevestigen en uw wachtwoord te veranderen om te voorkomen dat dit nog vaker zal gebeuren. Uw identiteit verifiëren kan via de onderstaande link:

[Bevestig uw identiteit](#)

Bevestig uw identiteit binnen 24 uur om verdere beperkingen te voorkomen. Wij waarderen uw vertrouwen en medewerking en hopen uw rekening gauw weer actief te kunnen maken.

Met vriendelijke groet,
Rabobank Beveiligingsteam

Voor het laatst bijgewerkt: zojuist

Nieuwe email FreeMail

Postvak IN 10

Verzonden

Concepten

Archiveren

Spam

Prullenmand

Belangrijk

Profiteer vóór 23:59 uur van 20% korting!

XXL Nutrition <klantenservice@xxlnutrition.com> Beantwoorden Doorsturen Rapporteren ...

Aan: U

Hey Sam,

Hieperdepiep! XXL Nutrition blaast vandaag alweer 20 kaarsjes uit. Om het in perspectief te plaatsen: deze tijd staat gelijk aan het drinken van 7.300 eiwitshakes.

Ga naar onze website **voor 23:59 uur vanavond** en profiteer van maar liefst **20% korting** op alles van XXL nutrition, XONE en Fitmeals!

Bestel nu

Volg ons

Klantenservice
Betaling
Verzending
Algemene
voorwaarde

Neem contact met ons op
✉ klantenservice@xxlnutrition.com

Voor het laatst bijgewerkt: zojuist

Nieuwe email FreeMail

Postvak IN 4

Verzonden

Concepten

Archiveren

Spam


Prullenmand

Belangrijk

Uitnodiging voor opening Kilo Kilo vintage store in Nijmegen!

Kilo Kilo <uitnodiging@kilokilostore.nl> Beantwoorden Doorsturen Rapporteren ...

Aan: U



Beste Sam,

Vanwege jouw eerdere interesse in vintage shopping ben je uitgenodigd voor de opening van onze nieuwe Kilo Kilo winkel in Nijmegen op **15 juni 2025!** Wat kunt je verwachten?

- **Exclusieve preview:** Ontdek zeldzame vintage items voor ze openbaar worden.
- **Persoonlijke kortingscode:** Speciaal voor onze gasten, zodat jij jouw favoriete items kunt scoren.
- **Netwerkmogelijkheden:** Maak kennis met influencers en anderen die jouw passie delen.

Omdat we gelimiteerde plekken hebben is deze uitnodiging slechts **twee dagen** geldig! Zorg dat je jouw code snel activeert via [deze link](#).

Wij kijken ernaar uit je te verwelkomen op dit bijzondere event en samen de wereld van vintage te vieren. Mocht je vragen hebben, aarzel dan niet om contact met ons op te nemen :).

Met vriendelijke groet

Marianne de Groot
Hoofd Marketing Kilo Kilo

Voor het laatst bijgewerkt: zojuist

FreeMail

Nieuwe email

Postvak IN 7

Verzonden

Concepten

Archiveren

Spam

Prullenmand

Belangrijk

Dringend: Bevestig je salarisaanpassing vóór 17:00 vandaag

HR Bol.com <hr-bol.com@bol.com> Beantwoorden Doorsturen Rapporteren ...

Aan: U

Beste Sam,

In verband met een interne salarisaanpassing willen we je op de hoogte stellen van een wijziging in jouw compensatie per volgende maand. Onze HR-afdeling heeft een correctie in de administratie ontdekt waardoor je recht hebt op een verhoogde vergoeding.

Om dit te verwerken, vragen we je om vóór 17:00 vandaag je gegevens te verifiëren via het onderstaande beveiligde HR-portaal door te klikken op [deze link](#).

Aangezien dit een dringende administratieve kwestie is, waarderen we je snelle actie. Mocht je vragen hebben, neem dan gerust contact op met jouw HR-contactpersoon.

Met vriendelijke groet,

Daan Vermeer
 HR Manager Bol.com
 Tel: +31 6 12345678
 Beschikbaar op ma t/m do tussen 08:00 – 16:30
 Pependorpseweg 100, 3528 BJ Utrecht

Voor het laatst bijgewerkt: zojuist

FreeMail

Nieuwe email

Postvak IN 13

Verzonden

Concepten

Archiveren

Spam

Prullenmand

Belangrijk

Starter met studieschuld... Wat doet dat met mijn hypotheek?

Rabobank <hypotheekadviesrabobank@outlook.com> Beantwoorden Doorsturen Rapporteren ...

Aan: U



Inloopmoment hypotheek pechgeneratie

Beste de Jong,

Veel starters van de pechgeneratie hebben dezelfde vragen: "Kan ik nog wel een hypotheek krijgen?", "Hoe zit het met mijn studieschuld?" en "Kom ik ooit nog van die schuld af?" Wij erkennen de zorgen die jullie hebben en schieten jullie te hulp.

Vanaf mei 2025 organiseren wij gratis online en fysieke informatie bijeenkomsten voor starters van de pechgeneratie.

Waar: Concertgebouw de vereniging
 Wanneer: Elke tweede maandag van de maand
 Tijdschema:

- Aanvang: 19:30
- Start bijeenkomst: 20:00 – 21:00
- Afsluitende borrel: 21:00 – 22:00

Zit jij met dezelfde vragen in deze snel veranderende wereld? Meld je dan aan via [deze link](#)

Met vriendelijke groet,
 Team Rabobank

Voor het laatst bijgewerkt: zojuist

FreeMail

Nieuwe email

Postvak IN 14

Verzonden

Concepten

Archiveren

Spam

Prullenmand

Belangrijk

Bestelling: [A0004T8C6A] Je pakje van Greetz komt eraan

PostNL <notificatie@postnl.nl> Beantwoorden Doorsturen Rapporteren ...

Aan: U

We bezorgen binnenkort je pakje van Greetz

Je krijgt nog een berichtje met de bezorg datum en -tijd 

Op track & Trace zie je wanneer we je pakje bezorgen en of je de bezorging kunt wijzigen.

[Naar track & trace](#)

Bezorgadres
Sam de Jong
Zonnewijzerlaan 123
1234 AB Nijmegen

Afzender
Greetz Nederland

Trak & trace-code
[3SJRFE6485304](#)

Handige besteltip!

- Bepaal zélf waar we je pakketten bezorgen. Stel je standaard bezorg-voorkeur in één keer in voor al je pakketten.
- [Stel je bezorgvoorkeur in](#)

Tot snel,
PostNL

Voor het laatst bijgewerkt: zojuist

4.3 Legitimate e-mails:

The screenshot shows the FreeMail web interface. The top navigation bar includes a '+ Nieuwe email' button, navigation arrows, a refresh icon, the 'FreeMail' logo, and settings/question mark icons. On the left, a sidebar lists folders: Postvak IN (5), Verzonden, Concepten, Archiveren, Spam, Prullenmand, and Belangrijk. The main content area displays an email from 'DHL eCommerce <noreply@dhlparcel.nl >' with subject 'We staan vandaag voor de deur tussen 19.35 - 21.30 uur (JJD000090254000040942533)'. The email body features the DHL logo and text: 'We staan vandaag voor je deur', 'Beste Sam de Jong,', 'Onze bezorger staat vandaag op de stoep met je pakket JJD000090254000040942533 van AMAZON EU SARM. Komt het niet goed uit? Wijzig dan eenvoudig je [bezorgafspraak](#).', 'Verwacht bezorgmoment: Donderdag 21 november, Tussen 19.35 - 21.30 uur', 'Volg je pakket: Met de Mijn DHL app heb je elke zending zelf in de hand. Letterlijk. Je volgt ze allemaal in één handig overzicht. Zo weet je precies wanneer de gele bus voor de deur staat!', and a 'Download de app' link. A footer note states: 'Dit bericht wordt automatisch verzonden, je kunt er niet op reageren. Vragen? Ga naar onze [support-pagina](#). Onze mailadressen eindigen altijd op @dhlecommerce.nl, @dhlparcel.nl of @dhl.com en we vragen je nooit via mail om inlog- of betaalgegevens. Iets niet in de haak? [Check het hier!](#) Lees [hier](#) hoe wij met je persoonsgegevens omgaan.'

The screenshot shows the FreeMail web interface. The top navigation bar includes a '+ Nieuwe email' button, navigation arrows, a refresh icon, the 'FreeMail' logo, and settings/question mark icons. On the left, a sidebar lists folders: Postvak IN (2), Verzonden, Concepten, Archiveren, Spam, Prullenmand, and Belangrijk. The main content area displays an email from 'Tandartsenpraktijk DuoDent <info@duodent.nu>' with subject 'Bevestiging van uw afspraak'. The email body contains: 'Geachte S. de Jong,', 'Hierbij bevestigen wij dat u een afspraak heeft gepland in onze praktijk.', 'In geval van verhindering wordt u verzocht daarvan 24 uur tevoren bericht te geven daar de tijd anders in rekening gebracht wordt.', 'Datum: dinsdag 06 mei 2025 om 10:20 uur', 'Behandelaar: Dr. M. Jansen', 'Patiënt: Sam de Jong', 'Met vriendelijke groet, Tandartsenpraktijk DuoDent', and the DuoDent logo. A footer note states: 'DuoDent heeft met geen enkele zorgverzekeraar contracten afgesloten. Dit kan mogelijk gevolgen hebben voor uw vergoedingen bij een prothese-behandeltraject of implantologie in de edentate kaak'

Nieuwe email FreeMail


Postvak IN 12

Verzonden
Concepten
Archiveren
Spam
Prullenmand
Belangrijk

We horen graag je mening!

Vue Netherlands <VueNetherlands@inmomentfeedback.com> Beantwoorden Doorsturen Rapporteren ...

Aan: U



Vue wil van je horen

Beste Sam

Bedankt voor je bezoek aan Vue Nijmegen op 2025-03-25.

Vue is altijd bezig om de bioscoopbeleving te verbeteren, daarom vragen we 3 minuten van je tijd om jouw ervaring van je bioscoopbezoek met ons te delen.

Alvast heel erg bedankt voor jouw feedback!

Om de vragenlijst te starten, klik hier:

[START VRAGENLIJST](#)

Deze vragenlijst is uiteraard anoniem. Jouw antwoorden worden niet in verband gebracht met jouw naam of e-mail. Nogmaals dank!

Vriendelijke groet,
Vue Cinemas

Voor het laatst bijgewerkt: zojuist

Nieuwe email FreeMail

Postvak IN 6

Verzonden
Concepten
Archiveren
Spam
Prullenmand
Belangrijk

Tijd voor je belastingaangifte!

Rabobank <noreply@email.rabobank.nl> Beantwoorden Doorsturen Rapporteren ...

Aan: U

Klaar voor je belastingaangifte?

[Alles wat je moet weten](#)

Beste S. de Jong,

Vanaf maart kun je weer je belastingaangifte doen. Met de juiste informatie is je aangifte zo gefixt. Wij helpen je graag om goed voorbereid te zijn.

Wij maken het je makkelijker

- Ontdek welke gegevens je nodig hebt voor je aangifte
- Welke belastingvoordelen voor jou van toepassing zijn
- Meer tips om je aangifte soepel te laten verlopen

Van aftrekposten tot deadlines: check hier alles wat je moet weten voor je aangifte in 2025.

[Dit wil je weten](#)

Met vriendelijke groet,
Rabobank

Vind je deze e-mail nuttig?
[Wil je deze mails niet meer ontvangen? Meld je dan hier af of wijzig je e-mailinstellingen. Lees in ons privacy statement hoe wij omgaan met jouw gegevens.](#)

Voor het laatst bijgewerkt: zojuist

FreeMail

Nieuwe email

Postvak IN 3

Verzonden

Concepten

Archiveren

Spam

Prullenmand

Belangrijk

Je iCloud-opslag is vol

iCloud <noreply@email.apple.com> Beantwoorden Doorsturen Rapporteren

Aan: U


Beste Sam de Jong,

Je iCloud-opslag is vol. Omdat je over de limiet van je opslagabonnement bent gegaan, worden er geen back-ups in iCloud meer gemaakt van je foto's, documenten, contacten en apparaatgegevens. Ook worden je foto's en video's niet meer naar iCloud-foto's geüpload. iCloud Drive en apps voor iCloud worden niet op je apparaten bijgewerkt.

Om deze iCloud-diensten te blijven gebruiken, moet je [bijwerken naar iCloud+](#) of minder opslagruimte gaan gebruiken.

[Werk bij naar iCloud+ met 50 GB voor € 0,99 per maand](#)

Met vriendelijke groet,
Het iCloud-team



iCloud is een dienst van Apple.
Apple ID | Support | Algemene voorwaarden | Privacybeleid
Copyright © 2025 Apple Distribution International Ltd, Hollyhill Industrial Estate, Hollyhill, Cork, Ireland. Alle rechten voorbehouden.

Voor het laatst bijgewerkt: zojuist

FreeMail

Nieuwe email

Postvak IN 11

Verzonden

Concepten

Archiveren

Spam


Prullenmand

Belangrijk

Bericht van Belastingdienst (document ontvangen)

MijnOverheid <noreply@mijn.overheid.nl> Beantwoorden Doorsturen Rapporteren

Aan: U

MijnOverheid. 

Geachte S. de Jong,

Er staat een document in uw Berichtenbox van Belastingdienst.
Log in op MijnOverheid om het bericht te bekijken.
Mogelijk moet u naar aanleiding van dit bericht actie ondernemen.
Lees het daarom op tijd.

Met vriendelijke groet,
MijnOverheid

Dit is een automatisch gegenereerd bericht. Een reactie op dit bericht zal niet worden gelezen of beantwoord.
MijnOverheid stuurt geen meldingen met een link naar de website. Dit is om te voorkomen dat u met valse e-mails naar een namaak-website wordt geleid (zogenaamde phishing).
Neem daarom het webadres van MijnOverheid op in uw Favorieten en ga altijd van daaruit naar de website. Ontvangt u toch een e-mail met daarin een link, dan is deze dus nooit van MijnOverheid.

Voor het laatst bijgewerkt: zojuist

+
Nieuwe email
FreeMail
⚙️ ?

✉️ Postvak IN 9
Kies zelf hoe je betaalt met Klarna

Klarna <noreply@e.klarna.com>
Beantwoorden Doorsturen Rapporteren ⋮

Klarna

Flexibel betalen voor je online shopping

Van grotere artikelen tot dagelijkse essentials, Klarna is de beste manier om te betalen voor alles wat je nodig hebt, op welke manier je maar wilt. Shop vandaag nog en deel je aankoop in 3 renteloze betalingen of betaal tot 30 dagen na het plaatsen van je bestelling.

[Shop nu](#)

Zo betaal je

Shop online bij je favoriete merken en betaal met Klarna.

<p>Betaal in 3 delen</p> <p>Je aankoop wordt automatisch gesplitst in 3 renteloze betalingen. Zodra je je eerste betaling hebt gedaan, worden de 2 laatste betalingen elke 30 dagen afgeschreven.</p>	<p>Betaal later in 30 dagen</p> <p>Geniet van de flexibiliteit om tot 30 dagen later te betalen. Zodra de winkel je bestelling verzendt, ontvang je een e-mail van Klarna met details over je betaling.</p>
--	--

Download de Klarna app voor: [iOS](#) | [Android](#)

[Klarna.com](#)
[Privacy](#)

[Klantenservice](#)
[Afmelden](#)

Voor het laatst bijgewerkt: zojuist

Appendix 5: Confirmatory factor analysis

Iteration 1:

	Value	HI95	HI99
SRMR	0,1020	0,0775	0,0832
d _{ULS}	1,0915	0,6312	0,7272
d _G	0,5273	0,2449	0,2757

Construct	Dijkstra-Henseler's rho (ρ_A)	Jöreskog's rho (ρ_C)	Cronbach's alpha(α)
fear_of_identity_the_1	1,0000	0,9094	0,8493
PCK_	1,0000	0,8408	0,7809
Self Efficacy	1,0000	0,9668	0,9484

Construct	Average variance extracted (AVE)
fear_of_identity_the_1	0,7704
PCK_	0,4020
Self Efficacy	0,9065

HTMT

Construct	fear_of_identity_the_1	PCK_	Self Efficacy_
fear_of_identity_the_1			
PCK_	0,1858		
Self Efficacy	0,0262	0,3694	

HTMT 2

Construct	fear_of_identity_the_1	PCK_	Self Efficacy_
fear_of_identity_the_1			
PCK_	N/A		
Self Efficacy	N/A	0,3765	

Fornell-Larcker criterion

Construct	fear_of_identity_the_1	PCK_	Self Efficacy_
fear_of_identity_the_1	0,7704		
PCK_	0,0229	0,4020	
Self Efficacy	0,0006	0,1011	0,9065

Squared correlations; AVE in the diagonal.

Loadings

Indicator	fear of identity the 1	PCK	Self Efficacy
fear_of_identity_the_1	0,9024		
fear_of_identity_the_2	0,9131		
fear_of_identity_the_3	0,8143		
PCK_1		0,5942	
PCK_2		0,6027	
PCK_3		0,4724	
PCK_4		0,7229	
PCK_5		0,7645	
PCK_6		0,5730	
PCK_7		0,6316	
PCK_8		0,6647	
Self_Efficacy_1			0,9434
Self_Efficacy_2			0,9573
Self_Efficacy_3			0,9556

Indicator reliability

Indicator	fear of identity the 1	PCK	Self Efficacy
fear_of_identity_the_1	0,8144		
fear_of_identity_the_2	0,8337		
fear_of_identity_the_3	0,6630		
PCK_1		0,3531	
PCK_2		0,3633	
PCK_3		0,2232	
PCK_4		0,5226	
PCK_5		0,5845	
PCK_6		0,3283	
PCK_7		0,3989	
PCK_8		0,4419	
Self_Efficacy_1			0,8899
Self_Efficacy_2			0,9163
Self_Efficacy_3			0,9133

Cross loadings

Indicator	fear_of_identity_the_1	PCK_	Self Efficacy_
fear_of_identity_the_1	0,9024	0,1175	-0,0281
fear_of_identity_the_2	0,9131	0,1347	-0,0284
fear_of_identity_the_3	0,8143	0,1457	-0,0052
PCK_1	0,1364	0,5942	0,1234
PCK_2	0,1062	0,6027	0,1781
PCK_3	0,1963	0,4724	0,2058
PCK_4	0,1058	0,7229	0,2495
PCK_5	0,0387	0,7645	0,2889
PCK_6	0,1292	0,5730	0,2486
PCK_7	0,0482	0,6316	0,1496
PCK_8	-0,0003	0,6647	0,1541
Self_Efficacy_1	-0,0035	0,3339	0,9434
Self_Efficacy_2	0,0061	0,2963	0,9573
Self_Efficacy_3	-0,0697	0,2779	0,9556

Indicator multicollinearity

Indicator	fear_of_identity_the_1	PCK_	Self Efficacy_
fear_of_identity_the_1	3,0895		
fear_of_identity_the_2	3,2397		
fear_of_identity_the_3	1,5642		
PCK_1		1,4083	
PCK_2		1,4746	
PCK_3		1,1840	
PCK_4		3,3855	
PCK_5		3,7374	
PCK_6		1,3666	
PCK_7		3,1580	
PCK_8		3,1402	
Self_Efficacy_1			4,1985
Self_Efficacy_2			5,5255
Self_Efficacy_3			5,3750

Variance inflation factors (VIF)

Inter-construct correlations

Construct	fear_of_identity_the_1	PCK_	Self Efficacy_
fear_of_identity_the_1	1,0000		
PCK_	0,1513	1,0000	
Self Efficacy	-0,0235	0,3179	1,0000

Empirical correlation matrix

	fear_of_identity_the_1	fear_of_identity_the_2	fear_of_identity_the_3	PCK_1	PCK_2	PCK_3	PCK_4	PCK_5	PCK_6	PCK_7	PCK_8	Self_Efficacy_1	Self_Efficacy_2	Self_Efficacy_3
fear_of_identity_the_1	1,0000	0,8166	0,5567	0,1342	0,1081	0,1549	0,0895	-0,0044	0,1324	0,0135	-0,0376	-0,0116	-0,0047	-0,0640
fear_of_identity_the_2	0,8166	1,0000	0,5847	0,0867	0,1108	0,1834	0,1215	0,0579	0,1175	0,0439	-0,0447	-0,0007	-0,0063	-0,0742
fear_of_identity_the_3	0,5567	0,5847	1,0000	0,1378	0,0603	0,1779	0,0673	0,0482	0,0899	0,0692	0,0815	0,0030	0,0270	-0,0450
PCK_1	0,1342	0,0867	0,1378	1,0000	0,4957	0,1635	0,3484	0,3596	0,1944	0,1941	0,2308	0,1818	0,0982	0,0724
PCK_2	0,1081	0,1108	0,0603	0,4957	1,0000	0,2096	0,3985	0,3699	0,1411	0,1679	0,2467	0,1906	0,1818	0,1363
PCK_3	0,1549	0,1834	0,1779	0,1635	0,2096	1,0000	0,3092	0,3812	0,1344	0,0633	0,1133	0,1973	0,1994	0,1910
PCK_4	0,0895	0,1215	0,0673	0,3484	0,3985	0,3092	1,0000	0,8283	0,2360	0,2517	0,2611	0,2857	0,2359	0,1910
PCK_5	-0,0044	0,0579	0,0482	0,3596	0,3699	0,3812	0,8283	1,0000	0,3612	0,2603	0,2820	0,3055	0,2736	0,2462
PCK_6	0,1324	0,1175	0,0899	0,1944	0,1411	0,1344	0,2360	0,3612	1,0000	0,4212	0,3915	0,2396	0,2375	0,2330
PCK_7	0,0135	0,0439	0,0692	0,1941	0,1679	0,0633	0,2517	0,2603	0,4212	1,0000	0,8157	0,1492	0,1067	0,1713
PCK_8	-0,0376	-0,0447	0,0815	0,2308	0,2467	0,1133	0,2611	0,2820	0,3915	0,8157	1,0000	0,1286	0,1561	0,1554
Self_Efficacy_1	-0,0116	-0,0007	0,0030	0,1818	0,1906	0,1973	0,2857	0,3055	0,2396	0,1492	0,1286	1,0000	0,8495	0,8449
Self_Efficacy_2	-0,0047	-0,0063	0,0270	0,0982	0,1818	0,1994	0,2359	0,2736	0,2375	0,1067	0,1561	0,8495	1,0000	0,8847
Self_Efficacy_3	-0,0640	-0,0742	-0,0450	0,0724	0,1363	0,1910	0,1910	0,2462	0,2330	0,1713	0,1554	0,8449	0,8847	1,0000

Iteration 2:

	Value	HI95	HI99
SRMR	0,0974	0,1380	0,1618
d _{ULS}	0,7398	1,4864	2,0419
d _G	0,7392	1,2450	2,5060

Construct	Dijkstra-Henseler's rho (ρ_A)	Jöreskog's rho (ρ_c)	Cronbach's alpha(α)
fear_of_identity_the_1	0,8621	0,8531	0,8493
Self_Efficacy_1	0,9575	0,9486	0,9484
PCK_1	0,8081	0,7703	0,7770

Construct	Average variance extracted (AVE)
fear_of_identity_the_1	0,6611
Self_Efficacy_1	0,8611
PCK_1	0,3751

HTMT

Construct	fear_of_identity_the_1	Self_Efficacy_1	PCK_1
fear_of_identity_the_1			
Self_Efficacy_1	0,0262		
PCK_1	0,1298	0,3229	

HTMT 2

Construct	fear_of_identity_the_1	Self_Efficacy_1	PCK_1
fear_of_identity_the_1			
Self_Efficacy_1	N/A		
PCK_1	N/A	0,3196	

Fornell-Larcker criterion

Construct	fear_of_identity_the_1	Self_Efficacy_1	PCK_1
fear_of_identity_the_1	0,6611		
Self_Efficacy_1	0,0008	0,8611	
PCK_1	0,0183	0,1072	0,3751

Squared correlations; AVE in the diagonal.

Loadings

Indicator	fear_of identity the 1	Self Efficacy 1	PCK 1
fear_of_identity_the_1	0,7569		
fear_of_identity_the_2	0,9108		
fear_of_identity_the_3	0,7622		
PCK_1			0,5810
PCK_2			0,6387
PCK_4			0,8025
PCK_5			0,7396
PCK_7			0,4482
PCK_8			0,3363
Self_Efficacy_1		0,9996	
Self_Efficacy_2		0,8134	
Self_Efficacy_3		0,9604	

Indicator reliability

Indicator	fear_of identity the 1	Self Efficacy 1	PCK 1
fear_of_identity_the_1	0,5729		
fear_of_identity_the_2	0,8296		
fear_of_identity_the_3	0,5809		
PCK_1			0,3376
PCK_2			0,4079
PCK_4			0,6440
PCK_5			0,5470
PCK_7			0,2009
PCK_8			0,1131
Self_Efficacy_1		0,9991	
Self_Efficacy_2		0,6617	
Self_Efficacy_3		0,9224	

Cross Loadings

Indicator	fear_of identity the 1	Self Efficacy 1	PCK 1
fear_of_identity_the_1	0,7569	-0,0298	0,0929
fear_of_identity_the_2	0,9108	-0,0299	0,1183
fear_of_identity_the_3	0,7622	-0,0070	0,1185
PCK_1	0,1440	0,1282	0,5810
PCK_2	0,1154	0,1817	0,6387
PCK_4	0,1158	0,2559	0,8025
PCK_5	0,0434	0,2959	0,7396
PCK_7	0,0519	0,1550	0,4482
PCK_8	-0,0036	0,1567	0,3363
Self_Efficacy_1	-0,0036	0,9996	0,3522
Self_Efficacy_2	0,0057	0,8134	0,2956
Self_Efficacy_3	-0,0758	0,9604	0,2637

Indicator Multicollinearity

Indicator	fear of identity the 1	Self Efficacy_1	PCK_1
fear_of_identity_the_1	3,0895		
fear_of_identity_the_2	3,2397		
fear_of_identity_the_3	1,5642		
PCK_1			1,4045
PCK_2			1,4662
PCK_4			3,3033
PCK_5			3,2803
PCK_7			3,0296
PCK_8			3,1219
Self_Efficacy_1		4,1985	
Self_Efficacy_2		5,5255	
Self_Efficacy_3		5,3750	

Variance inflation factors (VIF)

Inter-construct correlations

Construct	fear of identity the 1	Self Efficacy_1	PCK_1
fear_of_identity_the_1	1,0000		
Self_Efficacy_1	-0,0278	1,0000	
PCK_1	0,1353	0,3274	1,0000

Empirical correlation matrix

	fear of identity the 1	fear of identity the 2	fear of identity the 3	PCK_1	PCK_2	PCK_4	PCK_5	PCK_7	PCK_8	Self Efficacy_1	Self Efficacy_2	Self Efficacy_3
fear_of_identity_the_1	1,0000	0,8166	0,5567	0,1342	0,1081	0,0895	-0,0044	0,0135	-0,0376	-0,0116	-0,0047	-0,0640
fear_of_identity_the_2	0,8166	1,0000	0,5847	0,0867	0,1108	0,1215	0,0579	0,0439	-0,0447	-0,0007	-0,0063	-0,0742
fear_of_identity_the_3	0,5567	0,5847	1,0000	0,1378	0,0603	0,0673	0,0482	0,0692	0,0815	0,0030	0,0270	-0,0450
PCK_1	0,1342	0,0867	0,1378	1,0000	0,4957	0,3484	0,3596	0,1941	0,2308	0,1818	0,0982	0,0724
PCK_2	0,1081	0,1108	0,0603	0,4957	1,0000	0,3985	0,3699	0,1679	0,2467	0,1906	0,1818	0,1363
PCK_4	0,0895	0,1215	0,0673	0,3484	0,3985	1,0000	0,8283	0,2517	0,2611	0,2857	0,2359	0,1910
PCK_5	-0,0044	0,0579	0,0482	0,3596	0,3699	0,8283	1,0000	0,2603	0,2820	0,3055	0,2736	0,2462
PCK_7	0,0135	0,0439	0,0692	0,1941	0,1679	0,2517	0,2603	1,0000	0,8157	0,1492	0,1067	0,1713
PCK_8	-0,0376	-0,0447	0,0815	0,2308	0,2467	0,2611	0,2820	0,8157	1,0000	0,1286	0,1561	0,1554
Self_Efficacy_1	-0,0116	-0,0007	0,0030	0,1818	0,1906	0,2857	0,3055	0,1492	0,1286	1,0000	0,8495	0,8449
Self_Efficacy_2	-0,0047	-0,0063	0,0270	0,0982	0,1818	0,2359	0,2736	0,1067	0,1561	0,8495	1,0000	0,8847
Self_Efficacy_3	-0,0640	-0,0742	-0,0450	0,0724	0,1363	0,1910	0,2462	0,1713	0,1554	0,8449	0,8847	1,0000

Iteration 3:

	Value	HI95	HI99
SRMR	0,0651	0,0977	0,1205
d _{ULS}	0,1188	0,2673	0,4063
d _G	0,1117	0,1434	0,2374

Construct	Dijkstra-Henseler's rho (ρ_A)	Jöreskog's rho (ρ_C)	Cronbach's alpha(α)
Self_Efficacy_1	0,9447	0,9408	0,9388
PCK_4	0,7870	0,7826	0,7734
fear of identity the 1	0,7689	0,7349	0,7152

Construct	Average variance extracted (AVE)
Self_Efficacy_1	0,8885
PCK_4	0,5466
fear of identity the 1	0,5873

HTMT

Construct	Self Efficacy_1	PCK_4	fear of identity the 1
Self_Efficacy_1			
PCK_4	0,3072		
fear of identity the 1	0,0309	0,1130	

HTMT2

Construct	Self Efficacy_1	PCK_4	fear of identity the 1
Self_Efficacy_1			
PCK_4	0,3101		
fear of identity the 1	N/A	N/A	

Fornell-Larcker criterion

Construct	Self Efficacy_1	PCK_4	fear of identity the 1
Self_Efficacy_1	0,8885		
PCK_4	0,0915	0,5466	
fear of identity the 1	0,0012	0,0115	0,5873

Squared correlations; AVE in the diagonal.

Loadings

Indicator	Self Efficacy_1	PCK_4	fear of identity the 1
fear_of_identity_the_1			0,8800
fear_of_identity_the_3			0,6326
PCK_2		0,6759	
PCK_4		0,7975	
PCK_5		0,7395	
Self_Efficacy_2	0,8979		
Self_Efficacy_3	0,9852		

Indicator Reliability

Indicator	Self Efficacy_1	PCK_4	fear of identity the 1
fear_of_identity_the_1			0,7744
fear_of_identity_the_3			0,4001
PCK_2		0,4569	
PCK_4		0,6359	
PCK_5		0,5468	
Self_Efficacy_2	0,8063		
Self_Efficacy_3	0,9706		

Cross Loadings

Indicator	Self Efficacy 1	PCK 4	fear of identity the 1
fear_of_identity_the_1	-0,0378	0,0861	0,8800
fear_of_identity_the_3	-0,0113	0,0793	0,6326
PCK_2	0,1674	0,6759	0,1135
PCK_4	0,2251	0,7975	0,1033
PCK_5	0,2748	0,7395	0,0226
Self_Efficacy_2	0,8979	0,3131	0,0111
Self_Efficacy_3	0,9852	0,2601	-0,0722

Indicator Multicollinearity

Indicator	Self Efficacy 1	PCK 4	fear of identity the 1
fear_of_identity_the_1			1,4490
fear_of_identity_the_3			1,4490
PCK_2		1,1960	
PCK_4		3,2887	
PCK_5		3,2048	
Self_Efficacy_2	4,6001		
Self_Efficacy_3	4,6001		

Variance inflation factors (VIF)

Inter-construct correlation

Construct	Self Efficacy 1	PCK 4	fear of identity the 1
Self_Efficacy_1	1,0000		
PCK_4	0,3024	1,0000	
fear of identity the 1	-0,0344	0,1073	1,0000

Empirical correlation matrix

	fear of identity the 1	fear of identity the 3	PCK 2	PCK 4	PCK 5	Self Efficacy 2	Self Efficacy 3
fear_of_identity_the_1	1,0000	0,5567	0,1081	0,0895	-0,0044	-0,0047	-0,0640
fear_of_identity_the_3	0,5567	1,0000	0,0603	0,0673	0,0482	0,0270	-0,0450
PCK_2	0,1081	0,0603	1,0000	0,3985	0,3699	0,1818	0,1363
PCK_4	0,0895	0,0673	0,3985	1,0000	0,8283	0,2359	0,1910
PCK_5	-0,0044	0,0482	0,3699	0,8283	1,0000	0,2736	0,2462
Self_Efficacy_2	-0,0047	0,0270	0,1818	0,2359	0,2736	1,0000	0,8847
Self_Efficacy_3	-0,0640	-0,0450	0,1363	0,1910	0,2462	0,8847	1,0000

Appendix 6: Survey questions

- Would you like to participate in this study?
- What is your age? (please enter a number in years)
- What is your highest level of education completed?
- What is your gender?
- To check if you've been paying attention: Which bank does Sam use?
- After reading this e-mail, what action would you take if you were Sam?
- To check if you're still there: Choose the answer option you were just able to click for each question under the e-mails.
- Please answer the following statements based on how you currently feel. – I am compassionate and have a soft heart
- Please answer the following statements based on how you currently feel. – I can be cold and indifferent
- Please answer the following statements based on how you currently feel. – I am respectful and treat others with respect
- Please answer the following statements based on how you currently feel. – I am sometimes rude to others
- Please answer the following statements based on how you currently feel. – I assume that others have good intentions toward me
- Please answer the following statements based on how you currently feel. – I tend to find faults in others
- Answer the following statements: – I complete chores right away
- Answer the following statements: – I usually put things back in their place
- Answer the following statements: – I like order
- Answer the following statements: – I never make a mess of things
- Answer the following statements: – I do things without thinking
- Answer the following statements: – I act on impulse
- Answer the following statements: – I act quickly and on the spur of the moment
- Answer the following statements: – I buy things impulsively
- Answer the following statements: – I spend more money than I earn
- Answer the following statements: – Once I've made up my mind, I'm not likely to change it
- Answer the following statements: – My viewpoints are generally very consistent
- Answer the following statements: – I often change my mind

- Answer the following statements: – I don't change my mind easily
- To check if you're still there: – For this question, select the answer 'Agree'
- Answer the following statements: – I'm afraid someone could steal my personal and financial information online
- Answer the following statements: – I worry that someone could use my personal and financial information online without my permission
- Answer the following statements: – I worry that my reputation could be harmed through misuse of my personal and financial information online
- The following questions are about Generative AI. Generative AI (GenAI) is a category within AI that can create original content. GenAI can mimic human creativity based on patterns in data. Examples of new content that GenAI can produce include text, images, audio or videos. – I can recognize the artificial intelligence technologies used in the applications and products I use.
- The following questions are about Generative AI. Generative AI (GenAI) is a category within AI that can create original content. GenAI can mimic human creativity based on patterns in data. Examples of new content that GenAI can produce include text, images, audio or videos. – I understand how GenAI technologies help improve the quality of translations made by online translation tools.
- The following questions are about Generative AI. Generative AI (GenAI) is a category within AI that can create original content. GenAI can mimic human creativity based on patterns in data. Examples of new content that GenAI can produce include text, images, audio or videos. – I understand how GenAI technologies help improve the quality of translations made by online translation tools.
- The following questions are about Generative AI. Generative AI (GenAI) is a category within AI that can create original content. GenAI can mimic human creativity based on patterns in data.
- The following questions are about Generative AI. Generative AI (GenAI) is a category within AI that can create original content. GenAI can mimic human creativity based on patterns in data. Examples of new content that GenAI can produce include text, images, audio or videos. – I know how GenAI products perform voice recognition tasks.
- The following questions are about Generative AI. Generative AI (GenAI) is a category within AI that can create original content. GenAI can mimic human creativity based on patterns in data. Examples of new content that GenAI can produce include text, images, audio or videos. – I can skillfully use GenAI applications or products to assist me with my daily

tasks.

- The following questions are about Generative AI. Generative AI (GenAI) is a category within AI that can create original content. GenAI can mimic human creativity based on patterns in data. Examples of new content that GenAI can produce include text, images, audio or videos. – I generally find it easy to learn how to use new GenAI.
- The following questions are about Generative AI. Generative AI (GenAI) is a category within AI that can create original content. GenAI can mimic human creativity based on patterns in data. Examples of new content that GenAI can produce include text, images, audio or videos. – I can use GenAI applications or products to work more efficiently.
- The following questions are about Generative AI. Generative AI (GenAI) is a category within AI that can create original content. GenAI can mimic human creativity based on patterns in data. Examples of new content that GenAI can produce include text, images, audio or videos. – I can evaluate the functionalities and limitations of GenAI products after using them for a while.
- The following questions are about Generative AI. Generative AI (GenAI) is a category within AI that can create original content. GenAI can mimic human creativity based on patterns in data. Examples of new content that GenAI can produce include text, images, audio or videos. – I can choose the appropriate solution from the options provided by GenAI applications and products.
- The following questions are about Generative AI. Generative AI (GenAI) is a category within AI that can create original content. GenAI can mimic human creativity based on patterns in data. Examples of new content that GenAI can produce include text, images, audio or videos. – I can select the most appropriate GenAI application or product for different specific tasks.
- The following questions are about Generative AI. Generative AI (GenAI) is a category within AI that can create original content. GenAI can mimic human creativity based on patterns in data. Examples of new content that GenAI can produce include text, images, audio or videos. – When I use GenAI applications or products, I always follow ethical principles.
- The following questions are about Generative AI. Generative AI (GenAI) is a category within AI that can create original content. GenAI can mimic human creativity based on patterns in data. Examples of new content that GenAI can produce include text, images, audio or videos. – When I use GenAI applications or products, I stay alert about privacy and information.
- The following questions are about Generative AI. Generative AI (GenAI) is a category

within AI that can create original content. GenAI can mimic human creativity based on patterns in data. Examples of new content that GenAI can produce include text, images, audio or videos. – I am always alert to misuse of GenAI technology.

- When I find an e-mail suspicious, I always pay close attention to: – the sender's name
- When I find an e-mail suspicious, I always pay close attention to: – the sender's e-mail address
- When I find an e-mail suspicious, I always pay close attention to: – the e-mail address that appears when I reply to the e-mail
- When I find an e-mail suspicious, I always pay close attention to: – grammatical and spelling errors in the subject line and sender name
- When I find an e-mail suspicious, I always pay close attention to: – grammatical and spelling errors in the body of the e-mail
- When I find an e-mail suspicious, I always pay close attention to: – warnings in the e-mail message
- When I find an e-mail suspicious, I always pay close attention to: – statements indicating urgency
- When I find an e-mail suspicious, I always pay close attention to: – statements involving time pressure or time-sensitive matters
- Answer the following statements: – My knowledge about phishing is good.
- Answer the following statements: – My ability to recognize phishing e-mails is good.
- Answer the following statements: – I am alert to phishing e-mails.
- Answer the following statements: – I can easily identify an e-mail as spear phishing
- Answer the following statements: – I am confident in my ability to detect fake spear phishing e-mails
- Answer the following statements: – I am confident that I can determine whether an e-mail is a spear phishing attack
- I hereby give consent for my responses to be used for the purposes mentioned above.

Appendix 7: Descriptive page + consent form/debriefing

Descriptive page

Welcome to this study and thank you for your participation!

This study aims to investigate how individuals organize their mailbox and what actions they take after reading an email.

What can you expect?

-First, you will be asked a number of questions regarding your personal information, such as age and gender.

-Then, you will be shown 14 screenshots of emails that you have to read, and then answer a multiple-choice question about this email. This multiple-choice question will be about the action you would take after reading the email.

-Finally, you will be asked a number of multiple-choice questions.

Important information about your participation:

-You are free to stop this survey at any time without any consequences.

-After completing this questionnaire, your permission to use the collected data for the research will be requested again and you will be able to refuse this.

-If you do not give permission for the use of your data, your completed data will be completely deleted.

-Participation in this research is completely voluntary and completely anonymous.

-This research maintains a minimum age of 18 years and the data is only used for academic purposes.

-The research takes approximately 15 to 20 minutes.

-For questions about this research, please contact ...

-Click the box below if you want to participate in this research (Qualtrics box).

Consent form

Thank you very much for participating in this research! This not only helps us as researchers, but also science one step forward.

The collected data is used to realize the real goal of this research, this is explained below. When you are done, do not forget to click on the arrow filled in the page again to send your answers.

This research is about vulnerability on a personal level to spear phishing emails. This was not shared with you at the beginning of the research in order to achieve realistic results. In short, we explain what this research exactly entails:

You have just managed a number of emails, among which are fraudulent emails. These spear phishing emails are personalized based on the personality that caused you to carefully read through the research. Half of the participants of this research have come into contact with spear phishing emails created by humans, while the other half of the participants have managed emails created by generative AI. The Generative AI emails were created by ChatGPT 4-0. This research design is used to test the difference between the creator of the email (generative AI humans) and the effect of this on the vulnerability of individuals to phishing. The questions you answered after the email management task should provide information about your personal characteristics in order to investigate whether this has an effect on individual vulnerability to spear phishing emails.

Spear phishing is a form of online fraud in which a personalized fake message is used to obtain someone's unfortunate information or to provoke other harmful actions. In this case, it concerns emails.

The data from this research will only be used for a graduation purpose. This data will therefore be included in the Radboud University thesis repository for a period of at least seven years in accordance with the legal requirements. The data is anonymous.

If you would rather not participate in this research after knowing the true nature of this research, you can indicate this in the following question.

I give permission for my completed answers to be used for the purposes mentioned above.

If you have any questions, please do not hesitate to send an email to the email address at the bottom of the page, we will be happy to help you.

Thank you again for participating in this research!

Please click the arrow at the bottom of the page again to submit your answers.

Appendix 7: Attention checks

After persona:

To check if you are still there: Which bank does Sam have?

A) ABN AMRO

B) Rabobank

C) ING Bank

D) SNS Bank

After Emails:

To check if you are still there: Choose the answer option that you were just able to click while viewing the emails

A) Click on link/attachment

B) Forward

C) Assign priority

D) Answer

Between regular questions:

To check if you are still there: Choose the answer 'Agree' for this question

A) Completely disagree

B) Disagree

C) Somewhat disagree

D) Neutral/no opinion

E) Somewhat agree

F) Agree

G) Completely agree

Appendix 8: Persona

To make this research as realistic as possible, it is important that you can put yourself in the position of the person who appears in the various e-mails. This introduces Sam de Jong, a fictional persona that will be used in this study. Try to remember the information below.

About Sam

General information

Name: Sam de Jong

Age: 25 years old (born on September 30, 1999)

Place of residence: Zonnewijzerlaan 123. 1234AB, Nijmegen

Education: HBO and WO in communication and digital marketing

Living situation: Lives with two friends in an apartment in Nijmegen

Banking: A bank account at Rabobank

Professional

Works at: Bol.com

Function: Junior online marketer

Colleagues: Daan, Thomas, Lars, Emma, Julia and Anna

Interests and online behavior

Hobbies: Sports, festivals, vintage shopping, podcasts

Social media use: Active and interested in digital tools and social media

Why Sam?

The research includes the task of being able to classify e-mails as well as possible. Because personality variables are important for this research, a number of e-mails will also be personalized based on e-mails that may have been sent to Sam de Jong. Sam represents a 25-year-old professional from Nijmegen. For the e-mail classification task, it is important to empathize with Sam's life as much as possible and to answer the e-mails in the way Sam would do this.

Click **START** to begin (this is only possible after 30 seconds).

Appendix 9: Descriptives/frequencies/means

Descriptives

Descriptives

	Descriptive Statistics								
	N Statistic	Minimum Statistic	Maximum Statistic	Mean Statistic	Std. Deviation Statistic	Skewness		Kurtosis	
						Statistic	Std. Error	Statistic	Std. Error
PCK_new	156	2,67	7,00	6,0962	,89122	-1,434	,194	2,523	,386
fearid	156	1,00	7,00	3,9124	1,46457	-,111	,194	-,994	,386
selfef	156	1,00	7,00	4,9316	1,16565	-,792	,194	,546	,386
emailtn	156	,00	1,00	,5321	,50058	-,130	,194	-2,009	,386
accur_c	156	,00	1,00	,7125	,21343	-,519	,194	-,028	,386
Valid N (listwise)	156								

Frequencies

Statistics				
		Wat is uw leeftijd? (vul een getal in in jaren)	Wat is uw hoogst behaalde opleidingsnive au?	Wat is uw geslacht?
N	Valid	156	156	155
	Missing	0	0	1
Mean			5,73	1,54
Std. Error of Mean			,066	,040
Median			6,00	2,00
Mode			6	2
Std. Deviation			,822	,500
Skewness			-,169	-,144
Std. Error of Skewness			,194	,195
Kurtosis			-,499	-2,005
Std. Error of Kurtosis			,386	,387
Minimum			4	1
Maximum			7	2
Sum			894	238

Wat is uw leeftijd? (vul een getal in in jaren)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	19	6	3,8	3,8	3,8
	20	4	2,6	2,6	6,4
	21	16	10,3	10,3	16,7
	22	13	8,3	8,3	25,0
	23	23	14,7	14,7	39,7
	24	12	7,7	7,7	47,4
	25	7	4,5	4,5	51,9
	26	7	4,5	4,5	56,4
	27	9	5,8	5,8	62,2
	28	5	3,2	3,2	65,4
	29	2	1,3	1,3	66,7
	30	1	,6	,6	67,3
	32	3	1,9	1,9	69,2
	34	3	1,9	1,9	71,2
	35	1	,6	,6	71,8
	36	1	,6	,6	72,4
	38	1	,6	,6	73,1
	39	2	1,3	1,3	74,4
	40	1	,6	,6	75,0
	41	2	1,3	1,3	76,3
	44	1	,6	,6	76,9
	45	2	1,3	1,3	78,2
	46	3	1,9	1,9	80,1
	48	2	1,3	1,3	81,4
	49	1	,6	,6	82,1
	50	3	1,9	1,9	84,0
	51	2	1,3	1,3	85,3
	52	6	3,8	3,8	89,1
	53	2	1,3	1,3	90,4
	54	2	1,3	1,3	91,7
	55	3	1,9	1,9	93,6
	56	1	,6	,6	94,2
	57	1	,6	,6	94,9
60	1	,6	,6	95,5	
61	3	1,9	1,9	97,4	
62	1	,6	,6	98,1	
67	1	,6	,6	98,7	
69	1	,6	,6	99,4	
70	1	,6	,6	100,0	
	Total	156	100,0	100,0	

Wat is uw hoogst behaalde opleidingsniveau?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Vmbo, havo-onderbouw, vwo-onderbouw, mbo1	10	6,4	6,4	6,4
	Havo, vwo, mbo2-4	49	31,4	31,4	37,8
	Hbo-, wo-bachelor	70	44,9	44,9	82,7
	Hbo-, wo-master, doctor	27	17,3	17,3	100,0
Total		156	100,0	100,0	

Wat is uw geslacht?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Man	72	46,2	46,5	46,5
	Vrouw	83	53,2	53,5	100,0
	Total	155	99,4	100,0	
Missing	System	1	,6		
Total		156	100,0		

Means of detection accuracy per e-mail type

Report			
accur_c			
emailtn	Mean	N	Std. Deviation
,00	,7456	73	,20377
1,00	,6833	83	,21865
Total	,7125	156	,21343