Phishing Susceptibility through Theoretical Lenses: A Systematic Literature Review

Efa Shahira Iskandar, Syarulnaziah Anawar, Zakiah Ayop, and Nur Fadzilah Othman

Faculty of Information & Communication Technology, University Technical Malaysia Melaka (UTeM), Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia

DOI: https://dx.doi.org/10.47772/IJRISS.2025.907000456

Received: 11 July 2025; Accepted: 19 July 2025; Published: 22 August 2025

ABSTRACT

Phishing attacks, which leverage effective social engineering techniques to exploit human vulnerabilities, continue to pose significant risks to internet users. This systematic literature review analyzes phishing attack research from 2010 to 2025, focusing on phishing susceptibility among internet users. Following the guidelines outlined by Kitchenham and Charters (2007), the review comprises three primary phases: planning, execution, and reporting. Study questions were formulated using the PICOC framework to examine the types of phishing attacks, the theoretical frameworks applied, the persuasive elements utilized, and the challenges and research gaps present in existing literature. A comprehensive search of ten primary digital databases yielded 23,479 studies, from which 49 empirical studies were selected for analysis based on rigorous inclusion, exclusion, and quality assessment criteria. The review indicates that email-based phishing remains the predominant form of attack, followed by social media, smishing, and vishing. In addition to commonly employed persuasion strategies such as urgency, fear appeal, and authority, the review identifies prominent theoretical frameworks. This paper also highlights significant research gaps, particularly in platform development and unexplored user demographics, and provides recommendations for future phishing-related studies. The findings advocate for the development of robust preventative strategies and enhance the systematic understanding of phishing susceptibility.

Keywords: phishing attacks, social engineering, internet users, susceptibility, email phishing, social media phishing, smishing, vishing, persuasion, cybersecurity

INTRODUCTION

Phishing is among the most prevalent and impactful forms of online fraud. With the rise of digital interactions during the COVID-19 pandemic, phishing attacks have intensified across multiple platforms, including email, social media, messaging services, and other online channels. This shows that phishing attacks are becoming more diverse and sophisticated, as attackers strategically target widely trusted technology brands and services by exploiting users' implicit trust and emotional triggers.

Phishing is defined as "a scalable act of deception whereby impersonation is used to obtain information from a target" [43]. Traditionally, phishing involves acquiring users' confidential data through deceptive emails crafted to mislead victims into divulging sensitive information. Currently, common phishing variants include spear-phishing, social media phishing, vishing, SMiShing, pharming, and USB-based attacks [44][45]. Despite ongoing awareness campaigns and security measures, phishing remains highly effective, highlighting the inadequacy of current detection and preventive strategies at both individual and organizational levels.

Chiew et al. [46] emphasized that phishing victimization fundamentally arises from behavioral vulnerabilities. Supporting this perspective, Manoharan et al. [47] demonstrated that technological factors alone have minimal impact on reducing phishing susceptibility. Phishing attacks are effective primarily due to their use of social

engineering techniques that bypass conventional security measures by crafting personalized messages designed to evoke urgency, trust, and emotional reactions. Attackers exploit psychological states, prompting impulsive actions without careful evaluation. For example, individuals might hastily click on a malicious link due to excitement over perceived financial incentives or urgent notifications.

Numerous studies have examined user susceptibility to phishing attacks; however, many have predominantly concentrated on email-based phishing, particularly within organizational contexts. There remains a significant lack of empirical research exploring phishing susceptibility across various digital channels and platforms comprehensively. This systematic literature review (SLR) aims to bridge this gap by investigating research related to phishing susceptibility across multiple communication channels through diverse theoretical frameworks.

Additionally, this SLR addresses critical research gaps insufficiently explored by previous reviews. Prior systematic reviews, such as those conducted by [45] and [48], mainly focused on human and cognitive factors without applying theoretical frameworks, limiting the depth of their analyses. Das et al. [49] emphasized methodological approaches without integrating theoretical insights, whereas [50] examined cognitive aspects without considering theoretical frameworks. Davis et al. [51] specifically focused on the banking industry, thereby limiting the applicability of their findings. Similarly, Parker and Flowerday's [52] review concentrated narrowly on social media phishing without structured theoretical grounding.

In contrast, this SLR uniquely contributes by providing an in-depth exploration of phishing susceptibility through multiple theoretical lenses, categorizing various phishing attack types broadly across internet users, and systematically identifying susceptibility factors, theoretical frameworks, and research gaps. It further highlights key challenges and opportunities for future research on phishing susceptibility. By offering a comprehensive, theory-driven, and empirically informed synthesis, this review significantly advances the understanding of the behavioral aspects underlying phishing victimization and supports the development of more effective intervention strategies. Applying theoretical lenses allows for a more structured interpretation of user behavior, identifying the underlying motivations, perceptions, and social influences that contribute to phishing susceptibility. This theoretical grounding is essential for designing targeted interventions and developing robust predictive models to mitigate phishing threats.

REVIEW METHOD

Introduction

This section outlines the methodology for performing a systematic review focused on phishing attacks targeting internet users. Literature reviews play a crucial role in advancing the conceptual, methodological, and thematic aspects across various fields [1]. Nightingale (2009) asserts systematic reviews seek to uncover all studies related to a particular question, providing a comprehensive and impartial overview of the existing literature [2]. This approach ensures that the results are both precise and reliable, rendering them appropriate for scholarly, policy-related, or practical use. A systematic literature review is emphasized by Kitchenham and Charters (2007) as a process that involves identifying, evaluating, and interpreting all available research

Framing Research Questions for the Review

The PICOC framework, which stands for Participants, Interventions, Comparisons, Outcomes, and Context, is used to outline the research focus and create research questions, making sure the review process is organized and thorough (Indre Siksnelyte-Butkiene et al., 2021; Wondimagegn Mengist et al., 2019). The additional element, Context, extends the traditional PICO framework by sitting the research within a specific setting or environment.

Table 1 presents the structure of the research questions using the PICOC framework. This systematic literature review encompassed all empirical studies examining phishing attacks in digital contexts, irrespective of users' previous exposure to phishing awareness training. Consequently, this review did not incorporate any particular

comparison within the PICOC framework.

Hence, this systematic literature review aims, generally, to provide knowledge on the evidence of phishing attack issues and awareness among internet users. Consequently, in the present study, the defined the following research questions to obtain this knowledge:

(RQ):

RQ1: What are the categories of phishing attacks among internet users?

RQ2: Which theoretical frameworks have been employed in phishing susceptibility research?

RQ3: Which phishing susceptibility factors are involved in phishing attack research?

RQ4: What are the challenges and research opportunities for phishing attacks in phishing susceptibility research within users?

Identifying Relevant Works

Following the identification of the research questions, the next step involves defining the search strategy and formulating the search string. The primary aim of the search process is to identify pertinent articles addressing unethical Internet behavior within higher education contexts. The search strategy involved an automated search of digital libraries using a search string derived from the PICOC structure presented in Table 1.

Table 1. Summary Of Pico For This Study

Population	Individual
Intervention	Persuasion factors
Comparison	None
Outcome	Phishing susceptibility
Context	Any empirical studies on phishing susceptibility within internet users

Identifying Search String*:* Specific keywords were defined to outline the database search strings, criteria for inclusion, and exclusion from the systematic review. These search strings were developed according to the PICO framework and included significant synonyms and alternative variations, meanwhile combining keywords using the Boolean operators "AND" and "OR." Based on the PICO framework, the most relevant words were chosen to represent the scope of the study. Initial search phrases were: "internet users," "phishing susceptibility," and "persuasion cues".

The results of the original search were used as a test run to confirm the completeness of the review and were subsequently adjusted. The search string was changed to add different terms such as "email users," "employees," "students," "influence tactics", "social engineering," "urgency," "fear appeal," and "phishing risk," as some significant research was omitted from

the initial search. The final search string utilized for the literature review was: ("internet users" OR "employees" OR "students") AND ("persuasion cues" OR "influence tactics" OR "social engineering") AND ("phishing susceptibility" OR "phishing vulnerability" OR "phishing risk").

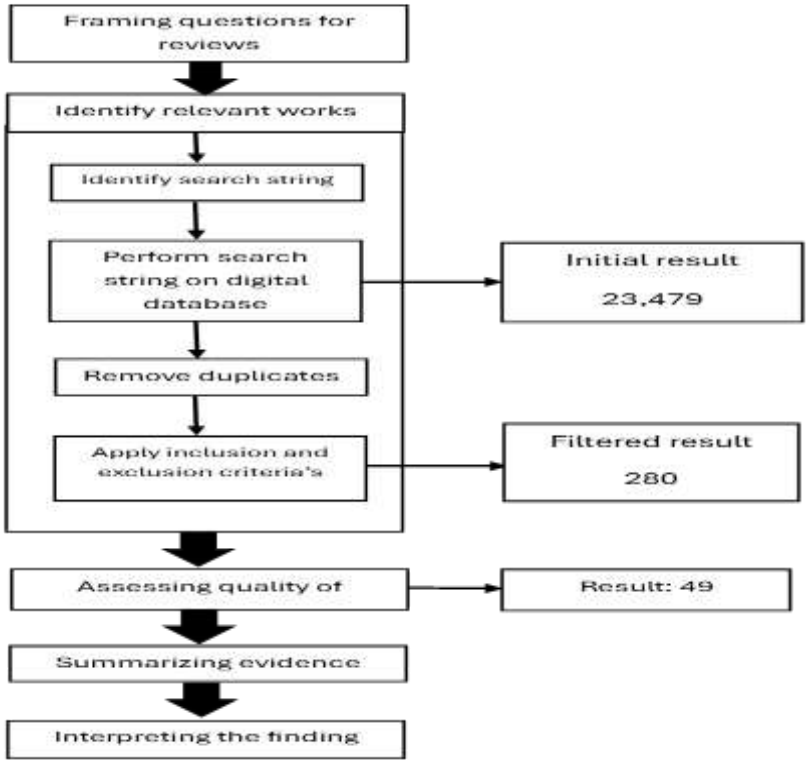

Figure 1. Systematic literature review methodology for this study

2) Identifying the Sources and Selection of Studies: The title and abstract of each publication were examined for keywords to get as many relevant articles as feasible. A total of ten digital databases were used in the primary search process: ACM Digital Library, Semantic Scholar, Emerald, IEEEXplore, Science-Direct, Scopus and SpringerLink.

A systematic literature search was conducted on chosen databases using the search phrase provided above; yielding 4651 studies as a result of the initial search (refer to Table 2). In the next step, all remaining articles' inclusion and exclusion criteria were applied before any duplicate papers were removed.

Inclusion criteria:

1. Articles from year 2010 - 2025
2. Articles must be published in a journal or a conference proceeding
3. Articles published must be empirical
4. Articles must be within the area/domain of computer science, engineering, social engineering, social sciences, education, and information science.

Exclusion criteria:

1. Articles related to law, economy, policy, and regulations,
2. Articles related to internet ethics subject and training.

Table 2. The Result Of The Selection Process

Online Databases	**Initial Results**	**Selected Studies**
ACM Digital Library	5729	10

Semantic Scholar	53	13
Emerald	267	4
IEEEXplore	13889	8
Science-Direct	1436	8
Scopus	58	3
SpringerLink	2047	3
TOTAL	**23,479**	**49**

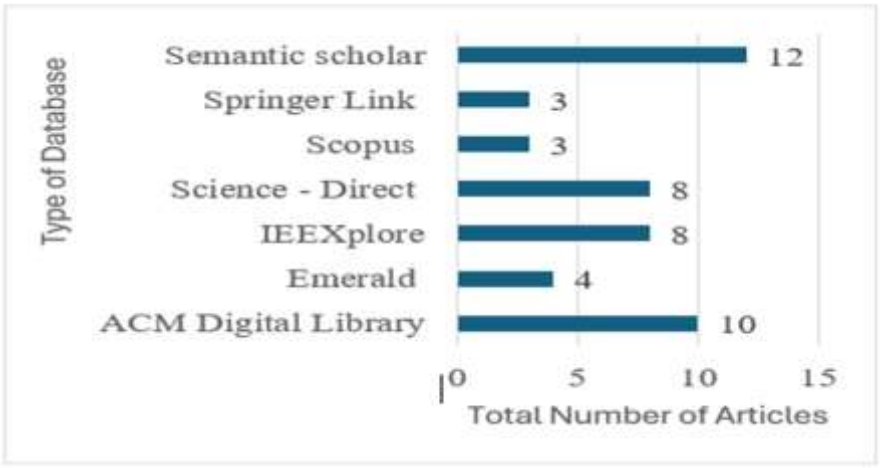

Figure 2. Number of publications based on databases.

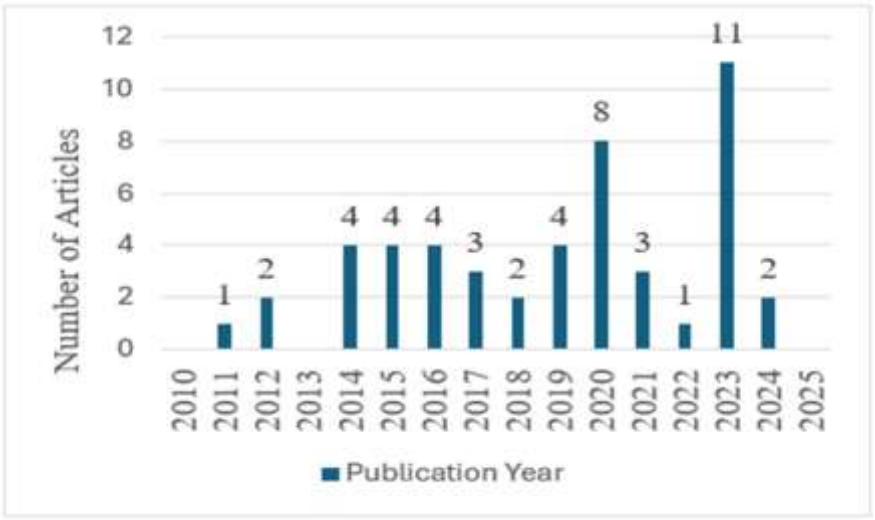

Figure 3. Distribution of studies based on year of publication

The relevant abstracts and full texts were thoroughly reviewed to ensure that only appropriate information was selected for inclusion. The selection processes involved assessing the selected literature to identify papers relevant to the review objectives. Consequently, stringent inclusion and exclusion criteria were applied to refine the results to those most relevant to the review objectives [7], resulting in a final selection of 128 papers. Papers that met the inclusion criteria were selected for further investigation and content assessment, as illustrated in Figure 1.

3) Quality Assessment: The methodology applied for the next step is based on the approaches described in [5], [7], and [8]. Quality assessment was conducted to further evaluate the eligibility of the selected studies, where any discrepancies in findings were discussed and resolved. This step was essential to ensure that the produced SLR on phishing attacks was conducted rigorously and to prevent bias from skewing the research methodology

or interpretation of the results. Common practices for quality assessment involve ranking the studies based on a checklist [8]. Several questions from previous studies [9], [10], [11] were reused when developing the quality checklist. The filtered data (see Fig. 1) were evaluated for each study using the quality assessment checklist (see Table 3). Entire articles were employed when titles and abstracts were inadequate to ascertain a paper's relevance. The quality assessment scoring technique was categorized as good, fair, bad, or unknown (i.e., no information was provided). During the final selection, papers and articles devoid of explicit empirical techniques were carefully rejected. Ultimately, 49 papers were selected as the final subjects for the systematic review (see Table 2).

Table 3. Quality Assessment Checklist

ASSESSMENT	DETAILS
Was the article refereed?	-
Were the aim of the study clearly stated?	-
Were data collections carried out very well?	Quantitative: The paper explains the questionnaire design procedure (mentioning the source of existing scale or explaining design procedure for new questionnaire). Qualitative: The paper explains the design of data collection tool (structured/unstructured question for interview or focus group, observation, diary, journal).
	Sampling: The paper mentions the number of respondents/participants.
	Duration (Longitudinal study/ Qualitative study): The paper mentions the recruitment or data collection time frame. For example: 3 weeks, from January to March
Were the approach to and formulation of the analysis well conveyed?	Quantitative: Minimum of descriptive statistics (mean or media) Qualitative: Include participant's quotation or excerpt from data collection tools.
Were the findings credible?	The paper must be methodologically explained.

RESULTS AND DISCUSSION

Introduction

The results of the search are produced based on the search strings provided in Section II. The current systematic literature review synthesized a total of 49 primary studies (see List of the Included Studies). This figure was established after a comprehensive evaluation of the literature incorporated in the present study. The concentrated-on studies that aligned with the inclusion criteria specified in Section II. Figure 2 illustrates the distribution of the selected studies across the various digital libraries. Figure 3 illustrates the distribution of all studies conducted between 2010 and 2025.

RQ1 - Categorization of Phishing Attacks

For the first research question, Table 4 presents the identified contexts of studies specifically focusing on certain phishing attacks. Phishing attacks have advanced in sophistication, with attackers utilizing various social engineering tactics to influence and deceive victims. Recognizing the diversity of phishing methods is crucial

for developing effective strategies to avoid falling victim to these threats. Studies have explored several vital types of phishing attacks that have been prevalent in the digital world since the early 2000s. The SLR identified thirty-three papers focused on email phishing, 9 articles on social media phishing, four on vishing, and five on smishing.

As phishing is a type of digital theft in which attackers impersonate legitimate or trusted sources in order to take the private and confidential information of users [13]. This behavior frequently manifests itself through phishing emails. Phishing emails are defined as electronic communications that are fraudulent and impersonate trusted organizations. The purpose of these communications is to deceive recipients into disclosing sensitive information, such as login credentials or credit card numbers, by redirecting them to fake websites [12]. Table 4 indicates that thirty - three papers examine phishing emails ([S1], [S2], [S3], [S4], [S5], [S7], [S8], [S9], [S10], [S11], [S12], [S13], [S14], [S17], [S18], [S19], [S21], [S22], [S23], [S25], [S26], [S27], [S28], [S29], [S30], [S39], [S40], [S41], [S43], [S44], [S46], [S47], [S49]) establishing them as one of the most extensively researched and significant categories of phishing attacks over time. Chiew et al. (2018) found that whereas internet users could readily identify older phishing emails due to obvious mistakes, they struggled to detect more recent phishing efforts, underscoring the growing sophistication of phishing strategies. Consequently, phishing emails persist in exerting considerable influence, with elevated success rates, rendering them the most extensively studied variant of phishing.

The extensive use of social media platforms, offering cybercriminals an extensive selection of potential victims, has resulted in the rise of social media phishing. Social media has become an indispensable element of modern life, with usage increasing dramatically over the last decade. Social media phishing, which refers to a type of phishing attack conducted through social media platforms like Facebook and Instagram, is defined as "a form of online identity theft that aims to steal sensitive information such as online passwords and credit card information" [15]. Table 4 indicates that six papers examine social media phishing. Despite social media's prevalence over the past decade, there is still much to explore in this emerging area.

Smishing is a form of social engineering attack that entails crafting deceptive text messages to entice users into engaging with them. The purpose of these messages is to acquire user credentials, deploy malware on devices, or initiate smishing attacks. [17]. The frequency of smishing attacks has been on the rise, coinciding with the global surge in mobile device utilization. The increasing prevalence of smartphones has created a broader target for cybercriminals [18]. The findings presented in the systematic literature review indicate five studies related to smishing attacks (see Table 4).

“Vishing has evolved into a persistent and costly issue" (Bullée, Montoya, Pieters, Junger, & Hartel, 2018). Griffin and Rackley (2008) define vishing, a portmanteau of "voice" and "phishing," as the act of an attacker calling an individual to deceive them into disclosing sensitive information, such passwords or personnel details.

In addition to these commonly studied forms of phishing, lesser-explored attack vectors such as USB-based attacks and pharming also require an attention. USB-based phishing typically involves the physical placement of infected USB drives in target environments, relying on user curiosity or interaction to trigger malware execution [53]. Pharming, by contrast, manipulates DNS settings to silently redirect users to fraudulent websites without their awareness [54]. However, the PICO-based categorization applied in this SLR did not yield empirical studies addressing these methods in relation to user susceptibility or persuasive cues. This absence highlights a significant concern, suggesting that future studies should investigate how such unconventional techniques leverage psychological manipulation and social engineering to deceive users.

Table 4. Type Of Unethical Internet Behaviour Studies Conducted Among Internet Users

Phishing Attacks	**Sources**	**Total Studies**
Email	[S1], [S2], [S3], [S4], [S5], [S7], [S8], [S9], [S10], [S11], [S12], [S13], [S14], [S17], [S18], [S19], [S21], [S22], [S23], [S25], [S26], [S27], [S28], [S29], [S30], [S39], [S40], [S41], [S43], [S44], [S46],	33

	[S47], [S49]	
Social media	[S6], [S15], [S16], [S20], [S24], [S31], [S42], [S45], [S48]	7
Vishing	[S32], [S33], [S34], [S40]	4
Smishing	[S35], [S36], [S37], [S38], [S40]	5

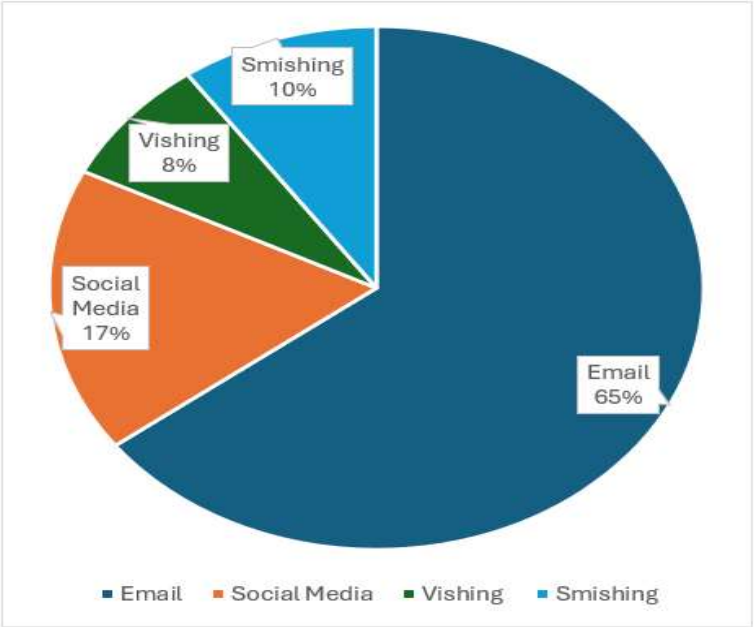

Figure 4. Distribution percentage for phishing attacks categories

RQ2 - Different Theoretical Lenses that are Used in Phishing Attack Research

Theory plays a vital role in research as it establishes a framework for study, facilitates optimal field development, and delivers coherent explanations for real-world occurrences (Wacker, 1998). In the context of phishing attack study, various theories have been employed to examine distinct facets of the issue. Some researchers have utilized integrated theoretical frameworks, whereas others apply a singular theory augmented with elements from additional models. Figure 5 encapsulates the behavioral and psychological theories employed in diverse types of phishing attack research.

The Principles of Persuasion (PP) and Dual Process Theory (DPT) have a significant impact on research on phishing emails. Two of the most popular theoretical frameworks for researching phishing and deceptive communication are PP and DPT. In fields including psychology, communication, information processing, and cybersecurity, these theories have been used as fundamental models for forecasting human behavior. The two cognitive pathways that people use to process information are the intentional, slow, and analytical "System 2" and the intuitive, quick, and automatic "System 1," according to DPT. [22]. Users are more susceptible to persuasion tactics included in phishing messages because phishing attacks frequently take advantage of System 1 processing, which relies on cognitive shortcuts (heuristics) rather than meticulous analysis [23][24]. Therefore, in order to prevent phishing emails, efforts should take into account both cognitive processing modes as well as the impact of behavioral and emotional factors like authority, urgency, and trust cues in message design.

Most researchers used the Heuristic-Systematic Model (HSM) as a framework for comprehending individual interpretation of compelling information. The theory is based on the fact that, depending on their motivation and capacity for interpreting information, humans rely on either heuristic shortcuts or systematic analysis [27]. Attackers often use the heuristic approach in email and social media phishing by flooding consumers with fast, emotionally charged material, which lowers their capacity or inclination for critical thinking [25]. This process makes people prone to regard fraudulent communications as trustworthy. Research indicates that the lure of reward and the fear of loss are psychological triggers that make users more prone to lie on social media sites

[26]. Consequently, HSM has grown to be a common methodology for evaluating user susceptibility to email and social media phishing campaigns.

Signal Detection Theory (SDT) has been widely applied in the study of phishing attacks. SDT is a fundamental framework for comprehending how individuals differentiate significant stimuli from ambiguous or irrelevant information [28]. The distinction is made between an individual's sensitivity as their genuine ability to recognise phishing and their reaction bias, which reflects a tendency to either over-report or under-report threats [29]. SDT has been applied in studies that concern vishing, social media phishing, and email phishing, where decision-making amid uncertainty is essential. Hence, researchers can better understand the psychological mechanisms behind phishing susceptibility and design more effective training and detection systems to reduce both false alarms and missed threats.

The Big Five personality traits cover five broad aspects of human personality. These traits have been extensively used in psychological research, especially with relation to phishing attacks, since researchers want to understand how different personality profiles influence a person's susceptibility. D.W. Fiske (1949) pioneered this approach by using factor analysis to try to bring order to the disorganized nature of several personality trait theories. The model evolved over time through contributions from various scholars and grew; finally, McCrae and John (1992) were formalized in standardizing the model as the Five-Factor Model (FFM), finalizing five consistent personality dimensions that surfaced across societies, age groups, and research approaches. In phishing research, the Big Five provides a methodical approach to examine how persistent personality traits might affect people's responses to false online threats.

These results imply that phishing attacks can be investigated using several theoretical perspectives, each of which helps to define different types of phishing activity. The predominance of some theories inside particular categories emphasizes how still this area of study is developing. Constant investigation of several points of view, including personality psychology, may reveal more about the processes behind people's phishing sensitivity and assist in the development of preventive plans.

No	Theory/Model	Total Studies	Sources
1	Polanyi's Tacit Knowledge Theory	Email • (1 paper)	[S1]
2	Luhmann's Trust as Uncertainty Reduction	Email • (1 paper)	[S1]
3	Lewicki et al.'s Trust-Distrust Dimensionality	Email • (1 paper)	[S1]
4	ELM	Email • (3 papers)	[S2], [S3], [S28]
5	Cialdini's Principles of Persuasion	Email • (9 papers), Social media • (1 paper) Vishing • (1 paper) Smishing • (1 paper)	[S4], [S5], [S7], [S8], [S9], [S18], [S21], [S25], [S36], [S33], [S46]
6	Integrated Information Processing Model (IIPM)	Email • (3 papers)	[S5], [S27], [S28]
7	Prospect Theory	Email • (2 papers)	[S5], [S47]
8	Media Habit Theory	Social media • (1 paper)	[S6]
9	Attitudinal Commitment	Social media • (1 paper)	[S6]
10	Privacy Concern Theory	Social media • (1 paper)	[S6]
11	Big Five Personality Traits	Email • (3 papers) Social media • (1 paper) Vishing • (1 paper)	[S7], [S21], [S41] [S43], [S48]
12	Recognition Primed Decision Model (RPD)	Email • (1 paper)	[S10]
13	Linguistic Inquiry Word Count (LIWC) model	Email • (1 paper)	[S11]
14	Routine Activity Theory (RAT)	Email • (1 paper)	[S12]
15	Suspicion, Cognition, and Automaticity Model (SCAM)	Email • (1 paper)	[S12]

16	Heuristic-Systematic Model (HSM)	Email • (5 papers) Social media • (6 papers)	[S12], [S16], [S19], [S20], [S22], [S24], [S42], [S43], [S44], [S48], [S49]
17	Theory of Deception	Email • (2 papers)	[S13], [S28]
18	Signal Detection Theory (SDT)	Email • (2 papers) Social media • (1 paper)	[S14], [S21], [S31]
19	Uses and Gratifications Theory	Social media • (1 paper)	[S15]
20	Attitudinal commitment theory	Social media • (1 paper)	[S15]
21	Dual-process model of persuasion	Email • (2 papers), Vishing • (1paper) Smishing • (1 paper)	[S17], [S23], [S40], [S47]
22	Socioemotional Selectivity Theory (SST)	Email • (1 paper)	[S18]
23	Lifespan Developmental Theory	Email • (1 paper)	[S18]
24	Suspicion, Cognition, and Automaticity Model (SCAM)	Email • (1 paper)	[S27]
25	Protection Motivation Theory (PMT)	Email • (2 papers) Smishing • (1 paper)	[S27] [S38] [S43]
26	Principles of Persuasion in Social Engineering (PPSE)	Email • (1 paper) Vishing • (1 paper)	[S29], [S32]
27	Space Transition Theory (STT)	Smishing • (1 paper)	[S35]
28	Truth-default theory (TDT)	Vishing • (1 paper)	[S34]
29	Rational Choice Theory	Smishing • (1 paper)	[S35]
30	Technology Acceptance Model (TAM)	Smishing • (1 paper)	[S35]
31	Divergent Thinking Theory	Smishing • (1 paper)	[S39]
32	Theory of Deception (TD)	• Smishing, Vishing, Email(1paper)	[S40]
33	Interpersonal Deception Theory (IDT)	• Smishing, Vishing, Email(1paper)	[S40]
34	Motivation Theory	Email • (1 paper)	[S46]
35	The Self-Regulation Theory	Social media • (1 paper)	[S42]
36	Four-Drive Theory	Email • (1 paper)	[S47]
37	Generalized Communicative Suspicion (GCS)	Email • (1 paper)	[S49]

Fig. 5. Types of theories used in unethical internet behavior research among internet users

RQ3 – Phishing Susceptibility Factors Involved in Phishing Attack Research

This section examines the susceptibility factors for phishing associated with users' engagement in online

interactions, whether as victims, perpetrators, or observers. These factors help explain the psychological and behavioral mechanisms that make individuals vulnerable to phishing scams.One of the most widely used frameworks in this domain is Cialdini's six principles of persuasion: authority, scarcity, reciprocity, commitment, liking, and social proof. These principles represent psychological tactics used in human communication to influence behavior and are frequently cited in phishing research [31]. Studies that incorporate these persuasive cues are especially prominent in explaining user susceptibility [29].

Table 5 provides an overview of how these six principles are distributed across different types of phishing attacks (email, social media, vishing, and smishing). It highlights that Authority and Commitment & Consistency are the most frequently studied tactics. The table also lists key cues linked to each principle, offering a snapshot of the persuasive methods employed in phishing. While figure 6 offers a more detailed analysis, presenting 23 specific susceptibility factors derived from 40 studies. These are mapped to their corresponding principles, including the number of studies that address each cue and their sources. This granular view helps explain how various persuasive elements operate across different phishing contexts and supports the thematic insights discussed in this section.

Table 5. Distribution Of Phishing Susceptibility Factors Across Attack Types

Social Engineering Tactic	Number of Phishing Studies				Unique Study Count
	Email	Social media	Vishing	Smishing	
Authority	32	3	3	4	38
Commitment & Consistency	29	3	1	0	31
Likeability	22	6	0	2	34
Scarcity	28	5	1	2	31
Reciprocity	8	3	2	3	16
Social Proof	5	5	0	0	12

A more granular examination of these susceptibility factors is presented in Figure 6, which breaks down each principle into specific dimensions and cues, along with the corresponding number of studies and their sources. This detailed view allows for a deeper understanding of how various persuasive tactics manifest in different phishing contexts and supports the thematic analysis presented in this section

1)Authority: According to Figure 6, the most often studied factor in phishing susceptibility research is authority. Specifically, 32 distinct papers examined the use of authority-based persuasion in email, social media phishing, vishing, and smishing-based phishing attacks. Primarily it is operationalized through impersonation. To establish credibility and boost the convincing influence of their messages, cybercriminals occasionally pass for trusted people or reputable companies [33], [34]. Cues such source credibility, domain names like official sites, logos, and other visual or textual signals usually connected with authoritative entities help to support this impersonation.

Among the cues under this principle, source credibility was the most frequently examined, appearing in thirty-eight studies ([S1], [S2], [S3], [S4], [S5], [S7], [S8], [S9], [S10], [S11], [S14], [S17], [S18], [S19], [S24], [S25], [S26], [S27], [S28], [S29], [S30], [S33], [S34], [S36], [S37], [S38], [S39], [S40], [S45], [S46], [S47], [S49]).Source credibility in phishing conditions is the way cybercriminals present themselves as trustworthy people or legal businesses to raise the possibility of victims interacting with harmful content. This is consistent with the claim made by Serman and Sims (2022), who underlined that the credibility of endorsers can affect the opinions, attitudes, and actions of receivers towards the endorsed messages. Apart from source credibility, other power-related signals include domain name used in nine studies([S1], [S2], [S3], [S5], [S7], [S10], [S12], [S18], [S45], [S47]]) and logo use (in ten studies: [S3], [S5], [S13], [S17], [S19], [S21], [S22], [S25], [S27], [S44]).

Less often under this persuasion principle were cues like copyright statements (S21) and authority seals[S24].

2) Commitment and consistency: Commitment and consistency are often studied by researchers in relation to phishing susceptibility. This principle captures the psychological tendency of people to act in line with their past behavior and promises. Halttu and Oinas-Kukkonen (2021), and Siddiqi, Pak, and Siddiqi (2022) have pointed out, people are more likely to repeat familiar activities when present activities match previously mentioned intentions. This idea is often expressed in phishing situations by habitual user actions. Thirty-eight studies in all found signals correlated with this inclination including links, attachments, and follow-up contacts. Link interaction was the most often occurring cue; thirty-one studies ([S1], [S2], [S3], [S5], [S7], [S8], [S9], [S10], [S11], [S12], [S13], [S17], [S18], [S19], [S21], [S22], [S23], [S25], [S26], [S27], [S31], [S35], [S38], [S41], [S43] , [S45], [S46], [S47],[S48], [S49]) and six study ([S1], [S7], [S12], [S25], [S35], [S40]) had attachments noted and two studies ([S40],[S41]); follow-up cues observed. People tend to interact more with familiar and engaging digital tools, especially those perceived as casual or intimate environments [33]. This behavioral tendency can be exploited in phishing attacks, where messages are crafted to blend into these familiar interfaces to increase engagement. Whether started by the user or replicated by cybercriminals, these kinds of actions usually happen automatically and raise the possibility of phishing attempts being taken in tow. Therefore, when operationalized through these regular activities, the commitment and consistency principle help much in phishing vulnerability.

3) Likeability: There are 22 studies that address likeability factors. Phishing attacks have been observed to employ a variety of persuasive cues, which have been divided into two primaries abstract: Source familiarity and attractiveness. A lot of recent research tends to alter the message source's properties and investigate how these changes affect the recipients' assessments of the message. Source attractiveness affects implicit attitudes more strongly than explicitly stated ones, claim Smith and Houwer (2014). Persuasive cues fall under source attractiveness and include things like images, logos, colours, typefaces, and grammar.

Eleven studies ([S3], [S5], [S13], [S17], [S19], [S21], [S22], [S25], [S27], [S42], [S48]) mention images; ten studies([S1], [S2], [S10], [S20], [S22], [S29], [S36], [S37], [S43], [S44]) mention logos; three studies [S2, S19, S25] mention colours; two studies ([S1, S25]) mention typeface; and thirteen studies([S1], [S2], [S3], [S5], [S6], [S8], [S9], [S10], [S15], [S18], [S19], [S20], [S25]) mention grammar. These results imply that users' vulnerability to phishing is significantly influenced by the message's linguistic and visual features.

The cues found under Familiarity contain personalization, social connection, and known identity. Reder and Ritter (1992) characterize familiarity, often referred to as the "feeling of knowing," as a metacognitive judgement where individuals assess whether information that cannot be immediately recalled is likely retained in memory and may be accessible in the future. This indicates that individuals often rely on their personal sense of familiarity instead of actively retrieving memories to assess whether something is known to them. The reduction in perceived unfamiliarity diminishes users' skepticism, leading them to overlook a thorough examination of sender email addresses, domain names, or attachments when considering their vulnerability to phishing. Two studies [S36, S37]) reference known identity, seven studies ([S13, S14, S15, S16, S18, S20, S39] reference social connection, and ten studies ([S4, S7, S12, S14, S16, S18, S20, S27, S31, S32, S33]) reference personalization.

4**) Scarcity: Concerning** the way cybercriminals control internet users in phishing schemes, the scarcity idea is rather important. This idea uses psychological triggers to induce urgency and force recipients to take quick action before it's "too late." Time-limited offers abound in phishing messages, meant to persuade recipients to act fast that is, by purchasing something or clicking a link before a deadline or price rise takes place (e.g., [33]). Often used to create urgency, this method has 28 studies looking at its relationship to phishing susceptibility. Phishing Behaviour also depends on persuasive signals connected to exclusiveness. Persuasive cues for scarcity are exclusivity that could refer statements like "selected users only", "private access", or "early invite" phishing messages could present offers or access as limited to a select group, so guiding recipients into acting to preserve a perceived advantage. In sixteen papers ([S1], [S2], [S4], [S5], [S7], [S8], [S9], [S11], [S13], [S14], [S19], [S26], [S33], [S36], [S37]), this tactic is covered. Concurrently, the other persuasive cue for scarcity is deadlines where, more precisely related to time constraints also are quite important. Unlike general urgency, deadlines give a known, limited period for decision-making, which drives people to act before time runs out. twenty papers ([S4], [S6], [S7], [S11], [S12], [S14], [S15], [S17], [S20], [S21], [S22], [S25], [S27], [S28], [S29], [S30], [S39],

[S43], [S46],[S48]]) discuss this aspect. Cognitive constraints greatly affect people's reactions to deadlines, as Altmann, Traxler, and Weinschenk (2017) point out, strengthening the effect of this scarcity strategy.

5) Reciprocity: Fourteen studies examined how reciprocity might be a persuasive element influencing internet users' phishing activity. Under this element, the persuasive cues found consist of offers ([S5], [S8], [S9], [S17], [S18], [S32], [S36], [S37], [S40], [S48]); rewards ([S38], [S39], [S47]); and favors ([S15], [S34], [S35]).

Cialdini (2009) suggests that a part of this phenomenon stems from the human inclination to praise moral behavior. Phishers frequently use kind gestures such as false refunds, free vouchers, or exclusive access to create a sense of obligation [41], so motivating recipients to click dangerous links or distribute private information in response. This is consistent with the gift-exchange theory, according to which people feel obliged by society to react favorably to supposed kindness.

Furthermore, phishing messages could lead to moral conundrums that force consumers into hasty decisions, such as acting fast to claim a prize or risk losing it, thus abusing cognitive limitations [40]. These false interactions can reflect bilateral exchanges, in which victims interact personally with attackers, or they can reflect competitive environments, in which even supposed acts of kindness are used manipulatively to set user reactions.

6) Social Proof: Few research studies have looked closely at how social proof might affect phishing sensitivity. Social proof is the inclination of people to make decisions online [42] depending on the shared experiences, behaviours, and endorsements of others. Under this aspect, two main persuasive cues found are public reviews and mutual friends. Five studies([S5], [S29], [S39], [S48], [S54], [S55]) all of which highlighted how cybercriminals may create positive reviews or testimonials to build credibility and fool consumers into interacting with phishing material, addressed public reviews. This strategy plays on consumers' confidence in peer experiences and social consensus. Supporting this, Amblee and Bui (2011) observed that people may give expert or aggregated public opinion top priority over advice from personally known but uninformed individuals in circumstances involving high-cost or difficult decisions, such buying expensive or technical products. Four studies ([S7], [S16], [S20], [S24], [S44]) addressed the second persuasive cue, mutual friends. These studies indicate that people often evaluate the genuineness of online messages by looking for signs of a social link, like friends or networks they share.

People are more likely to trust phishing messages that look like they came from friends or people they both know, which increases the chance that they will connect with the scam.

Hence, this section has examined various phishing susceptibility factors based on the six principles of persuasion, which influence the degree to which internet users are vulnerable to phishing attacks. These factors include psychological principles such as scarcity, reciprocity, social proof, and urgency, all of which attackers exploit to manipulate users into making incorrect or hasty decisions.

No.	Factor	Dimension	Cues	Total Phishing Studies	Source
1.	Authority	Impersonation	Source Credibility	Email • (24 papers) Social media • (2 papers) Vishing • (3 papers) Smishing • (4 papers)	[S1], [S2], [S3], [S4], [S5], [S7], [S8], [S9], [S10], [S11], [S14], [S17], [S18], [S19], [S24], [S25], [S26], [S27], [S28], [S29], [S30], [S33], [S34], [S36], [S37], [S38], [S39], [S40], [S45], [S46], [S47], [S49]
			Domain Name	Email • (8 papers) Social Media • (1 paper)	[S1], [S2], [S3], [S5], [S7], [S10], [S12], [S18], [S45], [S47]
			Authority's Seal	Email • (1 paper)	[S4]
			Logo	Email • (10 papers)	[S3], [S5], [S13], [S17], [S19], [S21], [S22], [S25], [S27], [S44]
			Copyright Statement	Email • (2 papers)	[S21], [S43]
2.	Likeability	Sources of Attractiveness	Images	Email • (9 papers) Social Media • (2 papers)	([S3], [S5], [S13], [S17], [S19], [S21], [S22], [S25], [S27], [S42], [S48]
			Logo	Email • (7 papers) Social Media • (1 paper) Smishing • (2 papers)	[S1], [S2], [S10], [S20], [S22], [S29], [S36], [S37], [S43], [S44]
			Colors	Email • (3 papers)	[S2], [S19], [S25]
			Typeface	Email • (2 papers)	[S1], [S25]
			Grammar	Email • (10 papers) Social Media • (3 papers)	[S1], [S2], [S3], [S5], [S6], [S8], [S9], [S10], [S15], [S18], [S19], [S20], [S25]
		Familiarity	Known Entity	Social Media • (2 papers)	[S36], [S37]
			Social Connections	Email • (4 papers) Social Media • (3 papers)	[S13], [S14], [S15], [S16], [S18], [S20], [S39]

			Personalization	Email • (6 papers) Social Media • (4 papers)	[S4], [S7], [S12], [S14], [S16], [S18], [S20], [S27], [S31], [S32], [S33]
3.	Reciprocity		Offer	Email • (5 papers) Social Media • (1 paper) Vishing • (2 papers) Smishing • (3 papers)	[S5], [S8], [S9], [S17], [S18], [S32], [S36], [S37], [S40], [S48]
			Rewards	Email • (2 papers) Smishing • (1 paper)	[S38], [S39], [S47]
			Favor	Email • (1 paper) Social Media • (2 papers)	[S15], [S34], [S35]
4.	Scarcity	Urgency	Exclusivity	Email • (13 papers) Vishing • (1 paper) Smishing • (2 papers)	[S1], [S2], [S4], [S5], [S7], [S8], [S9], [S11], [S13], [S14], [S19], [S26], [S33], [S36], [S37], [S46]
			Deadline	Email • (16 papers) Social Media • (4 papers)	[S4], [S6], [S7], [S11], [S12], [S14], [S15], [S17], [S20], [S21], [S22], [S25], [S27], [S28], [S29], [S30], [S39], [S43], [S46], [S48]

			Personalization	Email • (6 papers) Social Media • (4 papers)	[S4], [S7], [S12], [S14], [S16], [S18], [S20], [S27], [S31], [S32], [S33]
3.	Reciprocity		Offer	Email • (5 papers) Social Media • (1 paper) Vishing • (2 papers) Smishing • (3 papers)	[S5], [S8], [S9], [S17], [S18], [S32], [S36], [S37], [S40], [S48]
			Rewards	Email • (2 papers) Smishing • (1 paper)	[S38], [S39], [S47]
			Favor	Email • (1 paper) Social Media • (2 papers)	[S15], [S34], [S35]
4.	Scarcity	Urgency	Exclusivity	Email • (13 papers) Vishing • (1 paper) Smishing • (2 papers)	[S1], [S2], [S4], [S5], [S7], [S8], [S9], [S11], [S13], [S14], [S19], [S26], [S33], [S36], [S37], [S46]
			Deadline	Email • (16 papers) Social Media • (4 papers)	[S4], [S6], [S7], [S11], [S12], [S14], [S15], [S17], [S20], [S21], [S22], [S25], [S27], [S28], [S29], [S30], [S39], [S43], [S46], [S48]

5.	Commitment & Consistency	Habitual	Links	Email • (29 papers) Social Media • (3 papers) Vishing • (1 paper)	[S1], [S2], [S3], [S5], [S7], [S8], [S9], [S10], [S11], [S12], [S13], [S17], [S18], [S19], [S21], [S22], [S23], [S25], [S26], [S27], [S31], [S35], [S38], [S41], [S43], [S45], [S46], [S47], [S48], [S49]
			Attachments	Email • (6 papers)	[S1], [S7], [S12], [S25], [S35], [S40]
			Follow- Up	Email • (2 papers)	[S40], [S41]
6.	Social Proof		Public Review	Email • (3 papers Social Media • (2 papers)	[S29], [S39], [S48], [S54], [S55], [S5], [S46]
			Mutual friends	Email • (2 papers) Social Media • (3 papers)	[S7], [S16], [S20], [S24], [S44]

Fig. 6. List of persuasion factors investigated in phishing attacks studies

RQ4 – Challenges and Research Opportunities for Phishing Attack Research

This section addresses Research Question 4 by identifying the primary challenges and future research directions related to different types of phishing attacks in online environments. The studies reviewed are classified according to phishing attack types: Social Media, Smishing, and Vishing. This categorization facilitates a clearer understanding of the distinct limitations and gaps inherent to each domain. The challenges are summarized and presented in Table 7 to enable comparison and support further research in phishing mitigation.

Challenges in addressing social media phishing attacks are frequently highlighted across the literature, particularly regarding limitations in research design and participant diversity. Several studies emphasize the need for more representative and diverse samples, especially beyond the commonly used college student populations [S6, S20, S48]. Additionally, researchers highlight the absence of real-world behavioral validation—such as whether participants would actually disclose sensitive data, rather than just clicking on links [S48]. Other methodological issues include lack of cross-platform investigations [S16] and restricted geographic coverage [S42], which limit the generalizability of findings. Many studies also advocate for replication studies [S24, S45] and improved experimental controls to test variables such as message framing, urgency, and visual presentation of phishing messages [S31, S48]. These limitations suggest a growing need for more ecologically valid and globally inclusive research in social media phishing.

The existing literature on Smishing (phishing via SMS and mobile messaging) reveals significant research gaps. A primary focus is the need for a taxonomy of smishing and mobile instant messaging phishing attacks, underpinned by extensive and diverse datasets of actual phishing content [S37]. Current research in this area is impeded by insufficient cross-platform analysis and a lack of evaluation across various mobile operating systems and network providers [S36]. The psychological dimensions of smishing are underexplored, with calls for additional research into users' perceptions and responses to mobile-based phishing attempts [S38].

Additionally, recommendations involve enhancing anti-phishing measures for mobile devices and evaluating the effectiveness of persuasion techniques in mobile messaging environments ([S35, S37]). Numerous studies highlight the necessity for research on the efficacy of particular influence and persuasion methods in achieving user compliance in instances of Vishing (voice phishing) [S32, S33]). The utilization of natural language processing for the detection of vishing attempts via voice analysis is suggested as a viable avenue, however mostly unexamined ([S33, S40]).

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume IX Issue VII July 2025

Wider challenges encompass the restricted socio-demographic diversity of study samples and the necessity for longitudinal research methods to evaluate training retention over time [S34]. The efficacy of virtual environments, including chatbots, in training and detection initiatives need additional validation ([S34, S40]). Cultural and linguistic factors influencing vishing susceptibility are inadequately researched and necessitate more comprehensive and inclusive study frameworks

Phishing Attacks	Categories of Challenges	List of Challenges	Total Studies	Sources
Email	Methodological Limitations	i. Small/non-representative sample	4	[S2], [S12], [S43], [S49]
		ii. Indirect measurements / no real-world context and stimulus or design bias	1	[S49]
		iii. Lack of cross-validation / need for replication	2	[S13], [S23], [S43]
		iv. Limited experimental control	1	[S46]
	User and Psychological Factors	i. Unexplored psychological/cognitive mechanisms	5	[S3], [S5], [S7], [S13], [S44]
		ii. Motivation and personality traits	4	[S19], [S44], [S47], [S49]
		iii. Cognitive biases (e.g., Dunning-Kruger, System 1/2)	3	[S3], [S7], [S44]
		iv. Individual differences / baseline	3	[S7], [S17], [S18]
		v. Habitual behavior & risk perception	2	[S29], [S49]
	Technological Advancements in Phishing	i. AI-generated phishing (e.g., ChatGPT)	1	[S4]
		ii. Advanced/specialized attacks (spear-phishing/APT)	2	[S14], [S44]
		iii. Automation/dynamic detection model	3	[S27], [S30], [S44]
		iv. Technical Phishing features (URLs, semantics)	2	[S11], [S27]
	Generalizability and Diversity Issues	i. Lack of demographic/cultural/industry diversity	1	[S3], [S4], [S12], [S26], [S43], [S46], [S49]
		ii. Sampling limited to students or specific roles		[S13], [S17], [S43], [S49]
	Cross-Platform or Contextual Factors	i. Device and platform influence (e.g., phone vs. PC)	3	[S12], [S22], [S46]
		ii. Simultaneous use of SNS and email	1	[S46]
		iii. Non-email phishing (e.g., smishing, mobile)	2	[S39], [S49]
		iv. Contextual differences across environments	2	[S26], [S49]

Social media	Sample and Generalizability Issues	i.	Small or regional samples, lack of cultural/geographic diversity, over-reliance on students.	4	
	Cross-Platform & Device Diversity	i.	Studying only one platform (e.g., Facebook), neglecting mobile vs. PC differences.	3	[S16], [S20], [S48]
	Design & Message Cues	i.	Influence of design (e.g., visual layout) or urgency cues in phishing detection.	4	[S24], [S31], [S45], [S48]
	Need for Control Groups & Realism	i.	Lack of control groups, artificial conditions, self-selection bias.	3	[S6], [S15], [S42]
	Habits & Behavioral Patterns	i.	Exploring habitual use of social media/media multitasking and their correlation with phishing vulnerability.	2	[S6], [S15]
	Experimental Design Limitations	i.	Framing manipulation limitations, seasonal biases (e.g., exam timing), inadequate control of influencing factors.	2	[S42], [S48]
	Cross-cultural Research Needed	i.	Users in other countries or with different cultural backgrounds may respond differently.	2	[S42], [S48]
	Education & Demographic Factor	i.	Need for personalized training or analysis by age, gender, or academic major.	2	[S20], [S48]
Smishing	Real-World and Ecological Validity	i.	Research is needed using real-world interactions (not just simulations) to validate experimental outcomes in vishing/smishing contexts	1	[S35]
	Technical and OS/Carrier Variability	i.	Need for research into how vulnerabilities differ across mobile operating systems and network carriers, and how that influences user susceptibility.	1	[S36]
	Message & Persuasion Technique Taxonomy	i.	Calls for comprehensive collection and categorization of smishing (e.g., MIM-based) messages, including how persuasion tactics affect user responses.	1	[S37]
	Psychology and Awareness Training	i.	Focus on psychological factors and awareness programs specifically tailored for mobile instant messaging phishing (MIM), including automation solutions.	1	[S38]

Vishing	Influence Technique Effectiveness	i.	To examine how different persuasion/influence techniques affect compliance in various organizational and industrial contexts.	2	[S32], [S33]
	NLP and Detection Techniques	i.	Encourages the use of natural language processing to identify persuasion cues in vishing and develop linguistic models for adversarial detection	2	[S33], [S40]
	Broader and Diverse Populations	i.	Recommends using broader, socio-economically diverse participant samples, and accounting for cultural and language factors in phishing vulnerability	2	[S34, [S40]
	Longitudinal and Adaptive Study Design	i.	Advocates for longitudinal studies on training retention and improvements in simulated environments (e.g., chatbots and spear-phishing models)	2	[S34], [S40]
Social media	Sample and Generalizability Issues	i.	Small or regional samples, lack of cultural/geographic diversity, over-reliance on students.	4	[S6], [S20], [S42], [S48]
	Cross-Platform & Device Diversity	i.	Studying only one platform (e.g., Facebook), neglecting mobile vs. PC differences.	3	[S16], [S20], [S48]
	Design & Message Cues	i.	Influence of design (e.g., visual layout) or urgency cues in phishing detection.	4	[S24], [S31], [S45], [S48]
	Need for Control Groups & Realism	i.	Lack of control groups, artificial conditions, self-selection bias.	3	[S6], [S15], [S42]
	Habits & Behavioral Patterns	i.	Exploring habitual use of social media/media multitasking and their correlation with phishing vulnerability.	2	[S6], [S15]
	Experimental Design Limitations	i.	Framing manipulation limitations, seasonal biases (e.g., exam timing), inadequate control of influencing factors.	2	[S42], [S48]
	Cross-cultural Research Needed	i.	Users in other countries or with different cultural backgrounds may respond differently.	2	[S42], [S48]
	Education & Demographic Factor	i.	Need for personalized training or analysis by age, gender, or academic major.	2	[S20], [S48]

Fig. 7. List of challenges in phishing susceptibility studies (users)

In addition to the specific challenges identified in social media, smishing, and vishing, it is equally important to consider how phishing tactics are likely to evolve alongside emerging technologies. Platforms like WhatsApp and Telegram, which offer encrypted messaging, are increasingly being used as channels for phishing attempts. At the same time, AI-generated content such as synthetic voices, deepfake videos, and messages crafted by large language models, is making phishing attacks more personalized, convincing, and harder to detect. These newer techniques often bypass traditional security filters and exploit context-aware manipulation to trick users [54][55]. Looking ahead, future research should broaden its focus to include these advanced attack vectors and work toward developing adaptive, cross-platform detection and prevention strategies that can keep pace with the growing complexity of AI-driven phishing threats.

CONCLUSIONS

This study makes an important contribution by covering multiple phishing channels, moving beyond the

traditional focus on email phishing to also include social media, smishing, and vishing. This broader view shows how phishing attacks are changing in today's digital world. Unlike earlier reviews that mostly looked at cognitive or technical factors, this work combines several theoretical frameworks such as the Heuristic-Systematic Model, Protection Motivation Theory, and the Theory of Planned Behaviour to better explain how users become vulnerable. This approach helps guide more targeted and evidence-based interventions. As the researcher carefully identifying and classifying different phishing scenarios, the study offers a fresh perspective on the challenges of stopping these attacks. It points out gaps like current detection tools falling short, mobile platforms being overlooked, and the need for approaches that better fit real user environments. By filling these conceptual and practical gaps, this review sets the stage for future research and cybersecurity efforts. It advances a practical understanding of why users are vulnerable in an ever-changing online landscape, contributing to the behavioral science of phishing.

Moreover, the rapid rise of AI-generated content and encrypted messaging apps like WhatsApp and Telegram becoming popular channels for phishing, it is crucial for future studies to focus on these fast-developing threats. Many existing studies do not yet cover these emerging vectors, which makes it even more important to develop adaptive strategies that can keep up with new, sophisticated phishing techniques. Finally, by looking at both common and less-studied attack types, including USB-based phishing and pharming, this study encourages researchers and practitioners to explore how social engineering and psychological manipulation work across many different platforms. Overall, this review helps build a more complete and actionable understanding of how users are vulnerable to new and evolving online threats, pushing forward research and defense against phishing.

ACKNOWLEDGMENT

The author(s) gratefully acknowledge the support received from the Kesidang Scholarship program, which provided funding for this research. The scholarship facilitated access to necessary resources and enabled the successful completion of this study. The authors also thank their supervisors and colleagues for their valuable guidance and support throughout the research process.

REFERENCES

1. J. Paul and A. R. Criado, "The art of writing literature review: What do we know and what do we need to know?" International Business Review, vol. 29, no. 4, 2020, doi: 10.1016/j.ibusrev.2020.101717.
2. A. Nightingale, "A guide to systematic literature reviews," Surgery (Oxford), vol. 27, no. 9, pp. 381–384, 2009, doi: 10.1016/j.mpsur.2009.07.005.
3. [3] A. M. Drucker, P. Fleming, and A.-W. Chan, "Research techniques made simple: Assessing risk of bias in systematic reviews," Journal of Investigative Dermatology, vol. 136, no. 11, pp. e109–e114, 2016, doi: 10.1016/j.jid.2016.08.021.
4. J. P. T. Higgins et al., Cochrane Handbook for Systematic Reviews of Interventions, 2nd ed., Chichester, UK: John Wiley & Sons, 2019.
5. W. Mengist, T. Soromessa, and G. Legese, "Method for conducting systematic literature review and meta-analysis for environmental science research," MethodsX, vol. 7, 2019, Art. no. 100777, doi: 10.1016/j.mex.2019.100777.
6. I. Siksnelyte-Butkiene, D. Streimikiene, V. Lekavicius, and T. Balezentis, "Energy poverty indicators: A systematic literature review and comprehensive analysis of integrity," Sustainable Cities and Society, vol. 67, 2021, Art. no. 102756, doi: 10.1016/j.scs.2021.102756.
7. W. Mengist, T. Soromessa, and G. Legese, "Ecosystem services research in mountainous regions: A systematic literature review on current knowledge and research gaps," Science of The Total Environment, vol. 702, 2019, Art. no. 134581, doi: 10.1016/j.scitotenv.2019.134581.
8. Y. Xiao and M. Watson, "Guidance on conducting a systematic literature review," Journal of Planning Education and Research, vol. 39, no. 1, pp. 93–112, 2017, doi: 10.1177/0739456x17723971.
9. B. A. Kitchenham, "Systematic review in software engineering," in Proc. 2nd Int. Workshop on Evidential Assessment of Software Technologies, 2012, doi: 10.1145/2372233.2372235.

10. M. Petticrew and H. Roberts, Systematic Reviews in the Social Sciences: A Practical Guide, Oxford, UK: Blackwell Publishing, 2006, doi: 10.1002/9780470754887.
11. N. Salleh, E. Mendes, and J. Grundy, "Empirical studies of pair programming for CS/SE teaching in higher education: A systematic literature review," IEEE Transactions on Software Engineering, vol. 37, no. 4, pp. 509–525, 2011, doi: 10.1109/tse.2010.59.
12. I. Fette, N. Sadeh, and A. Tomasic, "Learning to detect phishing emails," CiteSeer X, 2007, doi: 10.1145/1242572.1242660.
13. N. Q. Do, A. Selamat, O. Krejcar, E. Herrera-Viedma, and H. Fujita, "Deep learning for phishing detection: Taxonomy, current challenges and future directions," IEEE Access, vol. 10, pp. 36429–36463, 2022, doi: 10.1109/access.2022.3151903.
14. K. L. Chiew, K. S. C. Yong, and C. L. Tan, "A survey of phishing attacks: Their types, vectors and technical approaches," Expert Systems with Applications, vol. 106, pp. 1–20, 2018, doi: 10.1016/j.eswa.2018.03.050.
15. M. N. Banu and S. M. Banu, "A comprehensive study of phishing attacks," in Proc. [Name of Conference], 2013.
16. E. Mouncey and S. Ciobotaru, "Phishing scams on social media: An evaluation of cyber awareness education on impact and effectiveness," Journal of Economic Criminology, 2025, Art. no. 100125, doi: 10.1016/j.jeconc.2025.100125.
17. M. L. Rahman, D. Timko, H. Wali, and A. Neupane, "Users really do respond to smishing," ArXiv, pp. 49–60, 2023, doi: 10.1145/3577923.3583640.
18. S. Mishra and D. Soni, "Smishing detection using backpropagation algorithm," Neural Computing and Applications, vol. 35, no. 10, pp. 4975–4992, 2023, doi: 10.1007/s00521-021-06305-y.
19. S. E. Griffin and C. C. Rackley, "Vishing," in Proc. 5th Annual Conf. Information Security Curriculum Development, Kennesaw, GA, USA, 2008, pp. 33–35, ACM.
20. J.-W. H. Bullée, L. Montoya, W. Pieters, M. Junger, and P. Hartel, "On the anatomy of social engineering attacks—A literature-based dissection of successful attacks," Journal of Investigative Psychology and Offender Profiling, vol. 15, no. 1, pp. 20–45, 2018.
21. J. G. Wacker, "A definition of theory: Research guidelines for different theory-building research methods in operations management," Journal of Operations Management, vol. 16, no. 4, pp. 361–385, 1998, doi: 10.1016/s0272-6963(98)00019-9.
22. J. Evans, "Dual-processing accounts of reasoning, judgment, and social cognition," Annual Review of Psychology, vol. 59, pp. 255–278, 2008, doi: 10.1146/annurev.psych.59.103006.093629.
23. L. Ribeiro, I. S. Guedes, and C. S. Cardoso, "Which factors predict susceptibility to phishing? An empirical study," Computers & Security, vol. 136, 2023, Art. no. 103558, doi: 10.1016/j.cose.2023.103558.
24. M. Waqas, A. Hania, F. Yahya, and I. Malik, "Enhancing cybersecurity: The crucial role of self-regulation, information processing, and financial knowledge in combating phishing attacks," SAGE Open, vol. 13, no. 4, 2023, doi: 10.1177/21582440231217720.
25. X. Luo, W. Zhang, S. Burd, and A. Seazzu, "Investigating phishing victimization with the heuristic–systematic model: A theoretical framework and an exploration," Computers & Security, vol. 38, pp. 28–38, 2013, doi: 10.1016/j.cose.2012.12.003.
26. S. Goel, K. Williams, and E. Dincelli, "Got phished? Internet security and human vulnerability," AIS Electronic Library (AISeL), 2017. [Online]. Available: https://aisel.aisnet.org/jais/vol18/iss1/2/
27. B. Harrison, A. Vishwanath, and R. Rao, "A user-centered approach to phishing susceptibility: The role of a suspicious personality in protecting against phishing," in Proc. 49th Hawaii International Conference on System Sciences (HICSS), 2016, pp. 5628–5634, doi: 10.1109/hicss.2016.696.
28. J. T. Wixted, "The forgotten history of signal detection theory," Journal of Experimental Psychology: Learning, Memory, and Cognition, vol. 46, no. 2, pp. 201–233, 2020, doi: 10.1037/xlm0000732.
29. P. Lawson, C. J. Pearson, A. Crowson, and C. B. Mayhorn, "Email phishing and signal detection: How persuasion principles and personality influence response patterns and accuracy," Applied Ergonomics, vol. 86, 2020, Art. no. 103084, doi: 10.1016/j.apergo.2020.103084.
30. R. R. McCrae and O. P. John, "An introduction to the five-factor model and its applications," Journal of Personality, vol. 60, no. 2, pp. 175–215, 1992, doi: 10.1111/j.1467-6494.1992.tb00970.x.
31. A. Ferreira and S. Teles, "Persuasion: How phishing emails can influence users and bypass security

measures," International Journal of Human-Computer Studies, vol. 125, pp. 19–31, 2018, doi: 10.1016/j.ijhcs.2018.12.004.
32. Z. E. Serman and J. Sims, "Source credibility theory: SME hospitality sector blog posting during the COVID-19 pandemic," Information Systems Frontiers, vol. 25, no. 6, pp. 2317–2334, 2022, doi: 10.1007/s10796-022-10349-3.
33. A. Kamruzzaman, K. Thakur, S. Ismat, M. L. Ali, K. Huang, and H. N. Thakur, "Social engineering incidents and preventions," in Proc. IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), 2023, pp. 494–498, doi: 10.1109/ccwc57344.2023.10099202.
34. M. A. Siddiqi, W. Pak, and M. A. Siddiqi, "A study on the psychology of social engineering-based cyberattacks and existing countermeasures," Applied Sciences, vol. 12, no. 12, Art. no. 6042, 2022, doi: 10.3390/app12126042.
35. Y. K. Dwivedi et al., "Setting the future of digital and social media marketing research: Perspectives and research propositions," International Journal of Information Management, vol. 59, 2021, Art. no. 102168, doi: 10.1016/j.ijinfomgt.2020.102168.
36. C. T. Smith and J. D. Houwer, "The impact of persuasive messages on IAT performance is moderated by source attractiveness and likeability," Social Psychology, vol. 45, no. 6, pp. 437–448, 2014, doi: 10.1027/1864-9335/a000208.
37. L. M. Reder and F. E. Ritter, "What determines initial feeling of knowing? Familiarity with question terms, not with the answer," Journal of Experimental Psychology: Learning, Memory, and Cognition, vol. 18, no. 3, pp. 435–451, 1992, doi: 10.1037/0278-7393.18.3.435.
38. S. Altmann, C. Traxler, and P. Weinschenk, "Deadlines and cognitive limitations," Econstor.eu, 2017. [Online]. Available: http://hdl.handle.net/10419/174039
39. X. Wang, B. Sung, and I. Phau, "How rarity and exclusivity influence types of perceived value for luxury," Journal of Brand Management, vol. 31, no. 6, pp. 576–592, 2024, doi: 10.1057/s41262-024-00359-8.
40. A. Falk and U. Fischbacher, "A theory of reciprocity," Games and Economic Behavior, vol. 54, no. 2, pp. 293–315, 2006, doi: 10.1016/j.geb.2005.03.001.
41. R. Cialdini, Influence: Science and Practice, Pearson Education, 2009.
42. N. Amblee and T. Bui, "Harnessing the influence of social proof in online shopping: The effect of electronic word of mouth on sales of digital microproducts," International Journal of Electronic Commerce, vol. 16, no. 2, pp. 91–114, 2011, doi: 10.2753/JEC1086-4415160205.
43. E. E. Lastdrager, "Achieving a consensual definition of phishing based on a systematic review of the literature," Crime Science, vol. 3, no. 1, pp. 1–10, 2014.
44. Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing attacks: A recent comprehensive study and a new anatomy," Frontiers in Computer Science, vol. 3, 2021, Art. no. 563060.
45. G. Desolda, L. S. Ferro, A. Marrella, T. Catarci, and M. F. Costabile, "Human factors in phishing attacks: A systematic literature review," ACM Computing Surveys (CSUR), vol. 54, no. 8, pp. 1–35, 2021.
46. K. L. Chiew, K. S. C. Yong, and C. L. Tan, "A survey of phishing attacks: Their types, vectors and technical approaches," Expert Systems with Applications, vol. 106, pp. 1–20, 2018.
47. S. Manoharan, N. Katuk, S. Hassan, and R. Ahmad, "To click or not to click the link: The factors influencing internet banking users' intention in responding to phishing emails," Information & Computer Security, vol. 30, no. 1, pp. 37–62, 2022.
48. D. Arévalo et al., "Human and cognitive factors involved in phishing detection: A literature review," in Proc. 2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE), 2023, pp. 608–614, IEEE.
49. S. Das, A. Kim, Z. Tingle, and C. Nippert-Eng, "All about phishing: Exploring user research through a systematic literature review," arXiv preprint arXiv:1908.05897, 2019.
50. P. Burda, L. Allodi, and N. Zannone, "Cognition in social engineering empirical research: A systematic literature review," ACM Transactions on Computer-Human Interaction, vol. 31, no. 2, pp. 1–55, 2024.
51. R. Davis, L. Futcher, and N. Gcaza, "Exploring the theories and factors relating to the susceptibility of the banking industry to social engineering attacks," unpublished.
52. H. J. Parker and S. V. Flowerday, "Contributing factors to increased susceptibility to social media

phishing attacks," South African Journal of Information Management, vol. 22, no. 1, pp. 1–10, 2020.
53. Nissim, N., Ran Yahalom, & Yuval Elovici. (2017). USB-based attacks. Computers & Security, 70, 675–688. https://doi.org/10.1016/j.cose.2017.08.002
54. Karlof, C., Shankar, U., Tygar, J. D., & Wagner, D. (2007). Dynamic pharming attacks and locked same-origin policies for web browsers. Proceedings of the 14th ACM Conference on Computer and Communications Security, 58–71. https://doi.org/10.1145/1315245.1315254
55. [55] Schneier, B. (2021, April). The Coming AI Hackers. Harvard.edu; Belfer Center for Science and International Affairs. https://dash.harvard.edu/entities/publication/3771a301-36aa-4850-981b-3994b5f1cebc
56. Schmitt, M., & Flechais, I. (2024). Digital deception: generative artificial intelligence in social engineering and phishing. Artificial Intelligence Review, 57(12). https://doi.org/10.1007/s10462-024-10973-

List Of Included Studies

1. P.-E. Arduin, "To click or not to click? Deciding to trust or distrust phishing emails," in Decision Support Systems X: Cognitive Decision Support Systems and Technologies, F. Dargam, P. Zaraté, and I. Linden, Eds., Proceedings of the 6th International Conference on Decision Support System Technology (ICDSST 2020), Zaragoza, Spain, May 27–29, 2020, pp. 73–85, 2020.
2. P. M. W. Musuva, K. W. Getao, and C. K. Chepken, "A new approach to modelling the effects of cognitive processing and threat detection on phishing susceptibility," Computers in Human Behavior, vol. 94, pp. 154–175, 2019, doi: 10.1016/j.chb.2018.12.036.
3. B. Harrison, E. Svetieva, and A. Vishwanath, "Individual processing of phishing emails," Online Information Review, vol. 40, no. 2, pp. 265–281, 2016, doi: 10.1108/OIR-04-2015-0106.
4. P. Burda, T. Chotza, L. Allodi, and N. Zannone, "Testing the effectiveness of tailored phishing techniques in industry and academia," in Proc. 15th Int. Conf. on Availability, Reliability and Security, 2020, doi: 10.1145/3407023.3409178.
5. E. J. Williams and D. Polage, "How persuasive is phishing email? The role of authentic design, influence, and current events in email judgements," Behaviour & Information Technology, vol. 38, no. 2, pp. 184–197, 2019, doi: 10.1080/0144929X.2018.1519599.
6. A. Vishwanath, "Habitual Facebook use and its impact on getting deceived on social media," Journal of Computer-Mediated Communication, vol. 20, no. 1, pp. 83–98, 2015, doi: 10.1111/jcc4.12100.
7. T. T. Longtchi, R. M. Rodriguez, L. Al-Shawaf, A. Atyabi, and S. Xu, "Internet-Based social engineering psychology, attacks, and defenses: A survey," Proceedings of the IEEE, vol. 112, no. 3, pp. 210–246, 2024, doi: 10.1109/jproc.2024.3379855.
8. D. Bera, O. Ogbanufe, and D. J. Kim, "Towards a thematic dimensional framework of online fraud: An exploration of fraudulent email attack tactics and intentions," Decision Support Systems, vol. 167, 2023, Art. no. 113977, doi: 10.1016/j.dss.2023.113977.
9. R. Valecha, P. Mandaokar, and H. R. Rao, "Phishing email detection using persuasion cues," IEEE Transactions on Dependable and Secure Computing, pp. 1–1, 2021, doi: 10.1109/tdsc.2021.3118931.
10. R. Wash, "How experts detect phishing scam emails," Proceedings of the ACM on Human-Computer Interaction, vol. 4, no. CSCW2, pp. 1–28, 2020, doi: 10.1145/3415231.
11. T. Xu and P. Rajivan, "Determining psycholinguistic features of deception in phishing messages," Information and Computer Security, vol. 31, no. 2, pp. 199–220, 2023, doi: 10.1108/ics-11-2021-0185.
12. F. Caravaca Sánchez, M. Falcón Romero, J. Navarro-Zaragoza, L. Ribeiro, I. S. Guedes, and C. S. Cardoso, "Which factors predict susceptibility to phishing? An empirical study," Computers & Security, vol. 136, Art. no. 103558, 2023, doi: 10.1016/j.cose.2023.103558.
13. R. Chen, J. Gaia, and H. R. Rao, "An examination of the effect of recent phishing encounters on phishing susceptibility," Decision Support Systems, vol. 133, Art. no. 113287, 2020, doi: 10.1016/j.dss.2020.113287.
14. T. Xu, K. Singh, and P. Rajivan, "Personalized persuasion: Quantifying susceptibility to information exploitation in spear-phishing attacks," Applied Ergonomics, vol. 108, Art. no. 103908, 2023, doi:

10.1016/j.apergo.2022.103908.
15. A. Vishwanath, "Habitual Facebook use and its impact on getting deceived on social media," Journal of Computer-Mediated Communication, vol. 20, no. 1, pp. 83–98, 2014, doi: 10.1111/jcc4.12100.
16. A. Vishwanath, "Getting phished on social media," Decision Support Systems, vol. 103, pp. 70–81, 2017, doi: 10.1016/j.dss.2017.09.004.
17. K. Parsons, M. Butavicius, P. Delfabbro, and M. Lillie, "Predicting susceptibility to social influence in phishing emails," International Journal of Human-Computer Studies, vol. 128, pp. 17–26, 2019, doi: 10.1016/j.ijhcs.2019.02.007.
18. T. Lin et al., "Susceptibility to spear-phishing emails: Effects of internet user demographics and email content," ACM Transactions on Computer-Human Interaction, vol. 26, no. 5, pp. 1–28, 2019, doi: 10.1145/3336141.
19. W. Zhang, X. Luo, S. D. Burd, and A. F. Seazzu, "How could I fall for that? Exploring phishing victimization with the heuristic-systematic model," in Proc. 45th Hawaii International Conference on System Sciences, 2012, pp. 2374–2380, doi: 10.1109/hicss.2012.302.
20. A. Vishwanath, "Diffusion of deception in social media: Social contagion effects and its antecedents," Information Systems Frontiers, vol. 17, no. 6, pp. 1353–1367, 2014, doi: 10.1007/s10796-014-9509-2.
21. P. Lawson, C. J. Pearson, A. Crowson, and C. B. Mayhorn, "Email phishing and signal detection: How persuasion principles and personality influence response patterns and accuracy," Applied Ergonomics, vol. 86, Art. no. 103084, 2020, doi: 10.1016/j.apergo.2020.103084.
22. B. Harrison, A. Vishwanath, Y. J. Ng, and R. Rao, "Examining the impact of presence on individual phishing victimization," in Proc. 48th Hawaii International Conference on System Sciences, 2015, pp. 3483–3489, doi: 10.1109/hicss.2015.419.
23. S. Zhuo et al., "What you see is not what you get: The role of email presentation in phishing susceptibility," ArXiv, 2023. [Online]. Available: https://arxiv.org/abs/2304.00664.
24. R. Valecha, R. Chen, T. Herath, A. Vishwanath, J. Wang, and R. Rao, "An exploration of phishing information sharing: A heuristic-systematic approach," AIS Electronic Library (AISeL), 2015. [Online]. Available: https://aisel.aisnet.org/wisp2015/2/.
25. O. A. Zielinska, A. K. Welk, C. B. Mayhorn, and E. Murphy-Hill, "A temporal analysis of persuasion principles in phishing emails," Proc. Human Factors and Ergonomics Society Annual Meeting, vol. 60, no. 1, pp. 765–769, 2016, doi: 10.1177/1541931213601175.
26. X. Li, D. Zhang, and B. Wu, "Detection method of phishing email based on persuasion principle," in Proc. 2020 IEEE 4th ITNEC, 2020, pp. 571–574, doi: 10.1109/itnec48623.2020.9084766.
27. E. J. Williams, J. Hinds, and A. N. Joinson, "Exploring susceptibility to phishing in the workplace," International Journal of Human-Computer Studies, vol. 120, pp. 1–13, 2018, doi: 10.1016/j.ijhcs.2018.06.004.
28. A. Vishwanath, T. Herath, R. Chen, J. Wang, and H. R. Rao, "Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model," Decision Support Systems, vol. 51, no. 3, pp. 576–586, 2011, doi: 10.1016/j.dss.2011.03.002.
29. A. Ferreira and G. Lenzini, "An analysis of social engineering principles in effective phishing," in Proc. IEEE STAST, 2015, pp. 9–16, doi: 10.1109/stast.2015.10.
30. J. Wang, T. Herath, R. Chen, A. Vishwanath, and H. R. Rao, "Phishing susceptibility: An investigation into the processing of a targeted spear phishing email," IEEE Transactions on Professional Communication, vol. 55, no. 4, pp. 345–362, 2012, doi: 10.1109/tpc.2012.2208392.
31. M. Silic and A. Back, "The dark side of social networking sites: Understanding phishing risks," Computers in Human Behavior, vol. 60, pp. 35–43, 2016, doi: 10.1016/j.chb.2016.02.050.
32. K. S. Jones, M. E. Armstrong, M. K. Tornblad, and A. Siami Namin, "How social engineers use persuasion principles during vishing attacks," Information & Computer Security, vol. 29, no. 2, pp. 314–331, 2020, doi: 10.1108/ics-07-2020-0113.
33. S. I. Hashmi et al., "Training users to recognize persuasion techniques in vishing calls," in Proc. 2023 CHI Conf. Human Factors in Computing Systems, 2023, pp. 1–8, doi: 10.1145/3544549.3585823.
34. M. E. Armstrong, K. S. Jones, and A. Siami Namin, "How perceptions of caller honesty vary during vishing attacks that include highly sensitive or seemingly innocuous requests," Human Factors, vol.

65, no. 2, pp. 275–287, 2021, doi: 10.1177/00187208211012818.
35. E. O. Yeboah-Boateng and P. M. Amanor, "Phishing, SMiShing & Vishing: An assessment of threats against mobile devices," Journal of Emerging Trends in Computing and Information Sciences, vol. 5, no. 4, pp. 297–307, 2014.
36. R. Ahmad, S. Terzis, and K. Renaud, "Content analysis of persuasion principles in mobile instant message phishing," in IFIP Advances in Information and Communication Technology, vol. 678, pp. 324–336, 2023, doi: 10.1007/978-3-031-38530-8_26.
37. R. Ahmad, S. Terzis, and K. Renaud, "Getting users to click: A content analysis of phishers' tactics and techniques in mobile instant messaging phishing," Information and Computer Security, 2024, doi: 10.1108/ics-11-2023-0206.
38. M. L. Rahman, D. Timko, H. Wali, and A. Neupane, "Users really do respond to smishing," in Proc. 13th ACM Conference on Data and Application Security and Privacy, 2023, pp. 49–60, doi: 10.1145/3577923.3583640.
39. P. Rajivan and C. Gonzalez, "Creative persuasion: A study on adversarial behaviors and strategies in phishing attacks," Frontiers in Psychology, vol. 9, 2018, doi: 10.3389/fpsyg.2018.00135.
40. [S. C. Yang, F. K. Chiang, C. L. Huang, and J. Black, "Individual differences in vulnerability to phishing, fake news, and vishing," Clemson OPEN, 2023. [Online]. Available: https://open.clemson.edu/all_theses/4069/
41. D. C. Wilks, J. N. Cruz, P. Sousa, and R. E. Yoro et al., "Personality traits and evidence of personality traits on phishing attack menace among selected university undergraduates in Nigeria," International Journal of Electrical and Computer Engineering, vol. 13, no. 2, pp. 1943–1953, 2023, doi: 10.11591/ijece.v13i2.pp1943-1953.
42. [M. Waqas, A. Hania, F. Yahya, and I. Malik, "Enhancing cybersecurity: The crucial role of self-regulation, information processing, and financial knowledge in combating phishing attacks," Sage Open, vol. 13, no. 4, 2023, doi: 10.1177/21582440231217720.
43. R. Yang, K. Zheng, B. Wu, D. Li, Z. Wang, and X. Wang, "Predicting user susceptibility to phishing based on multidimensional features," Computational Intelligence and Neuroscience, vol. 2022, pp. 1–11, 2022, doi: 10.1155/2022/7058972.
44. M. Hale, "A priori prediction of phishing victimization based on structural content factors," 2017.
45. A. Franz and E. Croitor, "Who bites the hook? Investigating employees' susceptibility to phishing: A randomized field experiment," AIS Electronic Library (AISeL), 2021. [Online]. Available: https://aisel.aisnet.org/ecis2021_rp/125/.
46. R. T. Wright, M. L. Jensen, J. B. Thatcher, M. Dinger, and K. Marett, "Influence techniques in phishing attacks: An examination of vulnerability and resistance," Information Systems Research, vol. 25, no. 2, pp. 385–400, 2014, doi: 10.1287/isre.2014.0522.
47. S. Goel, K. Williams, and E. Dincelli, "Got phished? Internet security and human vulnerability," AIS Electronic Library (AISeL), 2017. [Online]. Available: https://aisel.aisnet.org/jais/vol18/iss1/2/.
48. "Susceptibility to phishing on social network sites: A personality information processing model," Computers & Security, vol. 94, Art. no. 101862, 2020, doi: 10.1016/j.cose.2020.101862.
49. B. Harrison, A. Vishwanath, and R. Rao, "A user-centered approach to phishing susceptibility: The role of a suspicious personality in protecting against phishing," in Proc. 49th Hawaii International Conference on System Sciences (HICSS), 2016, pp. 5628–5634, doi: 10.1109/hicss.2016.696.