Computers in Human Behavior Reports 20 (2025) 100784

Contents lists available at ScienceDirect

Computers in Human Behavior Reports

journal homepage: www.sciencedirect.com/journal/computers-in-human-behavior-reports

Review

Phishing vulnerability and personality traits: Insights from a systematic review

Pablo López-Aguilar [a,*], Carlota Urruela [b], Edgar Batista [a], Juvenal Machin [a], Agusti Solanas [a]

[a] Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili, Barcelona, Spain
[b] The Norwegian Police University College, Oslo, Norway

ARTICLE INFO

Keywords:
Big Five personality traits
Phishing vulnerability
Systematic review
Phishing experiments
Cybercrime prevention

ABSTRACT

Phishing attacks have gained prominence and effectiveness over the years. Although many efforts are devoted to combat them, generic anti-phishing awareness and training campaigns have shown limited success. In this context, considering individuals' personality traits in relation to phishing behaviour could significantly enhance cybersecurity defence strategies. In this article, we concentrate on personality traits and their effects on vulnerability to phishing attacks. We implement a rigorous systematic review following the methodology proposed by vom Brocke et al. (2009) along with the PRISMA statement. We searched five major databases (*i.e.,* Web of Science, Scopus, IEEE Xplore, ACM Digital Library, and PubMed), with an all-years' time span from 1900 to January 2025. From the 1919 articles yielded in the initial search, 26 satisfied all criteria. Results reveal that extraversion, agreeableness, and neuroticism generally show a positive association with phishing vulnerability, whereas conscientiousness emerges as a protective factor. The review also highlights significant gaps in the current methodologies used to measure phishing vulnerability, noting a lack of standardised measurement tools to perform phishing experiments. Finally, this study underscores the need to develop secondary prevention strategies targeting at-risk groups to combat the increasingly sophisticated phishing threats. To enhance consistency in future research, the Appendix includes guidelines for measuring phishing vulnerability under experimental conditions.

1. Introduction

The proliferation of crime-as-a-service offerings in underground markets has led to an unprecedented rise in cyberattacks worldwide. These attacks have multifaceted impacts, including not only business disruptions but also financial losses and reputational damages (Furnell et al., 2020). While companies make substantial investments in sophisticated defencive tools like threat intelligence platforms and intrusion detection systems, attackers circumvent these defences by exploiting human behaviour. Thus, they often employ deceptive tactics to manipulate individuals into performing actions that serve their interests (Mitnick & Simon, 2003). Among these tactics, phishing stands as the most commonly employed method to deceive people.

Phishing refers to the use of social engineering techniques (Syafitri et al., 2022) in which attackers, masquerading as trustworthy entities, mislead users into disclosing sensitive and confidential information, such as login credentials, financial information, or personal data (Varshney et al., 2024). Traditionally, phishing was primarily conducted through email. However, with the proliferation of electronic devices and communication channels, attackers devised alternative methods to deploy these attacks, including text messages or instant messaging (known as smishing), phone calls (vishing), QR codes (quishing), and social media platforms (Alkhalil et al., 2021). Regardless of the media, phishing tactics are also evolving towards personalised communications, rather than generic ones, with the aim to enhance the success rate of these attacks. Within this context, while phishing generally targets a broad audience, methods such as whaling and spear-phishing adopt more focused and strategic approaches: whaling targets high-profile individuals within organisations (*e.g.,* executives) to obtain highly privileged information, whereas spear-phishing targets specific individuals or groups to exploit their vulnerabilities or interests. This practice poses a critical menace to both personal and organisational information security, as evidenced by the alarming rise in phishing frauds. In this regard, the Anti-Phishing Working Group (APWG) reported that in 2023, the highest number of phishing attacks

* Corresponding author.
E-mail addresses: pablo-marcos.lopez-aguilar@estudiants.urv.cat (P. López-Aguilar), carlota.urruela.cortes@phs.no (C. Urruela), edgar.batista@urv.cat (E. Batista), juvenal.machin@estudiants.urv.cat (J. Machin), agusti.solanas@urv.cat (A. Solanas).

https://doi.org/10.1016/j.chbr.2025.100784
Received 19 April 2025; Received in revised form 11 August 2025; Accepted 18 August 2025
Available online 26 August 2025

Table 1
Summary description of the PEN and Big Five Personality Traits.

Trait	Personality Model		Description
	PEN Model	Big Five Model	
Extraversion	✓	✓	Active, Lively, Sociable, Outgoing
Neuroticism	✓	✓	Anxious, Sensitive, Moody, Emotional
Psychoticism	✓		Risk-Taking, Unemphatic, Egocentric, Tough-minded
Agreeableness		✓	Kind, Altruistic, Pro-Social, Compassionate
Conscientiousness		✓	Self-Controlled, Thoughtful, Disciplined
Openness to Experience		✓	Curious, Imaginative, Creative

ever recorded occurred, totalling nearly five million incidents (APWG, 2024). Between June 2023 and Q3 2024, the number of reported phishing incidents has remained stable, with no significant variance during this period (APWG, 2025). Due to the favourable cost–benefit relationship associated with phishing attacks, they have become the primary method employed when launching cyberattacks, especially ransomware (ENISA, 2024). Likewise, the advent of methods and tools based in generative artificial intelligence will certainly increase the volume and efficacy of phishing attacks (Schmitt & Flechais, 2024).

Despite the availability of technological anti-phishing tools, the human factor plays a central role in these attacks (Chrysanthou et al., 2024; Desolda et al., 2021). Thus, given the fact that phishing attacks represent a global and widespread threat, governments and organisations have invested significant efforts to develop primary prevention strategies aimed at educating the general public. Since these strategies have proven to have limited impact (Williams & Levi, 2017), efforts should be devoted towards secondary prevention strategies aimed at identifying at-risk groups that are crucial in early intervention, and mitigating the negative impact of cybercrime (Brantingham & Faust, 1976; Caplan, 1980). While research has identified several risk factors related to secondary prevention, including gender, age, sociodemographic factors, intelligence, IT skills, and personality traits (Mohebzada et al., 2012; Sudzina & Pavlicek, 2020), there has been limited application of these findings in practical, real-world conditions. Therefore, understanding the individual factors influencing human behaviour that could contribute to phishing vulnerability is of great interest. From a differential psychology perspective, it has been observed that individuals do not always behave in the same manner under identical circumstances (Colom Marañón, 2018). One of the most relevant constructs to explain these diverse behaviours is personality.

According to Bergner (2020), an individual's personality is the enduring set of traits and styles that the individual exhibits. Moreover, personality traits predict important life outcomes, even after considering other relevant factors such as cognitive abilities and socioeconomic status (Roberts et al., 2007), as well as health outcomes (Jokela et al., 2013; Martin et al., 2007), academic achievement (Hakimi et al., 2011; Nechita et al., 2015), and job performance (He et al., 2019), among others. Thus, comprehending personality is essential for understanding human behaviour (Eysenck, 1991), typically characterised to be hierarchically structured, with specific behaviours at the lowest level and broad traits at the highest level (Goldberg, 1993). Over the past three decades, two factorial models have dominated personality research: the PEN Model (also known as the Giant Three Model; (Eysenck et al., 1992)) and the Five Factor Model (FFM, also known as the Big Five Model; (McCrae & Costa, 1999)). The PEN Model identifies three super-traits: Psychoticism, Extraversion, and Neuroticism. Conversely, the Five Factor Model categorises personality into five major factors: Extraversion, Neuroticism, Agreeableness, Conscientiousness, and Openness to Experience (see Table 1).

Since personality traits can influence how individuals behave under pressure or specific pretences, attackers often incorporate psychological cues to evoke certain behaviours. For example, individuals with high levels of extraversion may be less vigilant in terms of decision-making styles (Urieta et al., 2021), making them more likely to fall victim to phishing attempts. On the other hand, neuroticism makes people prone to risk avoidance and extremely sensitive to punishment (Aluja & Blanch, 2011) because they overvalue what they perceive as an impending threat, preventing them from exploring new things (Toledo & Carson, 2023). Likewise, conscientious individuals may be more cautious and vigilant (McCrae & Costa, 1999), making them less likely to be deceived. Thus, understanding individual personality traits and their relationship with phishing vulnerability is crucial for mitigating risks and devising effective, targeted educational initiatives.

Insights into these psychological profiles can pave the way for the development of personalised cybersecurity training programmes, which adapt their content, tone, and delivery method to align with individuals' behaviour. However, translating these insights into practice requires a nuanced understanding of personality as a complex psychological construct, characterised by interacting traits that influence behavioural responses. This complexity is compounded by the wide variation in phishing tactics and by contextual factors such as personal experience, technological familiarity, cultural background, risk perception, and socio-economic conditions. These factors collectively contribute to the difficulty of reaching definitive conclusions regarding the role of personality in phishing vulnerability and pose several methodological challenges to consistently measuring phishing vulnerability across diverse populations. While the scientific community has been studying the stable dimensions of individual differences (*i.e.,* personality) for decades (Sackett et al., 2017), there is a notable scarcity of literature reviews that explore this complex interplay in detail. Addressing this gap could help translate personality-based findings into actionable guidelines for cybersecurity education and risk communication, ultimately reducing phishing vulnerability at scale.

With the aim of providing a clear view of the evolution of this research area, Fig. 1 presents an overview of the key developments in phishing research and the subsequent inclusion of personality-based perspectives. It illustrates how the field has evolved from email attacks to more complex strategies, and underscores the increasing attention devoted to psychological and personality factors in recent years. Blue boxes refer to attack developments, while orange boxes refer to research on human factors.

1.1. Related work

Existing literature reviews addressing phishing victimisation generally focus on various human factors, often addressing personality superficially. In this regard, Kavvadias and Kotsilieris (2025) explores the influence of psychological aspects affecting users' vulnerability to phishing emails but does not place a strong emphasis on personality traits. Likewise, Alsharida et al. (2023) offer diverse perspectives on human cybersecurity behaviour by evaluating and synthesising various cybersecurity aspects, including independent variables, target variables, moderators, etc. In this context, Desolda et al. (2021) highlight the importance of psychological aspects, such as behavioural and attitudinal changes, in mitigating phishing attacks but do not address personality traits. Additionally, Das et al. (2019) note that phishing studies pay little attention to personality traits compared to other factors, such as the individuals' background knowledge or cognitive processes. Similarly, Tornblad et al. (2021) outline several predictors of phishing victimisation, including demographics, educational background, cybersecurity experience, and personality traits, yet but they do

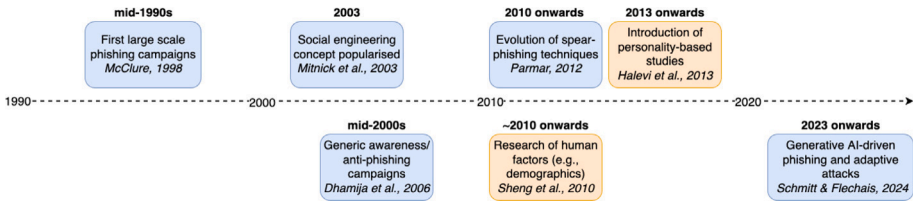

Fig. 1. Key conceptual developments in phishing research and integration of personality-based approaches.

Table 2
Research questions addressed in the literature review.

ID	Research Question	Discussion
RQ1	How extensively has existing literature investigated the relationship between personality and human phishing behaviour?	Section 3.1
RQ2	How are personality and phishing vulnerability operationalised in current studies?	Section 3.2
RQ3	What empirical relationships exist between phishing vulnerability and personality traits according to the literature?	Section 3.2
RQ4	Are current research designs appropriate to explore the relationship between vulnerability to phishing and personality traits?	Section 4
RQ5	Which new research directions can be proposed to focus on phishing prevention from a personality perspective?	Section 5

not conform to any established factorial models in the analysis of these traits. Finally, some literature reviews place more emphasis on personality traits, but they often focus exclusively on specific traits, such as neuroticism (López-Aguilar & Solanas, 2021) or extraversion (López-Aguilar et al., 2022). In contrast, this study focuses exclusively on personality traits as predictors of phishing vulnerability. It also addresses a critical gap by examining how both personality and phishing vulnerability are measured across studies, and by offering practical guidance to improve consistency in future research.

1.2. Contribution and plan of the article

Given the ongoing threat posed by phishing attacks to individuals and organisations, more rigorous and comprehensive research is needed to develop targeted preventative measures.

This literature review addresses a significant need by systematically analysing empirical studies that report associations between personality traits and phishing vulnerability. In particular, it offers a comprehensive analysis of the methods and tools employed in existing studies to operationalise both personality traits and phishing vulnerability, emphasising their strengths and limitations, thereby serving as a methodological reference for future researchers in the field. Furthermore, this study introduces a structured approach to evaluating phishing vulnerability in experimental conditions. We outline the essential phases of phishing experiments, including ethical considerations, common attack stages, and phishing assessment metrics, to enhance research comparability and reproducibility. Table 2 describes the main research questions addressed in this article. To the best of our knowledge, this is the first article providing a comprehensive and critical analysis of this research field. Through this review, we seek to encourage researchers and practitioners in the fields of computer security and behavioural sciences to fully grasp the current state of practice and jointly collaborate on developing strategies to reduce phishing scams effectively.

The remainder of the article is organised as follows: Section 2 describes the methodology followed to conduct the literature review and analysis. In Section 3, an analysis and synthesis of the selected studies are presented. Next, a comprehensive discussion of the results obtained is provided in Section 4. Future research endeavours are outlined in Section 5, and the theoretical and methodological implications encountered are discussed in Section 6. Finally, Section 7 closes the article with some concluding remarks. In Appendix A, this study provides complementary guidelines aimed at enhancing consistency in measuring phishing vulnerability under experimental conditions.

2. Methodology

This systematic review was conducted following the methodology proposed by vom Brocke et al. (2009) along with the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines (Moher et al., 2015). Thus, the focus of the review was to summarise the relevant outcomes of experimental studies intended to assess the role of personality traits in phishing victimisation. Intending to ensure reproducibility, we provide detailed explanations of all the steps and decisions involved in selecting and analysing the literature.

2.1. Definition of the review scope

The scope of this review is delineated in accordance with Cooper (1988) taxonomy of literature reviews and is differentiated by the following categories:

- **Focus**: Classified under the group of research outcomes, research methods, theories, and/or applications, this category emphasises the primary objective of the review. Specifically, this study aims to achieve a comprehensive understanding of human phishing behaviour, concentrating on practical studies that address personality traits and present empirical findings.
- **Goal**: Summarises the research objectives, including integration, criticism, and key issues. This study aims to examine the methods employed by the scientific community and to synthesise literature on the role of personality traits in the context of phishing. It also identifies current challenges in the field and proposes solutions to address these challenges.
- **Organisation**: As suggested by Cooper, a literature review can be structured historically, conceptually, or methodologically. This review is organised using a conceptual structure, grouping similar ideas and concepts together.
- **Perspective**: The authors' position on the research is conveyed through the review's perspective. Without having a predefined hypothesis to prove or disprove, this review aims to maintain a

critical position by analysing and synthesising the articles through the lens of critical evaluation, thereby adopting an impartial position.

- **Audience**: The audience shapes the writing style of the review. This particular review is tailored for researchers specialised in human factors and their role in cybersecurity behaviour.
- **Coverage**: Our research is categorised as exhaustive with selective citation. It aims to provide a comprehensive review of the empirical scientific literature concerning the role of personality traits in phishing attacks, ensuring a thorough analysis of relevant contributions.

2.2. Topic conceptualisation

In line with vom Brocke et al. (2009): *"to start by a broad conception of what is known about the topic and potential areas where knowledge may be needed"*, this review establishes working definitions for two central terms: personality and phishing. Additionally, according to Baker's suggestion (Baker, 2000), the review incorporates English-language sources that offer comprehensive summaries or overviews of key issues, including seminal textbooks, encyclopedias, and handbooks.

2.3. Database search

A comprehensive search strategy was developed to identify relevant publications available in the scientific literature. To ensure the coverage of high-quality publications, five well-known and widely recognised databases were selected as our search sources: Web of Science, Scopus, IEEE Xplore, ACM Digital Library, and PubMed. Due to the multidisciplinary nature of this review, the search string was built using the two central key terms: ALL (phishing AND personality). To obtain the widest coverage on the topic, no time span restrictions were applied and searches were configured to seek within all the articles (*i.e.,* title, abstract, keywords, full-text, and metadata). This search was conducted with an all-years' time span from 1900 to January 2025. To enhance transparency and reproducibility, the exact search strings used for each database are provided in Appendix B. These queries were adapted to the syntax of each database while maintaining equivalent search terms.

2.4. Eligibility criteria

Although different personality models have demonstrated relevance in psychological and behavioural research, including the 16 Personality Factor (16PF) model (Cattell & Mead, 2008), or typological approaches such as the Myers–Briggs Type Indicator (MBTI) (Myers et al., 1962), in this review we limited our search on studies employing personality theoretical frameworks based on, or adjacent to, the Five-Factor Model and the PEN model. These models were selected due to their theoretical robustness, empirical validation, and widespread use in the field of personality psychology. While the Five-Factor Model (FFM) and the Psychoticism-Extraversion-Neuroticism (PEN) model originate from different theoretical backgrounds (lexical versus biological), they capture overlapping core dimensions of personality and are broadly compatible. Empirical research has demonstrated moderate to strong correlations between the corresponding dimensions across both models (Scholte & De Bruyn, 2004; Zuckerman et al., 1993), supporting the idea that they assess similar underlying constructs. This theoretical and empirical alignment enables the models to be treated as functionally interchangeable when analysing behavioural outcomes (such as phishing vulnerability), particularly in the identification of broad personality-based predictors. Focusing on these models ensures a consistent theoretical foundation across studies, enabling better comparability of results and more reliable synthesis of findings.

On this basis, original research publications were deemed eligible if they met the following criteria: (1) the full text of the publication was available, (2) the publication was written in English, (3) the publication reported empirical findings on the relation between personality traits and phishing vulnerability, (4) experiments were focused on phishing, and (5) personality traits were measured using either the Five Factor, the PEN model or analogous models to aid in the interpretation of the results. In line with the scope of this review, only academic publications were considered. Grey literature and industry reports were intentionally excluded to ensure methodological rigour, reproducibility, and consistency in the quality of the analysis.

2.5. Literature selection

The selection process comprised three screening phases. Four reviewers independently evaluated each publication based on its title first, followed by its abstract, and finally by its full text, always according to the eligibility criteria. In each phase, every reviewer independently categorised the publications as either accepted or rejected. Discrepancies were addressed in round-table discussions with the aim of reaching consensus; when consensus could not be achieved, the decision was made by majority vote. Publications that did not obtain a majority of favourable votes were excluded. This procedure helps minimise researcher bias. This work was facilitated through the use of shared spreadsheet documents containing all relevant information about each publication and the assessment of each reviewer.

From the initial selection of publications, additional related publications were assessed for eligibility using the so-called backward search (*i.e.,* reviewing older literature referenced in the selected publications) and forward search (*i.e.,* examining articles that have cited the selected articles). Both searches were conducted in January 2025, using an all-years time span (from 1900 to January 2025) to ensure consistency with the initial search. Each search yielded a new set of publications, which were evaluated again following the same procedure as in the first selection. This iterative approach ensures an exhaustive literature search, thereby enhancing the robustness of this literature review.

2.6. Literature analysis

Accepted publications were carefully analysed and all relevant information was meticulously extracted, characterised, and classified. This rigorous examination guarantees a comprehensive understanding of each publication, facilitating the identification of new insights and knowledge and provide a fruitful discussion. To this end, a characterisation was conducted on how the different authors operationalised the constructs of relevance of this review: personality and vulnerability to phishing. This crucial step is essential for contextualising and comparing the findings reported in the selected publications. Regarding personality, there is no standard for using self-reports to evaluate personality traits, thus we report the specific tool and the personality model (if it differs from the Big Five Model) employed to evaluate this construct.

Phishing vulnerability assessment poses several complexities due to the subjective and context-dependent nature of "vulnerability". In this context, the lack of a definitive gold standard for assessing vulnerability leads to implementing diverse methodologies and tools in studies, and in many cases ad-hoc solutions. Since it is unfeasible to report all possible approaches to operationalise this construct, in Table 3, a taxonomy to organise and classify these procedures systematically is proposed. The taxonomy is organised by behavioural tasks (category B), detection tasks (category D), and self-report questionnaires (category S).

Behavioural tasks assess phishing vulnerability by directly observing participants' actions and responses in simulated phishing scenarios. Studies under this category sent one or more emails to participants and prompted them to make certain decisions. Within this group, a distinction should be established between studies that informed participants of the study's objective before the exercise and those that subsequently

Table 3
Taxonomy for phishing vulnerability operationalisation.

Category	Type of Measure	Description
B	Behavioural Task	Participants are exposed to examples of potential phishing emails and must perform one or several actions (*e.g.,* open the email, click on the link, delete email, submit sensitive information, etc.).
D	Detection Task	Participants are presented with examples of potential phishing emails and are asked to identify whether it is a phishing case or not. In some studies, they are additionally requested to specify the action they would take in response to these emails (*e.g.,* leave or delete the email in the inbox, share personal information, etc.).
S	Self-Report	Participants are not presented with any examples of phishing and are asked how they would proceed in the event of receiving an email that could potentially be a phishing attempt.

Table 4
Taxonomy for the methodological limitations (ML).

Category	Description
ML1	Assessment of personality (not reported, incomplete description, or methodologically weak).
ML2	Assessment of phishing vulnerability (not reported, incomplete description, or methodologically weak).
ML3	Methodology or statistical analysis (incomplete or missing sample description, inadequate sample size, statistical analysis, or results not properly reported).

provided this information. However, due to the lack of detailed reporting in some studies, it was not feasible to apply this criterion. In detection tasks, participants are typically presented with simulated phishing emails and are asked to classify them as either legitimate or fraudulent. Studies presenting self-assessment reports (category S) to operationalise vulnerability to phishing, entail a questionnaire wherein users self-assess their responses when confronted with various phishing emails.

Finally, a number of methodological limitations (ML) were identified during the analysis of the selected publications. These limitations can hinder the interpretation, replication, generalisation, or even the validity of the data and the results reported in those studies. For the sake of clarity, these ML are classified into three categories, as shown in Table 4.

2.7. Results synthesis

Ultimately, the main findings from each article were summarised. To enhance interpretability and facilitate comparison across articles, we report personality traits in the context of the Big Five model, namely Extraversion, Neuroticism, Conscientiousness, Agreeableness, and Openness to Experience. In cases in which the authors provided results for the opposite poles of these traits, results were accordingly reinterpreted. For instance, if authors reported findings for the trait "Emotional Stability", we reinterpreted them to align with the trait's pole of "Neuroticism".

It is important to mention that some studies conducted analyses measuring the indirect effects of personality traits on phishing vulnerability, mediated or moderated by other variables. We opted to report only direct effects, but we included notes indicating which analyses report indirect effects.

3. Results

This section elaborates on the results derived from the previously described methodology. First, we present the details of the selected publications resulting from the review methodology, and second, we provide a synthesis of the main findings identified in the selected literature.

3.1. Search results

The first search yielded a total of 1919 publications, but 34 were duplicated publications indexed by multiple databases. Given the large set of remaining publications (1885), a preliminary title screening was conducted to discard articles that were clearly out of the scope (*e.g.,* not related to information security), and 1316 publications were excluded at first. Subsequently, 415 publications were excluded based on the abstract screening. As a result, 154 publications were assessed for eligibility. After the full-text screening, 130 publications were excluded, and 24 publications were accepted in the first search.

From the 24 publications accepted in the first search, a backward search was conducted where 1109 publications were obtained. A total of 325 publications were excluded at first because they were duplicated or already screened during the first search, thereby remaining in 784 distinct publications to be screened. From those, 770 publications were excluded after the abstract screening, thus having 14 publications to be assessed for eligibility. After full-text reading, only two publications were accepted and included in the literature review.

Finally, a forward search was conducted, resulting in 390 publications. From those, 245 publications were excluded because they were duplicated or already screened during the first search. Thus, 145 were screened in this phase. A total of 130 publications were excluded after the abstract screening, and 15 publications were assessed for eligibility. In this case, none of them were included in the literature review.

All things considered, a total number of 26 publications were selected to be included in this literature review, as shown in Fig. 2. Additional details of the selected publications are provided in Table 5.

3.2. Literature analysis

The analysis of results represents a critical phase in exploring the research domain. This section presents a detailed examination of the relationship between personality traits and phishing vulnerability identified in the reviewed literature. Table 6 outlines how these two constructs were operationalised across the empirical studies. Additionally, a summary of each article's main findings and the methodological limitations identified are provided. While a meta-analysis would have offered a quantitative synthesis of findings, this was not feasible due to high heterogeneity in study designs, the operationalisation of personality traits and phishing, and inconsistencies in statistical reporting. In particular, many studies did not report standardised effect sizes, preventing a valid quantitative synthesis of the results.

The comprehensive analysis reported in Table 6 facilitated the identification of empirical relationships between phishing vulnerability and personality traits. Thus, extraversion emerged as the trait most strongly associated with increased vulnerability to phishing, based on the positive relation reported across a large number of the examined articles (Alseadoon et al., 2012, 2015; Anawar et al., 2019; Ayob &

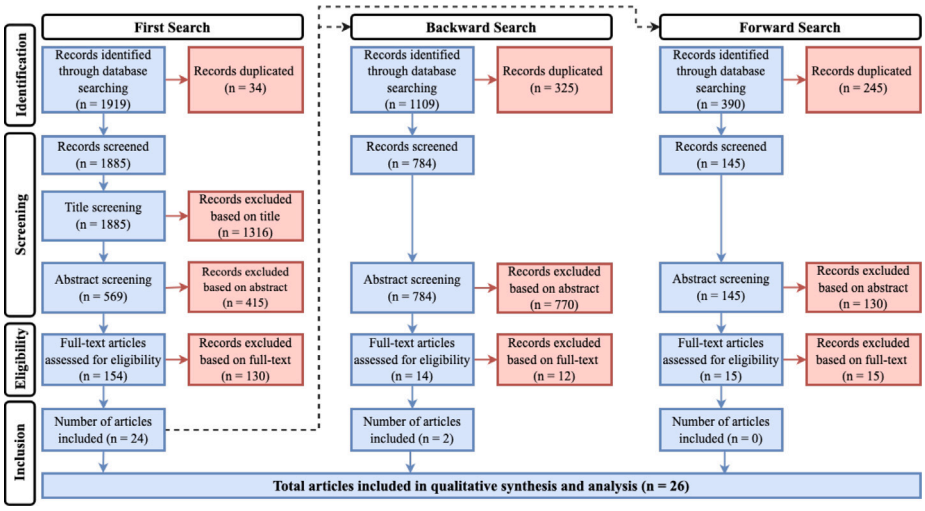

Fig. 2. Literature search evaluation methodology.

Weir, 2021; Canham et al., 2022; Eftimie et al., 2022; Frauenstein et al., 2023; Lawson et al., 2019; Sarno et al., 2023; Welk et al., 2015; Yang et al., 2022). Regarding extraverted individuals, Huseynov and Ozdenizci Kose (2022) reported a positive association with the facet of *excitement seeking* and a negative association with the facet of *assertiveness* when phishing was performed over short message services (SMS). In Schöni et al. (2024), extraversion exhibited a weak negative association with phishing vulnerability, but only in the post-training condition. Likewise, agreeableness has similarly revealed a tendency to be positively associated with phishing behaviour (Alseadoon et al., 2015; Anawar et al., 2019; Ayob & Weir, 2021; Canham et al., 2022; Eftimie et al., 2022; Frauenstein et al., 2023). Nevertheless, according to Sarno et al. (2023), individuals who rated high on agreeableness are less vulnerable to phishing attacks. In Huseynov and Ozdenizci Kose (2022), the facet of *morality* that belongs to the trait of agreeableness was also negatively associated with phishing vulnerability.

Some of the articles accepted in this review have also demonstrated an increased phishing vulnerability for neuroticism (Anawar et al., 2019; Eftimie et al., 2022; Islam et al., 2025; Welk et al., 2015). In this line, the positive association in Halevi et al. (2013) was only reported for women. Conversely, authors in Greitzer et al. (2021) reported a positive effect between phishing vulnerability and emotional stability, which implies a negative association with neuroticism. Although the *vulnerability* facet of neuroticism showed a positive association with phishing text messages, the facet of *self-consciousness* appeared to act as a protective factor (Huseynov & Ozdenizci Kose, 2022).

While one study found that conscientiousness is associated with increased phishing vulnerability (Halevi et al., 2015), highly conscientious individuals may be less prone to be victims of phishing attacks (Anawar et al., 2019; Ayob & Weir, 2021; Eftimie et al., 2022; Frauenstein et al., 2023; Huseynov & Ozdenizci Kose, 2022; Lawson et al., 2020). Therefore, it emerges as a personality trait that could be a protective factor in phishing vulnerability. Conversely, the role of openness in phishing vulnerability seems to be inconclusive. Although some studies found a positive association (Alseadoon et al., 2012, 2015; Frauenstein et al., 2023; Lawson et al., 2020), others found that increased openness may be associated with a decreased likelihood of phishing victimisation (Eftimie et al., 2022; Ge et al., 2021; Sarno et al., 2023; Sudzina & Pavlicek, 2017).

Other studies have not found statistically significant evidence on the role of personality traits in phishing vulnerability (Canham et al., 2024; Jones et al., 2019; Kleitman et al., 2018; Pattinson et al., 2012; Yoro et al., 2023).

From the ten studies listed in category B (behavioural tasks), six studies operationalise phishing in a dichotomous manner (Alseadoon et al., 2012, 2015; Ayob & Weir, 2021; Greitzer et al., 2021; Halevi et al., 2013; Yoro et al., 2023). The other four studies in this group, besides analysing whether participants clicked on the link, also examined other actions such as (1) opening the email, (2) sending sensitive information, (3) denying or discarding the email, or (4) blacklisting the sender (Canham et al., 2024; Eftimie et al., 2022; Halevi et al., 2015; Rahman et al., 2022).

In this review, we found thirteen articles pertaining to category D (detection tasks). Of those articles, four studies were limited to leading participants to classify emails in a dichotomous manner (Canham et al., 2022; Jones et al., 2019; Lawson et al., 2019, 2020). However, other articles sought to explore broader aspects of participants' behaviour with questions such as "How would you handle this email?" (Pattinson et al., 2012).

In contrast to the previously mentioned studies, the three studies belonging to category S (self-report questionnaires) do not incorporate visual elements or create simulated scenarios (Anawar et al., 2019; Islam et al., 2025; Sudzina & Pavlicek, 2017). Instead, they rely on asking the participants about their behaviour when faced with a phishing email (*e.g.,* "Would you click on a suspicious link?").

It is worth noting that a relevant number of studies use convenience sampling of either students or employees. In particular, nearly half of the studies (49%) use student samples, 22% are conducted with workers, 13% employ both profiles, and only one study (Sarno et al., 2023) reports a sample with representation from individuals aged from 18 to 71. The subsequent Section 4 provides an interpretation of the results.

4. Discussion

This section provides a critical evaluation of the methodologies and instruments employed in the reviewed studies to measure the constructs of personality and phishing vulnerability. By examining common patterns in research designs, we aim to identify methodological gaps and advance robust strategies in the context of personality and phishing research.

4.1. Personality assessment

With one exception, all the reviewed articles employed the Five Factor Model (FFM) framework for personality assessment. Only one article, Kleitman et al. (2018), used the Saucier's (2009) Big Six Model. This widespread use of the FFM theoretical framework facilitates comparison between studies. As depicted in Fig. 3, researchers employed

Table 5
List of the selected publications (n=26) in this literature review (listed in alphabetical order).

Reference	Title	Source	Year	Search
Alseadoon et al. (2012)	Who is more susceptible to phishing emails?: A Saudi Arabian study	Proc. 23rd Australasian Conf. on Information Systems	2012	First
Alseadoon et al. (2015)	What Is the Influence of Users' Characteristics on Their Ability to Detect Phishing Emails?	Proc. 1st Intl. Conf. on Communication and Computer Engineering	2015	First
Anawar et al. (2019)	Analysis of Phishing Susceptibility in a Workplace: A Big-Five Personality Perspectives	Journal of Engineering Science and Technology	2019	First
Ayob and Weir (2021)	Is Human Behaviour the Real Challenge in Combating Phishing	Cyber Physical, Computer and Automation System: A Study of New Technologies	2021	First
Canham et al. (2024)	Not All Victims Are Created Equal: Investigating Differential Phishing Susceptibility	International Conference on Human–Computer Interaction	2024	First
Canham et al. (2022)	Phish Derby: Shoring the Human Shield Through Gamified Phishing Attacks	Frontiers in Education	2022	First
Eftimie et al. (2022)	Spear-Phishing Susceptibility Stemming From Personality Traits	IEEE Access	2022	First
Frauenstein et al. (2023)	Unravelling the behavioural influence of social media on phishing susceptibility: A Personality-Habit-Information Processing model	Information & Management	2023	First
Ge et al. (2021)	How personal characteristics impact phishing susceptibility: The mediating role of mail processing	Applied Ergonomics	2021	First
Greitzer et al. (2021)	Experimental Investigation of Technical and Human Factors Related to Phishing Susceptibility	ACM Transactions on Social Computing	2021	First
Halevi et al. (2013)	Phishing, Personality Traits and Facebook	ArXiv Computer Science	2013	Backward
Halevi et al. (2015)	Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks	SSRN Electronic Journal	2015	Backward
Huseynov and Ozdenizci Kose (2022)	Using machine learning algorithms to predict individuals' tendency to be victim of social engineering attacks	Information Development	2022	First
Islam et al. (2025)	Identifying personality traits associated with phishing susceptibility	Security Journal	2025	First
Jones et al. (2019)	Email fraud: The search for psychological predictors of susceptibility	PLoS ONE	2019	First
Kleitman et al. (2018)	It is the deceiver and the receiver: Individual differences in phishing susceptibility and false positives with item profiling	PLoS ONE	2018	First
Lawson et al. (2019)	Baiting the Hook: Exploring the Interaction of Personality and Persuasion Tactics in Email Phishing Attacks	Proc. 20th Cong. of the Intl. Ergonomics Association	2019	First
Lawson et al. (2020)	Email phishing and signal detection: How persuasion principles and personality influence response patterns and accuracy	Applied Ergonomics	2020	First
Pattinson et al. (2012)	Why do some people manage phishing e-mails better than others?	Information Management & Computer Security	2012	First
Rahman et al. (2022)	Discovering the Correlation Between Phishing Susceptibility Causing Data Biases and Big Five Personality Traits Using C-GAN	IEEE Transactions on Computational Social Systems	2022	First
Sarno et al. (2023)	Which phish is captured in the net? Understanding phishing susceptibility and individual differences	Applied Cognitive Psychology	2023	First
Schöni et al. (2024)	You Know What? Evaluation of a Personalised Phishing Training Based on Users' Phishing Knowledge and Detection Skills	European Symposium on Usable Security	2024	First
Sudzina and Pavlicek (2017)	Propensity to Click on Suspicious Links: Impact of Gender, of Age, and of Personality Traits	Proc. 30th Bled eConference: Digital Transformation	2017	First
Welk et al. (2015)	Will the "Phisher-Men"' Reel You In? Assessing Individual Differences in a Phishing Detection Task	International Journal of Cyber Behaviour, Psychology and Learning	2015	First
Yang et al. (2022)	Predicting User Susceptibility to Phishing Based on Multidimensional Features	Computer Intelligence and Neuroscience	2022	First
Yoro et al. (2023)	Evidence of personality traits on phishing attack menace among selected university undergraduates in Nigerian	International Journal of Electrical and Computer Engineering	2023	First

various tools within this framework, including the IPIP-NEO, NEO-PI-R/NEO-FFI, "A Very Brief Measure of the Big-Five Personality Domains" questionnaire, and the BFI.

However, a recurring issue regarding the evaluation of personality traits in these studies is the use of very brief questionnaires. The questionnaire created by Gosling et al. (2003) "A very brief measure of

Table 6
Personality, phishing operationalisation, MLs and results of the articles found in this literature review (listed in alphabetical order).

Reference	Operationalisation		ML	Results
	Personality	Phishing		
Alseadoon et al. (2012)	A Very Brief Measure of the Big-Five Personality Domains - (Gosling et al., 2003).	B	ML3	Openness and Extraversion* increased the likelihood of phishing vulnerability. *Note: p = 0.068
Alseadoon et al. (2015)	A Very Brief Measure of the Big-Five Personality Domains - (Gosling et al., 2003).	B	–	Agreeableness, Openness and Extraversion increased the likelihood of phishing vulnerability.
Anawar et al. (2019)	Ad-hoc items adapted from the NEO-PI-R - (Costa & McCrae, 1992).	S	ML1, ML2, ML3	Conciensciousness was negatively associated with phishing vulnerability. Extraversion, Neuroticism, and Agreeableness were positively associated with phishing vulnerability.
Ayob and Weir (2021)	FFM. No information about the questionnaire or its content.	B	ML1, ML2, ML3	Agreeableness and Extroversion increased the likelihood of phishing vulnerability. Conscientiousness decreased the likelihood of phishing vulnerability.
Canham et al. (2024)	IPIP–NEO–60 - (Maples-Keller et al., 2019).	B	ML3	There were no statistically significant associations between personality traits and phishing vulnerability.
Canham et al. (2022)	IPIP–NEO–60 - (Maples-Keller et al., 2019).	D	–	Extraversion and Agreeableness were positively associated with phishing vulnerability.
Eftimie et al. (2022)	FFM questionnaire provided by a specialised independent company. No further information about the questionnaire or its content.	B	ML1	Neuroticism and Agreeableness were positively associated with opening the email. Openess and Conscientiousness were negatively associated with opening the email. Openess and Conscientiousness were negatively associated with clicking a malicious link. Extraversion, Neuroticism and Agreeableness were positively associated with clicking a malicious link. Openess and Conscientiousness were negatively associated with sensitive data submission. Extraversion, Neuroticism and Agreeableness were positively associated with sensitive data submission.
Frauen-stein et al. (2023)	BFI - (John & Srivastava, 1999).	D	–	Extraversion, Agreeableness, and Openness were positively associated with phishing vulnerability. Conscientiousness was negatively associated with phishing vulnerability.
Ge et al. (2021)	BFI-44 Chinese version - (Carciofo et al., 2016).	D	–	Openness was negatively associated with phishing vulnerability. Other personality traits (i.e. low Conscientiousness, low Openness, and high Neuroticism) show indirect effects on phishing vulnerability mediated by other variables, please refer to the paper for further details.
Greitzer et al. (2021)	Mini-IPIP - (Donnellan et al., 2006). *Note: Assessment only for Neuroticism (Emotional Stability), Agreeableness, and Conscientiousness. *Note: The authors measure another construct they call neuroticism/anxiety as a trait separate from emotional stability. We refer to neuroticism as the opposite pole of the emotional stability trait.	B	ML1, ML2	Neuroticism decreased the likelihood of phishing vulnerability.
Halevi et al. (2013)	NEO-PI-R - (Costa & McCrae, 1992).	B	ML3	Neuroticism was positively associated with phishing vulnerability in women. There were no statistically significant associations between personality traits and phishing vulnerability for men.
Halevi et al. (2015)	Mini-IPIP - (Donnellan et al., 2006).	B	ML3	Conscientiousness was positively associated with phishing vulnerability.

(*continued on next page*)

the Big-Five personality domain questionnaire" was a frequent choice in these studies. However, using such brief tools to measure personality has a series of psychometric consequences.

According to Gosling et al. (2003), these short measures do not allow the facets of personality traits to be measured, which implies a considerable loss of nuances and information, and they show lower reliability indices than longer multi-item measures. Brief measures have their place in research in which there are considerable time limitations or problems with access to the sample. However, considering the samples and designs of the reviewed studies, which primarily employ normative convenience samples (*e.g.,* university students, employees in a corporate environment, etc.) and rely on online questionnaires, the use of such tools does not appear to be justified.

A significant methodological limitation observed in several publications included in this review is not reporting or correctly citing the tools used to measure personality. This represents a methodological

Table 6 (*continued*).

Reference	Operationalisation		ML	Results
	Personality	Phishing		
Huseynov and Ozdenizci Kose (2022)	IPIP-NEO-120 - (Johnson, 2014). *Note: The authors analyse facets of the FFM personality traits. The trait to which each facet corresponds is provided in parentheses in the results column.	D	–	Excitement Seeking (Extraversion) increased the likelihood of phishing vulnerability in general and social media phishing vulnerability. Cautiousness (Conscientiousness) decreased the likelihood of phishing vulnerability in general and search engine phishing vulnerability. Assertiveness (Extraversion) decreased the likelihood of SMS phishing vulnerability. Morality (Agreeableness) decreased the likelihood of SMS phishing vulnerability. Vulnerability and Self-Consciousness (Neuroticism) increased and decreased the likelihood of SMS phishing vulnerability, respectively.
Islam et al. (2025)	FFM - The specific questionnaire is not reported.	S	ML1, ML2, ML3	High susceptibility was associated with higher neuroticism and lower conscientiousness and agreeableness scores. *Note: The authors do not provide specific results for these differences based on individual traits.
Jones et al. (2019)	IPIP-BIG5 - (Goldberg, 1999).	D	–	There were no statistically significant associations between personality traits and phishing vulnerability.
Kleitman et al. (2018)	25-item inventory based on the Big Six Model - (Saucier, 2009). No reference was provided for this specific 25 item inventory.	D	ML1	There were no statistically significant associations between personality traits and phishing vulnerability.
Lawson et al. (2019)	NEO-FFI-3 - (Costa & McCrae, 1992).	D	–	Extraversion was positively associated with phishing vulnerability.
Lawson et al. (2020)	NEO-FFI-3 - (Costa & McCrae, 1992).	D	–	Extraversion increased the likelihood of phishing vulnerability. Conscientiousness decreased the likelihood of phishing vulnerability. Openness increased the likelihood of correctly identifying legitimate emails. *Note: not for all phishing emails presented to the participants, please refer to the paper for further details.
Pattinson et al. (2012)	BFI - (John & Srivastava, 1999).	D	ML3	There were no statistically significant associations between personality traits and phishing vulnerability.
Rahman et al. (2022)	IPIP-NEO-120 - (Johnson, 2014)	B	ML2, ML3	Order of highest to lowest phishing vulnerability scores among participants*: - Extraversion - Agreeableness - Openness - Neuroticism - Conscientiousness. *Note: The authors did not perform analyses that allow for a generalisation of the results.
Sarno et al. (2023)	BFI - (John & Srivastava, 1999).	D	–	Extraversion was positively associated with phishing vulnerability. Agreeableness and openness to experience were negatively associated with phishing vulnerability.
Schöni et al. (2024)	BFI-10 - (Rammstedt & John, 2007)	D	–	Extraversion showed a weak negative association with phishing susceptibility only in the post-training condition.

(*continued on next page*)

malpractice as it hinders the interpretation of the results and the replication of the studies in question.

4.2. Phishing vulnerability assessment

Under real-world conditions, individual vulnerability to phishing attacks is influenced by a myriad of variables, including psychological traits, demographic factors, cultural background, and experience. From a technical perspective, the continuous advent of new tactics and technologies enables attackers to deploy increasingly sophisticated and complex strategies where the isolation of variables affecting vulnerability is increasingly more complex. Therefore, operationalising phishing vulnerability for research purposes within controlled settings is inherently complex. In this context, the absence of standardised assessment methods among studies leads to inconsistencies, and complicates the isolation and identification of specific variables contributing to vulnerability.

As outlined in Section 3.2, the 26 articles reviewed in this study implemented different approaches to operationalise phishing vulnerability which were subsequently classified into three different categories, *i.e.,* category B (Behavioural Tasks), category D (Detection Tasks), and category S (Self-Report Questionnaire). Thus, ten studies assessed this construct using behavioural tasks, thirteen employed classification

Table 6 (*continued*).

Reference	Operationalisation		ML	Results
	Personality	Phishing		
Sudzina and Pavlicek (2017)	BFI-10 - (Rammstedt & John, 2007).	S	ML2, ML3	Openness to Experience decreased the likelihood of phishing vulnerability.
Welk et al. (2015)	A Very Brief Measure of the Big-Five Personality Domains - (Gosling et al., 2003). *Note: The authors consider each item in the questionnaire as if it were an independent personality trait. To report results coherently, given that the questionnaire contains two items per personality trait (one direct and one inverse), the direct item represents high scores on the trait and the inverse item represents low scores.	D	ML1	Neuroticism and Extraversion were positively associated with phishing vulnerability.
Yang et al. (2022)	FFM questionnaire No information was provided about the questionnaire or its content.	D	ML1	Extraversion was positively associated with phishing vulnerability. *Note: The authors do not report the value of this association.
Yoro et al. (2023)	IPIP-NEO-120 - (Johnson, 2014) *Note: The analysis focuses on facets and not domains.	B	ML1	No statistically significant associations were found between personality traits and phishing vulnerability.

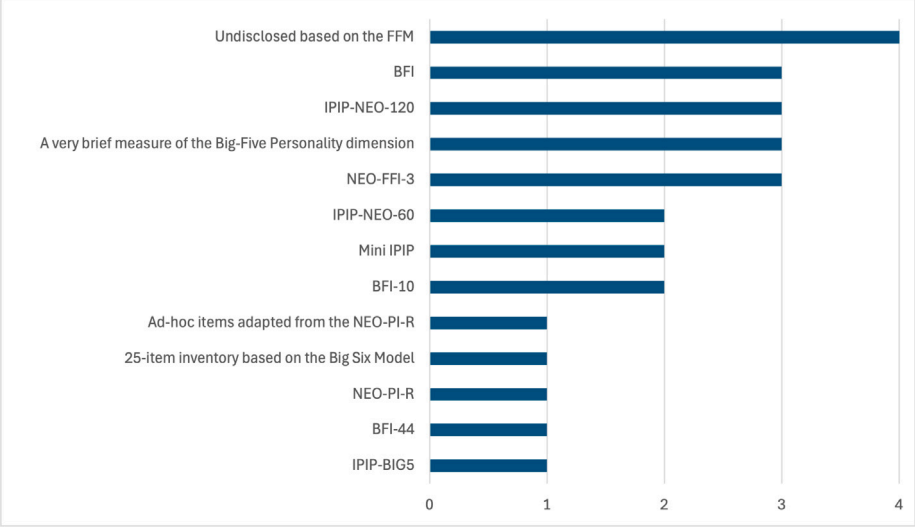

Fig. 3. Personality assessment tools used by the reviewed articles.

tasks, and three implemented self-report questionnaires. A description of each category is outlined below.

- **Behavioural tasks**: In the case of behavioural studies, the authors of this study aimed at distinguishing the articles that provided information to participants about the study's objectives before the exercise. However, only five studies explicitly indicated that participants were not informed of the study's objective before undertaking the exercise (Alseadoon et al., 2012, 2015; Canham et al., 2024; Halevi et al., 2015; Schöni et al., 2024). Emphasising this factor merits consideration, as informing participants about the study's purpose before the phishing experiment might potentially introduce bias into their behaviour and diminish the validity of the results.
  Behavioural tasks conducted without previously informing participants about the phishing exercise are probably the most effective method to simulate real-world conditions. Although this procedure may raise ethical concerns regarding deception, participants' information policies, and informed consents (Finn & Jakobsson, 2007), it certainly provides greater ecological validity of findings. Likewise, while analysing users' behaviour towards clicking/not clicking a link is a crucial step to improve the understanding of phishing behaviour, restricting the analysis solely to this variable would not reflect a real-world scenario.
- **Detection tasks**: While phishing operationalisation through behavioural tasks focuses on observing participants' behaviour and responses to specific phishing stimuli, detection tasks focus on participants' detection capabilities. This invites the question of whether these detection tasks really measure vulnerability to phishing or, rather, phishing detection capacity, which would pose a problem of criterion validity (Strauss & Smith, 2009). Moreover, although detecting deceptive cues like incorrect hyperlinks or email sources can offer insights into participants' behaviour, generating credible pretexts remains the primary aspect of successful phishing attacks. Therefore, implementing detection tasks in phishing exercises might not accurately predict phishing vulnerability under real-world conditions.
- **Self-report questionnaires**: Self-report measures can be valuable tools in assessing certain aspects of human behaviour, including attitudes, beliefs, and perceptions. However, relying on self-reporting to measure vulnerability to phishing attacks may not provide accurate data on an individual's vulnerability to phishing, since these measures rely heavily on participants' self-perception.

Table 7
Summary of findings, implications, and suggested research directions for each Big Five personality trait.

Personality Trait	Findings from Literature		Implications	Future Research Directions
	Positive Effect	Negative Effect		
Extraversion	Trait-level: 12 studies Facet-level: 1 study (Excitement Seeking)	Trait-level: 1 study Facet-level: 1 study (Assertiveness)	Extraversion should be considered when developing awareness and training interventions, as individuals high in excitement-seeking may be more susceptible.	Examine specific facets (*e.g.,* excitement-seeking vs. assertiveness). Study behavioural changes after training and develop interventions tailored to extraverted profiles.
Agreeableness	Trait-level: 6 studies	Trait-level: 2 studies Facet-level: 1 study (Morality)	Awareness strategies should address trust tendencies and promote moral reasoning as a protective factor.	Investigate facet-level differences (*e.g.,* morality vs. trust) and examine how factors such as a familiar or authoritative sender influence phishing responses.
Neuroticism	Trait-level: 5 studies Facet-level: 1 study (Vulnerability)	Trait-level: 1 studies Facet-level: 1 study (Self-Consciousness)	Targeted training to manage stress and anxiety could help reduce risk for high-neuroticism individuals.	Examine facet-level patterns, gender-specific effects, and the impact of emotional regulation and stress management on phishing resilience.
Conscientiousness	Trait-level: 1 study	Trait-level: 7 studies Facet-level: 1 study (Cautiousness)	Conscientious traits such as diligence and caution can be reinforced in phishing training and simulations.	Clarify why exceptions occur and explore how conscientious strategies (e.g., systematic verification) can be integrated into training.
Openness to Experience	Trait-level: 3 studies	Trait-level: 5 studies	Openness may lead to exploration of suspicious content, but also supports critical evaluation in some contexts.	Explore how openness interacts with factors such as novelty, complexity, and curiosity in phishing scenarios.

Note: Positive and negative effects refer to the reported direction of the association between personality traits and phishing vulnerability.

4.3. Research designs and methodological limitations

As reported in Section 3.2, a significant portion of research studies uses student samples. The reason behind the large representation of students might be because these studies are often conducted in academic environments, where access to students is more available than other profiles. Consequently, the results may be difficult to generalise to the broader population. Hence, with the aim to determine the appropriate sample size for a given population, researchers need to develop a sampling strategy that is reliable and tailored to the specific need of their research study (Kothari, 2004).

The study of human factors influencing phishing vulnerability remains a complex challenge, influenced by multiple psychological and contextual factors. While numerous studies have contributed with valuable insights, the lack of standardised methodologies has limited the comparability and reproducibility of experimental findings. Although not intended to be a core component of the article, the Appendix A section synthesises key insights from prior research to provide complementary guidelines aimed at enhancing methodological rigour, ethical considerations, and experimental validity.

The methodological limitations of the reviewed articles are notable and require attention for future research. It is worth noting that these limitations do not include those referring to the operationalisation and measurement of personality or vulnerability to phishing, described in Section 4.

One of the most notable limitations was the failure of several studies to report participants' basic demographic information, including age, gender, and origin. In certain instances, details provided only referred to the total sample size and the participants' status as students or employees. Such omissions significantly constrain the ability to contextualise the findings and accurately replicate the studies. Moreover, some studies merely offered broad descriptions of results within the text, omitting the actual data in tables, which further compromises the transparency of their findings. Notably, some analyses were conducted with inadequate sample sizes, potentially resulting in unreliable and biased outcomes.

5. Directions for future research

With the aim of advancing the understanding of the role of personality traits in phishing behaviour, future research could explore personality traits at the level of specific facets rather than focusing solely on broader domains or factors. This approach may enhance behavioural prediction, as research indicates that a small set of carefully selected personality facet scales can predict outcomes as effectively as, or even better than the aggregate FFM scales. On the other hand, a sizable portion of the criterion variance that is predicted at facet level is not predicted at factor level (Paunonen & Ashton, 2001).

Moreover, one of the reviewed articles (Huseynov & Ozdenizci Kose, 2022) demonstrated different results in the association between personality facets and phishing vulnerability in the case of neuroticism: while the vulnerability facet showed a positive association with phishing vulnerability, the self-consciousness facet appeared to act as a protective factor. This indicates that in the case of vulnerability to phishing, different facets within the same trait can increase or reduce said vulnerability; hence, the results usually obtained at the personality domain level may not be as nuanced as desired. Methodologically, this suggests that future research designs should incorporate comprehensive personality assessments that evaluate specific facets, such as the NEO-PI-R, rather than relying on the shorter questionnaires that have been prevalent in the reviewed studies. A synthesis of the main findings, their implications, and suggested research directions for each of the Big Five personality traits is provided in Table 7.

From a phishing operationalisation's perspective, the implementation of standardised phishing vulnerability metrics (see Table A.9), enhances cross-study comparability, improves the reproducibility of

experimental findings, and ensures that research outcomes contribute to the broader field rather than remaining isolated case studies. These guidelines aim to establish a foundation for advancing discussions on best practices and standardisation in phishing experimental research.

To enhance realism, participants should ideally not be informed of the study's objectives prior to the exercise, as this could bias their behaviour. Although this approach may pose ethical challenges, researchers should address these challenges with methodological rigour and transparency. Furthermore, ethical guidelines should establish comprehensive frameworks to facilitate researchers in pursuing these lines of research. In this context, Thomopoulos et al. (2023) provide an exploration of the complex ethical dilemmas of studies involving phishing exercises.

Recent literature has explored the relationship between phishing vulnerability and other factors, including gender, age, and demographic characteristics. In addition, it would be interesting to examine the effect and relationship of other constructs within the field of individual differences, such as cognitive abilities or self-control, since it is known that these variables have a relationship with decision-making (Cokely & Kelley, 2009; Frederick, 2005; Jackson et al., 2017; Pang et al., 2015; Skagerlund et al., 2022; Vohs et al., 2008; Wan & Agrawal, 2011) and vulnerability to deception (Calso et al., 2020; Ebner et al., 2020; Mesch & Dodel, 2018). Hence, future research should enhance the comprehension of these constructs' effect on phishing vulnerability and consider their possible moderating effect when designing studies exploring the relationship between personality and phishing vulnerability.

An emerging and pressing direction for future research concerns the rapid evolution of AI-generated phishing content, including large language models (LLMs) and deepfake technologies (Patel et al., 2023; Twomey et al., 2025). These systems are capable of producing highly convincing and personalised messages (Schmitt & Flechais, 2024), synthetic voices (Li et al., 2025), and manipulated video content (Alrashoud, 2025) at scale (often indistinguishable from genuine content). Such capabilities enable hybrid phishing attacks, most commonly used in spear-phishing campaigns (Birthriya et al., 2025), that combine multiple channels (*e.g.,* email, voice, and video) and may undermine the effectiveness of traditional detection and training approaches. Future research should therefore investigate how individual differences influence responses to these AI-enhanced, multimodal attacks, and how these insights can inform the development of adaptive, real-time defence mechanisms. In this line, incorporating gamification techniques (Mpanza et al., 2025) or simulation-based environments (Manoharan et al., 2025) may provide more effective ways to enhance engagement and immersion, thereby improving the quality of the data collected and the impact of training interventions.

Finally, given the multifaceted nature of phishing behaviour, future research should integrate interdisciplinary collaboration across cybersecurity, psychology, and behavioural sciences. These diverse perspectives enable more robust and practical models for mitigating phishing threats. Moreover, fostering stronger partnerships between academia and industry will help create real-world solutions that are more responsive to the evolving phishing landscape.

6. Implications of the study

Based on the observed results, certain personality traits (*i.e.,* neuroticism, extraversion, conscientiousness, and agreeableness) play a relevant role in determining vulnerability to phishing threats. Understanding these roles can lead to improving the already existing awareness and training campaigns and foster the development of targeted interventions and educational programs to mitigate the risks associated with phishing. Likewise, this study highlights the need to enhance consistency in research findings and advance the global state-of-the-art in human behaviour in the phishing context.

While primary prevention measures focus on interventions that target the entire population or specific groups who have not yet been affected by the problem, secondary prevention targets individuals who may be at higher risk or who have already been exposed to the problem (but have not yet experienced negative consequences). In this line, implementing phishing awareness training programs targeted to the profile of each individual might provide more effective results. This approach will certainly enhance the cyber-resilience of specific target groups.

Beyond tailored awareness campaigns, the findings of this review can also guide the design of adaptive phishing exercises, in which content and feedback are tailored to users' personality characteristics. These personalised simulations would improve the realism of training exercises, provide a more detailed understanding of vulnerability patterns, and support the development of more effective interventions.

7. Conclusions

As the number of phishing attacks increases worldwide, it is imperative to adopt novel strategies to enhance the cyber-resilience of the population. This involves not only improving technological defences but also educating individuals about recognising and responding to phishing attempts. Particularly, since personality traits influence the way individuals behave under specific circumstances, understanding the relationship between these traits and vulnerability to phishing is of utmost importance to develop effective, personalised awareness initiatives. By following a rigorous review methodology, this article has presented a literature review on the relationship between personality traits and phishing vulnerability in the available empirical research.

Most studies showed meaningful results on the relationship between phishing vulnerability and the personality traits of neuroticism, extraversion, conscientiousness, and agreeableness. The association with openness to experience produced mixed findings. In this line, the use of diverse methodologies, designs, and measurement tools, disparities in participant characteristics and analytical approaches and, more importantly, the absence of a common standard for operationalising phishing vulnerability demonstrate the complexity of performing substantial progress in the field. However, addressing this complexity and providing clear findings of individuals' phishing behaviour under real-world conditions is paramount.

Despite the undeniable impact of phishing attacks in recent years, the advent of artificial intelligence will certainly present new methods and tools for attackers, given its capacity to autonomously generate highly targeted and credible pretexts. Therefore, if awareness and education campaigns do not adopt the right focus, enhance their effectiveness, and target at-risk groups, societies and corporations will encounter a significant global escalation in successful phishing attacks in the years to come.

Abbreviations

AI	Artificial Intelligence
BFI	Big Five Inventory
BFI-10	Big Five Inventory, 10-item version
BFI-44	Big Five Inventory, 44-item version
FFM	Five-Factor Model
IPIP-NEO-60	International Personality Item Pool, 60-item version
IPIP-NEO-120	International Personality Item Pool, 120-item version
IRB	Institutional Review Board
IT	Information Technology
LLM	Large Language Model
Mini-IPIP	Shortened International Personality Item Pool
ML	Methodological Limitation

NEO-FFI-3	NEO Five-Factor Inventory, 3rd edition
NEO-PI-R	Revised NEO Personality Inventory
PEN	Psychoticism, Extraversion, Neuroticism (Eysenck's Model)
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
SMS	Short Message Service (Text Messaging)

CRediT authorship contribution statement

Pablo López-Aguilar: Writing – review & editing, Writing – original draft, Visualization, Validation, Methodology, Formal analysis, Data curation, Conceptualization. **Carlota Urruela:** Writing – review & editing, Writing – original draft, Visualization, Validation, Methodology, Formal analysis, Data curation, Conceptualization. **Edgar Batista:** Writing – review & editing, Visualization, Validation, Methodology, Formal analysis, Data curation, Conceptualization. **Juvenal Machin:** Visualization, Data curation, Conceptualization. **Agusti Solanas:** Writing – review & editing, Validation, Supervision, Methodology, Funding acquisition, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This work is supported by Ministerio de Ciencia, Innovación y Universidades, Gobierno de España (Agencia Estatal de Investigación, Fondo Europeo de Desarrollo Regional -FEDER-, European Union) under the research grant PID2021-127409OB-C33 CONDOR.

Appendix A. Guidelines for conducting phishing experiments

According to this literature review, experimental phishing studies frequently exhibit methodological inconsistencies, resulting in variations in the assessment of phishing behaviour. Table A.8 summarises the key challenges found in phishing experimental research, categorising them into ethical challenges, inconsistencies to measure phishing vulnerability, ecological validity issues, methodological transparency, and the influence of psychological and contextual factors.

This section introduces guidelines to measure phishing vulnerability within experimental conditions, aiming to overcome the challenges identified in this review. Considering the wide range of phishing tactics and the challenges associated with email management in certain environments (Lanctot & Duxbury, 2025), these guidelines are specially concentrated on experiments in which email serves as the primary attack vector.

A.1. Ethical considerations in experimental designs

Ethical considerations are paramount in the design and execution of phishing experiments, particularly regarding the extent to which participants disclose information. Thus, to guarantee research integrity and safeguard participants' information, phishing experiments should rigorously adhere to established ethical principles. In this context, prior to beginning an experiment, researchers should obtain approval from an institutional ethics review board (IRB), ensuring alignment with human research standards. This review process evaluates the potential risks associated to the use of deception, the adequacy of measures implemented to protect participants, and the study's adherence to established ethical standards.

Under experimental conditions, while participants must formally agree to participate, full disclosure of the study's objectives may introduce bias and undermine the validity of findings (Parsons et al., 2015). To prevent bias and ensure the authenticity of responses, the specific objective of the experiment should not be disclosed before the phishing exercise. However, after the experiment, a comprehensive debriefing should be provided to disclose the study's actual objectives.

Participants should not be informed about the phishing component before the experiment, as prior knowledge may significantly influence their responses. Therefore, partial disclosure is necessary to minimise participant bias in phishing studies. Nonetheless, deception should be limited to the extent required and fully clarified during the debriefing process to maintain ethical integrity.

A.2. Phishing vulnerability metrics

While phishing attacks can take several forms, they typically follow the stages outlined by Mitnick and Simon (2003). As illustrated in Table A.9, experiments designed to measure phishing vulnerability should reflect these key stages and incorporate variables including: opening the email, clicking the link, time to click, replying the email, entering confidential information, and clicking to download a file.

A.3. Ecological validity of phishing experiments

Ecological validity refers to the degree to which research findings can be generalised from controlled laboratory environments to real-world contexts (Schmuckler, 2001). Thus, enhancing ecological validity is critical for ensuring that experimental phishing studies produce findings that accurately represent human behaviour to phishing attacks. While phishing attacks can take endless forms, their objective remains consistent: to establish credibility towards their victims and prompt them to act for the benefit of cybercriminals. In this regard, developing credible pretexts intended to establish credibility would probably furnish more precise information than exercises simulating a fictitious situation. To bridge the gap between controlled experiments and real-world phishing scenarios, researchers should aim to simulate realistic phishing scenarios, recruit participants from diverse demographic groups, and explicitly acknowledge the limitations when findings are based on a homogeneous sample.

- **Realistic phishing scenarios:** A significant limitation in current phishing research is the reliance on simplistic attack simulations, which inadequately replicate the complexity of real-world phishing attempts. Likewise, many studies use generic phishing templates that lack the nuanced social engineering strategies (*e.g.,* email pretext tailored to the target's role, context, or personal circumstances that characterise actual campaigns). In this line, researchers should design contextually relevant pretexts that align with participants' profiles, thereby persuading them to perform actions consistent with the variables detailed in Table A.9. For example, an experiment might simulate an email from the organisation's IT support team, urgently requesting a password reset due to "suspicious login activity" and referencing internal security protocols to enhance credibility.
- **Representative participant sampling:** The generalisability of phishing research is frequently constrained by the use of convenience sampling, particularly the reliance on university student populations. Although this group is easily accessible within the academic context, it fails to reflect the demographic diversity of internet users, whose vulnerability to phishing is influenced by factors including age, professional experience, context, and cultural background. Consequently, researchers should strive to recruit participants from a wider range of demographic groups and explicitly acknowledge the limitations of findings derived from homogeneous samples.

Table A.8
Challenges in measuring phishing vulnerability.

Challenge	Summary
Ethical Challenges	Ethical considerations pose a significant challenge in designing and conducting phishing experiments, particularly concerning participants' deception. Research institutions typically implement rigorous ethical approval processes, which may limit researchers' ability to conduct fully realistic phishing experiments that accurately replicate real-world scenarios.
Phishing Operationalisation	The measurement of phishing vulnerability varies across studies due to the absence of universally accepted variables and metrics. This inconsistency complicates cross-study comparisons and undermines the reliability of phishing vulnerability assessments.
Ecological Validity	Many studies rely on convenience samples, typically consisting of university students or corporate employees. Consequently, the generalisability of findings may be limited, and researchers should explicitly acknowledge these sample limitations, and interpret results within the specific context of the studied population.
Methodological Transparency	Many studies have demonstrated insufficient transparency in reporting essential methodological aspects, including dataset composition, participant recruitment procedures, and experimental conditions.
Psychological and Contextual Factors	The use of inadequate assessment tools to measure these variables can result in findings that lack contextual depth and broader applicability.

Table A.9
Phishing vulnerability variables.

Variable	Description	Phishing Attack Stage
Email Open Rate	Determines if the recipient opens the phishing email, providing insight into the success of the initial deception.	Initial Contact
Click Link Rate	Quantifies the proportion of users who click on phishing links, reflecting their vulnerability to engaging with malicious content.	Engagement
Time to Click	Measures the interval between email receipt and link interaction, offering insights into user impulsivity or cautiousness.	Engagement
Email Reply Rate	Identifies whether participants respond to phishing emails, which may lead to sharing personal information.	Engagement
Credential Submission Rate	Evaluates whether users input login credentials on a phishing site, indicating a deeper level of deception.	Exploitation
File Download Rate	Determines whether recipients download the malicious attachment.	Payload Delivery

Table B.10
Database search strings.

Database	Search string
Scopus	`ALL (''phishing'' AND ''personality'')`
IEEE Xplore	`(''All Metadata'':''phishing'') AND (''All Metadata'':''personality'')`
ACM Digital Library	`[All: ''phishing''] AND [All: ''personality'']`
Web of Science	`TS=(''phishing'' AND ''personality'')`
PubMed	`(''phishing'') AND (''personality'')`

A.4. Methodological transparency and reproducibility

Ensuring methodological transparency and reproducibility is essential for advancing phishing research and establishing reliable, comparable findings across studies. However, inconsistencies in study designs, data reporting, and measurement approaches have limited the ability to replicate experiments effectively.

To overcome these limitations, researchers should implement standardised reporting guidelines that include clear documentation of participant demographics, sample size, experimental design specifications, variable operationalisation, and ethical considerations, incorporating informed consent and debriefing protocols. Standardisation in these areas facilitates cross-study comparisons and enhances research reliability.

Additionally, open data practices and reproducible experiment designs should be prioritised by leveraging data-sharing platforms (*e.g.,* Open Science Framework and Zenodo). These initiatives promote transparency, enable independent verification of findings, and support replication efforts across the research community.

Appendix B. Search strings used for each database

The exact search strings used for each database during the literature search are presented in Table B.10.

Data availability

Data will be made available on request.

References

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, *3*, Article 563060. http://dx.doi.org/10.3389/fcomp.2021.563060.

Alrashoud, M. (2025). Deepfake video detection methods, approaches, and challenges. *Alexandria Engineering Journal*, *125*, 265–277. http://dx.doi.org/10.1016/j.aej.2025.04.007.

Alseadoon, I., Chan, T., Foo, E., & Gonzalez Nieto, J. (2012). Who is more susceptible to phishing emails?: a Saudi Arabian study. In *Proceedings of the 23rd australasian conference on information systems* (pp. 1–11). AIS Electronic Library.

Alseadoon, I., Othman, M., & Chan, T. (2015). What is the influence of users' characteristics on their ability to detect phishing emails? In *Advanced computer and communication engineering technology (LNEE): vol. 315, Proceedings of the 1st international conference on communication and computer engineering* (pp. 949–962). Springer, http://dx.doi.org/10.1007/978-3-319-07674-4_89.

Alsharida, R. A., Al-rimy, B. A. S., Al-Emran, M., & Zainal, A. (2023). A systematic review of multi perspectives on human cybersecurity behavior. *Technology in Society*, *73*, Article 102258. http://dx.doi.org/10.1016/j.techsoc.2023.102258.

Aluja, A., & Blanch, A. (2011). Neuropsychological behavioral inhibition system (BIS) and behavioral approach system (BAS) assessment: A shortened sensitivity to punishment and sensitivity to reward questionnaire version (SPSRQ–20). *Journal of Personality Assessment*, *93*(6), 628–636. http://dx.doi.org/10.1080/00223891.2011.608760.

Anawar, S., Kunasegaran, D. L., Mas'ud, M. Z., & Zakaria, N. A. (2019). Analysis of phishing susceptibility in a workplace: A big-five personality perspectives. *Journal of Engineering Science and Technology*, *14*(5), 2865–2882.

APWG (2024). *Phishing Activity Trends Report – 4th Quarter 2023: Technical Report*, (pp. 1–10). Anti-Phishing Working Group, URL https://docs.apwg.org/reports/apwg_trends_report_q4_2023.pdf.

APWG (2025). *Phishing Activity Trends Report – 3rd Quarter 2024: Technical Report*, (pp. 1–10). Anti-Phishing Working Group, URL https://docs.apwg.org/reports/apwg_trends_report_q3_2024.pdf.

Ayob, Z., & Weir, G. R. (2021). Is human behavior the real challenge in combating phishing. In *Advances in intelligent systems and computing: vol. 1291, Cyber physical, computer and automation system: a study of new technologies* (pp. 27–38). Springer, http://dx.doi.org/10.1007/978-981-33-4062-6_3.

Baker, M. J. (2000). Writing a literature review. *The Marketing Review*, *1*(2), 219–247. http://dx.doi.org/10.1362/1469347002529189.

Bergner, R. M. (2020). What is personality? Two myths and a definition. *New Ideas in Psychology*, *57*, Article 100759. http://dx.doi.org/10.1016/j.newideapsych.2019.100759.

Birthriya, S. K., Ahlawat, P., & Jain, A. K. (2025). Detection and prevention of spear phishing attacks: A comprehensive survey. *Computers & Security*, Article 104317. http://dx.doi.org/10.1016/j.cose.2025.104317.

Brantingham, P. J., & Faust, F. L. (1976). A conceptual model of crime prevention. *Crime & Delinquency*, *22*(3), 284–296. http://dx.doi.org/10.1177/001112876022003002.

Calso, C., Besnard, J., & Allain, P. (2020). Study of the theory of mind in normal aging: focus on the deception detection and its links with other cognitive functions. *Aging, Neuropsychology, and Cognition*, *27*(3), 430–452. http://dx.doi.org/10.1080/13825585.2019.1628176.

Canham, M., Dawkins, S., & Jacobs, J. (2024). Not all victims are created equal: Investigating differential phishing susceptibility. In *International conference on human-computer interaction* (pp. 3–21). Washington DC, USA: http://dx.doi.org/10.1007/978-3-031-61569-6_1.

Canham, M., Posey, C., & Constantino, M. (2022). Phish derby: Shoring the human shield through gamified phishing attacks. *Frontiers in Education*, *6*, Article 807277. http://dx.doi.org/10.3389/feduc.2021.807277.

Caplan, G. (1980). An approach to preventive intervention in child psychiatry. *The Canadian Journal of Psychiatry*, *25*(8), 671–682. http://dx.doi.org/10.1177/070674378002500813.

Carciofo, R., Yang, J., Song, N., Du, F., & Zhang, K. (2016). Psychometric evaluation of Chinese-language 44-item and 10-item big five personality inventories, including correlations with chronotype, mindfulness and mind wandering. *PLoS One*, *11*(2), Article e0149963. http://dx.doi.org/10.1371/journal.pone.0149963.

Cattell, H. E., & Mead, A. D. (2008). The sixteen personality factor. In *The SAGE Handbook of Personality Theory and Assessment: Personality Measurement and Testing: vol. 2*, (p. 135). Sage.

Chrysanthou, A., Pantis, Y., & Patsakis, C. (2024). The anatomy of deception: Measuring technical and human factors of a large-scale phishing campaign. *Computers & Security*, *140*, Article 103780. http://dx.doi.org/10.1016/j.cose.2024.103780.

Cokely, E. T., & Kelley, C. M. (2009). Cognitive abilities and superior decision making under risk: A protocol analysis and process model evaluation. *Judgment and Decision Making*, *4*(1), 20–33. http://dx.doi.org/10.1017/S193029750000067X.

Colom Marañón, R. (2018). Manual de psicología diferencial: Métodos, modelos y aplicaciones. In Spanish.

Cooper, H. (1988). Organizing knowledge syntheses: A taxonomy of literature reviews. *Knowledge in Society*, *1*(1), 104–126. http://dx.doi.org/10.1007/BF03177550.

Costa, P. T., & McCrae, R. R. (1992). Normal personality assessment in clinical practice: The NEO personality inventory. *Psychological Assessment*, *4*(1), 5–13. http://dx.doi.org/10.1037/1040-3590.4.1.5.

Das, A., Baki, S., El Aassal, A., Verma, R., & Dunbar, A. (2019). SoK: A comprehensive reexamination of phishing research from the security perspective. *IEEE Communications Surveys & Tutorials*, *22*(1), 671–708. http://dx.doi.org/10.1109/COMST.2019.2957750.

Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2021). Human factors in phishing attacks: A systematic literature review. *ACM Computing Surveys*, *54*(8), 1–35. http://dx.doi.org/10.1145/3469886.

Donnellan, M. B., Oswald, F. L., Baird, B. M., & Lucas, R. E. (2006). The mini-IPIP scales: Tiny-yet-effective measures of the big five factors of personality. *Psychological Assessment*, *18*(2), 192–203. http://dx.doi.org/10.1037/1040-3590.18.2.192.

Ebner, N. C., Ellis, D. M., Lin, T., Rocha, H. A., Yang, H., Dommaraju, S., Soliman, A., Woodard, D. L., Turner, G. R., Spreng, R. N., & Oliveira, D. S. (2020). Uncovering susceptibility risk to online deception in aging. *The Journals of Gerontology: Series B*, *75*(3), 522–533. http://dx.doi.org/10.1093/geronb/gby036.

Eftimie, S., Moinescu, R., & Răcuciu, C. (2022). Spear-phishing susceptibility stemming from personality traits. *IEEE Access*, *10*, 73548–73561. http://dx.doi.org/10.1109/ACCESS.2022.3190009.

ENISA (2024). *Threat landscape 2024: Technical Report*, (pp. 1–131). European Union Agency for Cybersecurity (ENISA), URL https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

Eysenck, H. J. (1991). Dimensions of personality. In J. Strelau, & A. Angleitner (Eds.), *Perspectives on individual differences*, *Explorations in temperament: international perspectives on theory and measurement* (pp. 87–103). Springer US, http://dx.doi.org/10.1007/978-1-4899-0643-4_7.

Eysenck, H. J., Barrett, P., Wilson, G., & Jackson, C. (1992). Primary trait measurement of the 21 components of the P-E-N system. *European Journal of Psychological Assessment*, *8*(2), 109–117. http://dx.doi.org/10.1027/1015-5759.8.2.109.

Finn, P., & Jakobsson, M. (2007). Designing ethical phishing experiments. *IEEE Technology and Society Magazine*, *26*(1), 46–58. http://dx.doi.org/10.1109/MTAS.2007.335565.

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), Article 103858. http://dx.doi.org/10.1016/j.im.2023.103858.

Frederick, S. (2005). Cognitive reflection and decision making. *Journal of Economic Perspectives*, *19*(4), 25–42. http://dx.doi.org/10.1257/089533005775196732.

Furnell, S., Heyburn, H., Whitehead, A., & Shah, J. N. (2020). Understanding the full cost of cyber security breaches. *Computer Fraud & Security*, *2020*(12), 6–12. http://dx.doi.org/10.1016/s1361-3723(20)30127-5.

Ge, Y., Lu, L., Cui, X., Chen, Z., & Qu, W. (2021). How personal characteristics impact phishing susceptibility: The mediating role of mail processing. *Applied Ergonomics*, *97*, Article 103526. http://dx.doi.org/10.1016/j.apergo.2021.103526.

Goldberg, L. R. (1993). The structure of phenotypic personality traits. *American Psychologist*, *48*(1), 26–34. http://dx.doi.org/10.1037/0003-066X.48.1.26.

Goldberg, L. R. (1999). A broad-bandwidth, public domain, personality inventory measuring the lower-level facets of several five-factor models. *Personality Psychology in Europe*, *7*(1), 7–28.

Gosling, S. D., Rentfrow, P. J., & Swann, W. B. (2003). A very brief measure of the big-five personality domains. *Journal of Research in Personality*, *37*(6), 504–528. http://dx.doi.org/10.1016/S0092-6566(03)00046-1.

Greitzer, F. L., Li, W., Laskey, K. B., Lee, J., & Purl, J. (2021). Experimental investigation of technical and human factors related to phishing susceptibility. *ACM Transactions on Social Computing*, *4*(2), 1–48. http://dx.doi.org/10.1145/3461672.

Hakimi, S., Hejazi, E., & Lavasani, M. G. (2011). The relationships between personality traits and students. *Procedia - Social and Behavioral Sciences*, *29*, 836–845. http://dx.doi.org/10.1016/j.sbspro.2011.11.312.

Halevi, T., Lewis, J., & Memon, N. (2013). Phishing, personality traits and facebook. http://dx.doi.org/10.48550/arXiv.1301.7643, arXiv:1301.7643.

Halevi, T., Memon, N., & Nov, O. (2015). Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. *SSRN Electronic Journal*, 1–10. http://dx.doi.org/10.2139/ssrn.2544742.

He, Y., Donnellan, M. B., & Mendoza, A. M. (2019). Five-factor personality domains and job performance: A second order meta-analysis. *Journal of Research in Personality*, *82*, Article 103848. http://dx.doi.org/10.1016/j.jrp.2019.103848.

Huseynov, F., & Ozdenizci Kose, B. (2022). Using machine learning algorithms to predict individuals' tendency to be victim of social engineering attacks. *Information Development*, *40*(2), http://dx.doi.org/10.1177/02666669221116336.

Islam, A., Rashid, M. M., Othman, F., Kaosar, M. G., & Islam, L. (2025). Identifying personality traits associated with phishing susceptibility. *Security Journal*, *38*, 18. http://dx.doi.org/10.1057/s41284-025-00466-4.

Jackson, S. A., Kleitman, S., Stankov, L., & Howie, P. (2017). Individual differences in decision making depend on cognitive abilities, monitoring and control. *Journal of Behavioral Decision Making*, *30*(2), 209–223. http://dx.doi.org/10.1002/bdm.1939.

John, O. P., & Srivastava, S. (1999). The big-five trait taxonomy: History, measurement, and theoretical perspectives. In *Handbook of personality: theory and research* (pp. 102–138). Guilford Press.

Johnson, J. A. (2014). Measuring thirty facets of the five factor model with a 120-item public domain inventory: Development of the IPIP-NEO-120. *Journal of Research in Personality*, *51*, 78–89. http://dx.doi.org/10.1016/j.jrp.2014.05.003.

Jokela, M., Batty, G. D., Nyberg, S. T., Virtanen, M., Nabi, H., Singh-Manoux, A., & Kivimäki, M. (2013). Personality and all-cause mortality: Individual-participant meta-analysis of 3,947 deaths in 76,150 adults. *American Journal of Epidemiology*, *178*(5), 667–675. http://dx.doi.org/10.1093/aje/kwt170.

Jones, H. S., Towse, J. N., Race, N., & Harrison, T. (2019). Email fraud: The search for psychological predictors of susceptibility. *PLoS One*, *14*(1), Article e0209684. http://dx.doi.org/10.1371/journal.pone.0209684.

Kavvadias, A., & Kotsilieris, T. (2025). Understanding the role of demographic and psychological factors in users' susceptibility to phishing emails: A review. *Applied Sciences*, *15*(4), 2236. http://dx.doi.org/10.3390/app15042236.

Kleitman, S., Law, M. K., & Kay, J. (2018). It's the deceiver and the receiver: Individual differences in phishing susceptibility and false positives with item profiling. *PLoS One*, *13*(10), Article e0205089. http://dx.doi.org/10.1371/journal.pone.0205089.

Kothari, C. R. (2004). *Research methodology: Methods and techniques* (1st ed.). New Age International.

Lanctot, A., & Duxbury, L. (2025). You've got mail – whether you want it or not: An emic investigation into how email use can be managed. *Computers in Human Behavior Reports*, *18*, http://dx.doi.org/10.1016/j.chbr.2025.100618.

Lawson, P. A., Crowson, A. D., & Mayhorn, C. B. (2019). Baiting the hook: Exploring the interaction of personality and persuasion tactics in email phishing attacks. In *Advances in intelligent systems and computing: vol. 822, Proceedings of the 20th congress of the international ergonomics association* (pp. 401–406). Springer, http://dx.doi.org/10.1007/978-3-319-96077-7_42.

Lawson, P. A., Pearson, C. J., Crowson, A. D., & Mayhorn, C. B. (2020). Email phishing and signal detection: How persuasion principles and personality influence response patterns and accuracy. *Applied Ergonomics*, *86*, Article 103084. http://dx.doi.org/10.1016/j.apergo.2020.103084.

Li, M., Ahmadiadli, Y., & Zhang, X.-P. (2025). A survey on speech deepfake detection. *ACM Computing Surveys*, *57*(7), 1–38. http://dx.doi.org/10.1145/3714458.

López-Aguilar, P., Patsakis, C., & Solanas, A. (2022). The role of extraversion in phishing victimisation: A systematic literature review. In *Proceedings of the APWG Symposium on Electronic Crime Research* (pp. 1–10). IEEE, http://dx.doi.org/10.1109/eCrime57793.2022.10142078.

López-Aguilar, P., & Solanas, A. (2021). Human susceptibility to phishing attacks based on personality traits: the role of neuroticism. In *Proceedings of the IEEE 45th Annual Computers, Software, and Applications Conference* (pp. 1363–1368). IEEE, http://dx.doi.org/10.1109/COMPSAC51774.2021.00192.

Manoharan, A., Sriskantharajah, A., Herath, H., Guruge, L., & Yasakethu, S. (2025). Metahuman based phishing attacks in the metaverse realm: Awareness for cyber security education. *Education and Information Technologies*, 1–27. http://dx.doi.org/10.1007/s10639-025-13326-w.

Maples-Keller, J. L., Williamson, R. L., Sleep, C. E., Carter, N. T., Campbell, W. K., & Miller, J. D. (2019). Using item response theory to develop a 60-item representation of the NEO PI–r using the international personality item pool: Development of the IPIP–NEO–60. *Journal of Personality Assessment*, *101*(1), 4–15. http://dx.doi.org/10.1080/00223891.2017.1381968.

Martin, L. R., Friedman, H. S., & Schwartz, J. E. (2007). Personality and mortality risk across the life span: The importance of conscientiousness as a biopsychosocial attribute. *Health Psychology*, *26*(4), 428–436. http://dx.doi.org/10.1037/0278-6133.26.4.428.

McCrae, R. R., & Costa, P. T. (1999). A five-factor theory of personality. In L. Pervin, & O. John (Eds.), *Handbook of personality: theory and research* (pp. 139–153). The Guilford Press.

Mesch, G. S., & Dodel, M. (2018). Low self-control, information disclosure, and the risk of online fraud. *American Behavioral Scientist*, *62*(10), 1356–1371. http://dx.doi.org/10.1177/0002764218787854.

Mitnick, K. D., & Simon, W. L. (2003). *The art of deception: Controlling the human element of security* (1st ed.). (p. 368). John Wiley & Sons.

Mohebzada, J. G., El Zarka, A., Bhojani, A. H., & Darwish, A. (2012). Phishing in a university community: Two large scale phishing experiments. In *Proceedings of the international conference on innovations in information technology* (pp. 249–254). Abu Dhabi, United Arab Emirates: http://dx.doi.org/10.1109/innovations.2012.6207742.

Moher, D., Shamseer, L., Clarke, M., Ghersi, D., Liberati, A., Petticrew, M., Shekelle, P., Stewart, L. A., & Group, P.-P. (2015). Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement. *Systematic Reviews*, *4*, 1–9. http://dx.doi.org/10.1186/2046-4053-4-1.

Mpanza, A., Gundu, T., & Futcher, L. (2025). Gamified defence: Practical guidelines for combating social engineering attacks. In *IFIP world conference on information security education* (pp. 140–151). Springer, http://dx.doi.org/10.1007/978-3-031-94924-1_10.

Myers, I. B., et al. (1962). *The myers-briggs type indicator: vol. 34*, Consulting Psychologists Press Palo Alto, CA.

Nechita, F., Alexandru, D. O., Turcu-Ştiolică, R., & Nechita, D. (2015). The influence of personality factors and stress on academic performance. *Current Health Sciences Journal*, *1*, 47–61. http://dx.doi.org/10.12865/CHSJ.41.01.07.

Pang, B., Otto, A. R., & Worthy, D. A. (2015). Self-control moderates decision-making behavior when minimizing losses versus maximizing gains. *Journal of Behavioral Decision Making*, *28*(2), 176–187. http://dx.doi.org/10.1002/bdm.1830.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2015). The design of phishing studies: Challenges for researchers. *Computers & Security*, *52*, 194–206. http://dx.doi.org/10.1016/j.cose.2015.02.008.

Patel, Y., Tanwar, S., Gupta, R., Bhattacharya, P., Davidson, I. E., Nyameko, R., Aluvala, S., & Vimal, V. (2023). Deepfake generation and detection: Case study and challenges. *IEEE Access*, *11*, 143296–143323. http://dx.doi.org/10.1109/ACCESS.2023.3342107.

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others? *Information Management & Computer Security*, *20*(1), 18–28. http://dx.doi.org/10.1108/09685221211219173.

Paunonen, S. V., & Ashton, M. C. (2001). Big five factors and facets and the prediction of behavior. *Journal of Personality and Social Psychology*, *81*(3), 524–539. http://dx.doi.org/10.1037/0022-3514.81.3.524.

Rahman, A. U., Al-Obeidat, F., Tubaishat, A., Shah, B., Anwar, S., & Halim, Z. (2022). Discovering the correlation between phishing susceptibility causing data biases and big five personality traits using C-GAN. *IEEE Transactions on Computational Social Systems*, *11*(4), 4800–4808. http://dx.doi.org/10.1109/TCSS.2022.3201153.

Rammstedt, B., & John, O. P. (2007). Measuring personality in one minute or less: A 10-item short version of the big five inventory in english and german. *Journal of Research in Personality*, *41*(1), 203–212. http://dx.doi.org/10.1016/j.jrp.2006.02.001.

Roberts, B. W., Kuncel, N. R., Shiner, R., Caspi, A., & Goldberg, L. R. (2007). The power of personality: The comparative validity of personality traits, socioeconomic status, and cognitive ability for predicting important life outcomes. *Perspectives on Psychological Science*, *2*(4), 313–345. http://dx.doi.org/10.1111/j.1745-6916.2007.00047.x.

Sackett, P. R., Lievens, F., Van Iddekinge, C. H., & Kuncel, N. R. (2017). Individual differences and their measurement: A review of 100 years of research. *Journal of Applied Psychology*, *102*(3), 254–273. http://dx.doi.org/10.1037/apl0000151.

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. http://dx.doi.org/10.1002/acp.4075.

Saucier, G. (2009). Recurrent personality dimensions in inclusive lexical studies: Indications for a big six structure. *Journal of Personality*, *77*(5), 1577–1614. http://dx.doi.org/10.1111/j.1467-6494.2009.00593.x.

Schmitt, M., & Flechais, I. (2024). Digital deception: Generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review*, *57*, 324. http://dx.doi.org/10.1007/s10462-024-10973-2.

Schmuckler, M. A. (2001). What is ecological validity? A dimensional analysis. *Infancy*, *2*(4), 419–436. http://dx.doi.org/10.1207/S15327078IN0204_02.

Scholte, R. H. J., & De Bruyn, E. E. J. (2004). Comparison of the giant three and the big five in early adolescents. *Personality and Individual Differences*, *36*(6), 1353–1371. http://dx.doi.org/10.1016/S0191-8869(03)00234-4.

Schöni, L., Carles, V., Strohmeier, M., Mayer, P., & Zimmermann, V. (2024). You know what?-evaluation of a personalised phishing training based on users' phishing knowledge and detection skills. In *Proceedings of the 2024 European symposium on usable security* (pp. 1–14). Karlstad, Sweden: http://dx.doi.org/10.1145/3688459.3688460.

Skagerlund, K., Forsblad, M., Tinghög, G., & Västfjäll, D. (2022). Decision-making competence and cognitive abilities: Which abilities matter? *Journal of Behavioral Decision Making*, *35*(1), 2242. http://dx.doi.org/10.1002/bdm.2242.

Strauss, M. E., & Smith, G. T. (2009). Construct validity: Advances in theory and methodology. *Annual Review of Clinical Psychology*, *5*, 1–25. http://dx.doi.org/10.1146/annurev.clinpsy.032408.153639.

Sudzina, F., & Pavlicek, A. (2017). Propensity to click on suspicious links: Impact of gender, of age, and of personality traits. In *Proceedings of the 30th bled eConference: digital transformation - from connecting things to transforming our lives* (pp. 593–602). AIS Electronic Library.

Sudzina, F., & Pavlicek, A. (2020). Virtual offenses: Role of demographic factors and personality traits. *Information*, *11*(4), 188. http://dx.doi.org/10.3390/info11040188.

Syafitri, W., Shukur, Z., Asma' Mokhtar, U., Sulaiman, R., & Ibrahim, M. A. (2022). Social engineering attacks prevention: A systematic literature review. *IEEE Access*, *10*, 39325–39343. http://dx.doi.org/10.1109/ACCESS.2022.3162594.

Thomopoulos, G. A., Lyras, D., & Fidas, C. A. (2023). Methodologies and ethical considerations in phishing research: A comprehensive review. In *Proceedings of the 2nd international conference of the ACM greek SIGCHI chapter* (pp. 1–10). Association for Computing Machinery, http://dx.doi.org/10.1145/3609987.3609990.

Toledo, F., & Carson, F. (2023). Neurocircuitry of personality traits and intent in decision-making. *Behavioral Sciences*, *13*(5), http://dx.doi.org/10.3390/bs13050351.

Tornblad, M. K., Jones, K. S., Namin, A. S., & Choi, J. (2021). Characteristics that predict phishing susceptibility: A review. In *Proceedings of the human factors and ergonomics society annual meeting: vol. 65*, (pp. 938–942). SAGE Publications, http://dx.doi.org/10.1177/1071181321651330.

Twomey, J., Ching, D., Peter Aylett, M., Quayle, M., Linehan, C., & Murphy, G. (2025). What is so deep about deepfakes? A multi-disciplinary thematic analysis of academic narratives about deepfake technology. *IEEE Transactions on Technology and Society*, *6*, 64–79. http://dx.doi.org/10.1109/TTS.2024.3493465.

Urieta, P., Aluja, A., Garcia, L. F., Balada, F., & Lacomba, E. (2021). Decision-making and the alternative five factor personality model: Exploring the role of personality traits, age, sex and social position. *Frontiers in Psychology*, *12*, Article 717705. http://dx.doi.org/10.3389/fpsyg.2021.717705.

Varshney, G., Kumawat, R., Varadharajan, V., Tupakula, U., & Gupta, C. (2024). Anti-phishing: A comprehensive perspective. *Expert Systems with Applications*, *238*, Article 122199. http://dx.doi.org/10.1016/j.eswa.2023.122199.

Vohs, K. D., Baumeister, R. F., Schmeichel, B. J., Twenge, J. M., Nelson, N. M., & Tice, D. M. (2008). Making choices impairs subsequent self-control: A limited-resource account of decision making, self-regulation, and active initiative. *Journal of Personality and Social Psychology*, *94*(5), 883–898. http://dx.doi.org/10.1037/0022-3514.94.5.883.

vom Brocke, J., Simons, A., Niehaves, B., Reimer, K., Plattfaut, R., & Cleven, A. (2009). Reconstructing the giant: On the importance of rigour in documenting the literature search process. In *Proceedings of the 17th European conference on information systems* (pp. 2206–2217). Verona, Italy: AISeL.

Wan, E. W., & Agrawal, N. (2011). Carryover effects of self-control on decision making: A construal-level perspective. *Journal of Consumer Research*, *38*(1), 199–214. http://dx.doi.org/10.1086/658471.

Welk, A. K., Hong, K. W., Zielinska, O. A., Tembe, R., Murphy-Hill, E., & Mayhorn, C. B. (2015). Will the "phisher-men" reel you in? Assessing individual differences in a phishing detection task. *International Journal of Cyber Behavior, Psychology and Learning*, *5*(4), 1–16. http://dx.doi.org/10.4018/IJCBPL.2015100101.

Williams, M. L., & Levi, M. (2017). Cybercrime prevention. In *Handbook of crime prevention and community safety* (pp. 454–469). Routledge, http://dx.doi.org/10.4324/9781315724393-21.

Yang, R., Zheng, K., Wu, B., Li, D., Wang, Z., & Wang, X. (2022). Predicting user susceptibility to phishing based on multidimensional features. *Computational Intelligence and Neuroscience*, *2022*, Article 7058972. http://dx.doi.org/10.1155/2022/7058972.

Yoro, R. E., Aghware, F. O., Akazue, M. I., Ibor, A. E., & Ojugo, A. A. (2023). Evidence of personality traits on phishing attack menace among selected university undergraduates in Nigerian. *International Journal of Electrical and Computer Engineering*, *13*(2), 1943–1953. http://dx.doi.org/10.11591/ijece.v13i2.pp1943-1953.

Zuckerman, M., Kuhlman, D. M., Joireman, J., Teta, P., & Kraft, M. (1993). A comparison of three structural models for personality: the big three, the big five, and the alternative five. *Journal of Personality and Social Psychology*, *65*(4), 757. http://dx.doi.org/10.1037/0022-3514.65.4.757.