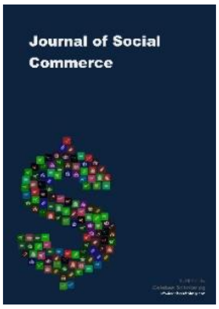

ISSN 2809-929X (Print)
ISSN 2809-9303(Online)

Journal of Social Commerce

Vol. 5 No. 2, 2025 (Page: 173-194)
DOI: https://doi.org/10.56209/jommerce.v5i2.166

University Student Vulnerability to Phishing in Digital Banking across Social Platforms

Mutia Salsanu Fitrah[1], Sri Ramadhani[1], Ahmad Syakir[1]

[1]Universitas Islam Negeri Sumatera Utara, Medan, Indonesia

Article History

Keywords

Phishing Banking
University Students
Digital Banking Services

JEL Classification
D83, L81, M31, O33, Z33

Abstract

Human fallibility to phishing is not the byproduct of ignorance anymore, but the one kept alive by the very structure of digital existence. The aesthetic of deception finds a fertile ground in the repetitiveness of trust, the aesthetic of familiarity, and fluid choreography of the communication process that occurs via a platform. The current paper investigates the effect that can be observed in students of Indonesian universities who, due to their exposure to mobile banking and messaging culture, do not regard phishing as a perversion but as something that may appear to be reality. The research, which is based on in-depth interviews, baffles the conclusion that deception is not triumphing with tricky technical challenges rather with social engineering that hopscotches through interpersonal pathways, uses institutional jargon, and play with emotional instinct. Subjects were not blind to the danger. They are weak, instead, because of the same set of circumstances that conditions them to act quickly, to accept as true signals that are visually consistent, and to place the value of the urgent ahead of checking. This evidence means that the issue is not the absence of awareness but the weakness of awareness in the face of pressure. Therefore, there is a need to change the way the digital vulnerability is thought of. Security should not be a personal issue that creates a vacuum out of a context. Rather, it needs to be regarded as a social/infrastructural question, one that is informed by design, by platform logic, by the relational predilections by which we characterize our everyday digital practice.

Introduction

In the modern context of platformed living digital financial services have entered the everyday life of university students. The rising popularity of mobile banking, apps and online payment tools amounts to more than adapting to the latest technology, instead, it is an indication of the naturalization of the digitally constructed financial being. This realignment is very conspicuous in Indonesia. With the rates of mobile penetration increasing and financial technologies becoming more affordable, digital tools to manage personal finances, pay tuition fees, consumer purchases, and transfers between peers are also used by the students more. As per

[1]Corresponding Author: Mutia Salsanu Fitrah, Email: mutiasalsanu958@gmail.com, Address: Jl. William Iskandar Ps. V, Medan Estate, Kec. Percut Sei Tuan, Kabupaten Deli Serdang, Sumatera Utara 20371

the 2022 data released by Bank Indonesia and OJK, digital banking operations witnessed significant rise among young individuals, wherein university students composed a considerable percentage of mobile banking users in registration. The trends are widely considered to reflect the growth of digital literacy and economic inclusiveness. And, indeed, behind all that optimism is a low-visibility rewiring of risk that is critically important. Users grow accustomed to relying on the performance and comfort of these systems, so they can succumb to their inconvenience by simply relying on their performance and ease of use.

These behavior changes have gone hand in hand with phishing changes. No more are simple emails with links which could lead to unknown programs and bad grammar; phishing is an art now. The misleading messages are conveyed using channels that the recipients are familiar with like WhatsApp, SMS and even university based. Such messages no longer affect us as external threats; instead, they are styled and look similar to their reputable and trusted institution counterparts. The ways phishers are leaning towards using personalized speech and visual consistency in order to display authority have been noted by La Torre & Angelini (2025). Most recent studies by Maseko (2023) also show that modern phishing messages are designed so that they resemble genuine ones as much as possible, including using logos, tone and timing of the message that is identical to those used by legitimate bank services. The paper records a revolutionary moment in the creation of online fraud. The modern misdirection spreads further than the event of insufficient information today; the environments with aesthetic excess of recognition and automation of behavior have erased the epistemic borders.

It is in this context that the university students form a critical group. Though their familiarity with digital environments may be confused with the knowledge regarding digital security, their repurpose use of messaging systems, their peer-to-peer dependence, and their multiple-tasking tendencies expose them to carefully crafted phishing processes in particular. In previous studies, especially Abroshan et al. (2021) and Chou et al. (2021), it was established that students have conceptual understanding of the dangers of phishing, but they are not able to convert that understanding into behavioral changes. Okoli (2021) also demonstrate that users will be more likely to apply intuitive reasoning as opposed to analyzing the situation when under an emotional urgent condition or during mental fatigue, even despite identifying possible dangers. Therefore, the sensitivity turns out to be a weak barrier and to be overwhelmed by the emotional and situational stresses of the moment of choice.

Phishing is, also, closely tied to the communication infrastructures through which they pass. It prospers in an environment in which individual, educational, and affluent transactions take place on one platform and more often in the same lines of issues. Akeiber (2025) emphasize that in procedural terms modern phishing has to be caught not only as a technical infiltration but also as a kind of social engineering that in its course takes advantage of platform affordances and the trust in relationships. Msallati (2021) enhance this analysis by showing that message credibility is never judged alone; according to previous research, credibility always happens to be mediated by who is saying it, when messages are said, and what they are deemed to be relevant to a situation.

To conclude, this study draws attention to another digital deception stage, where technical vulnerabilities are not the only factors in mediating shift in directions of action but the widespread acquaintance, automation, and emotional pliability of the current digital environments. In the environment of modern Indonesian universities, where students are normally provided with legit bank notifications, group updates, as well as text messages sent by peers via one application, effective phishing operation would not involve creating the sense of trust by phishing but rather simulating the circumstances within which the trust is traditionally granted. The convergence of the language systems that finds itself in the common digital realms also erodes the effectiveness of traditional phishing countermeasures, i.e., authenticating sender identities or analysing URLs.

In such a way, the present research questions the prerequisites of phishing being probable among Indonesian university students and redirects the emphasis away of the technical vulnerability or psychological weakness to the way the regularity in the platform, emotional triggers, and peer-driven information transmission interact with one another. It addresses this issue by conducting in-depth qualitative interviewing of students who have experienced or had a close escape of phishing lures to gain an understanding of how users interpret and cope with such deceptive messages, and in what ways these socio-technological processes are mediated by broader social and technological processes. As opposed to the characterization of these users as passive victims or uninformed actors, the study dismisses treating them as situated agents, whose choices are formed in a situation where it is difficult to draw a line between authenticity and fraud. In these ways, it helps to make the study of digital risk more empirically rooted, recognizing that vulnerability is often a structural product of the manners in which trust are produced, diffused, and engineered inside and across digital platforms.

Theoretical Framework

Student Vulnerability Level

Vulnerability is a condition that results in the inability of a person or group of people to resist a threat that occurs (Tasri et al., 2021). Individual vulnerability to external influences includes two main aspects: normative vulnerability and informational vulnerability. Normative vulnerability occurs when individuals follow the norms or expectations of their social groups, such as peers or academic communities, without considering the risks. Meanwhile, informational vulnerability arises when individuals tend to rely on information from sources that are considered more authoritative. In the context of university students, these two aspects can influence their behavior in using digital technology and banking services (Valiansyah et al., 2023).

In the KBBI or Big Indonesian Dictionary, it explains that the definition of a student is a person who studies in college. Students are considered as individuals who have a high level of intelligence and intellect and are able to think logically and structured in planning actions. The ability to think critically and act quickly and precisely is a characteristic that is generally possessed by students, where the two aspects complement each other (Yano et al., 1975).

A student's level of vulnerability refers to the condition in which the student is susceptible to external influences that may affect their decisions and behaviors. This vulnerability includes normative vulnerability, which is when students follow social norms without considering risks, and informational vulnerability, which is the reliance on information from perceived authoritative sources without verification. Although university students are known for their critical thinking skills, social and environmental pressures can increase their level of vulnerability in various aspects of life.

Digital Banking Services

According to the Financial Services Authority Regulation Number 12/POJK.03/2021 of 2021 concerning Commercial Banks (2021), a Digital Bank is a BHI Bank that provides and conducts business activities primarily through electronic channels without physical offices other than KP or using limited physical offices. Digital banking includes various banking services that can be accessed through digital platforms, such as internet banking and mobile banking (Simatupang et al., 2024). Virtual banks are banking institutions that provide retail services through the internet or various other electronic channels, without requiring the presence of physical branches. This service includes all online transactions, whether conducted through websites, emails, or ATM machines (Batubara & Anggraini, 2022).

Digital banking services have changed the way banks operate and interact with customers, especially in Indonesia, along with the development of technology. These services include internet banking, mobile banking, SMS banking and phone banking, which enable easier and more efficient transactions. Its advantages include flexible access, time saving, and real-time balance monitoring. To maintain security, banks implement encryption and double authentication in their systems (Margie et al., 2024).

Phishing Banking

Phishing according to Muda (2024) comes from the English language, namely fishing or fishing, this activity is carried out according to its name, namely committing fraud by luring its victims to provide their personal information unconsciously. Phishing is a requesting activity by luring computer users to reveal personal secrets about personal data, which is carried out by sending fake important messages, which can be in the form of emails, websites, or other forms of electronic communication (Nur, 2023). Phishing is a growing threat to companies around the world, with increasingly sophisticated attack techniques. After successfully bypassing security systems, most phishing emails are opened by recipients, which increases the potential for users to access malicious content and cause cybersecurity incidents. These attacks exploit human psychological aspects by leveraging emotions such as concern, fear, and uncertainty to gain unauthorized access to sensitive information (CyberTalk, 2022).

Phishing attacks are inseparable from social engineering techniques, which are methods of psychological manipulation used to trick victims into taking certain actions without realizing the threat. One technique often used in phishing is to take advantage of the alpha mode in the human brain, which is characterized by a relaxed state, lack of focus, and a tendency to think automatically. Under these conditions, victims are more prone to follow directions without critical thinking, making them more easily fooled by convincing phishing messages (Anindyaa et al., 2024).

Phishing banking is a form of cybercrime that aims to steal sensitive information, such as personal data, account numbers, or login credentials to digital banking services. Phishing is usually done through manipulative techniques such as posing as a trusted party, such as a bank or official institution, by sending fake links via email, SMS, or media (Agusthin et al., 2024). This technique takes advantage of the victim's negligence or lack of awareness of digital security, so the victim tends to follow the directions of the perpetrator without realizing the risks. This is further exacerbated when victims are in alpha mode, which makes them more susceptible to psychological manipulation and more likely to provide personal information without thinking. Therefore, understanding social engineering techniques is key in preventing and reducing the risk of phishing attacks. Phishing prevention in digital banking can be done through user education, email protection, anti-phishing software, and OTP systems. Banks in Indonesia have implemented preventive measures, such as displaying warnings for users to beware of malware and phishing (Muftiadi et al., 2022). However, their effectiveness still depends on users' awareness and caution in keeping their accounts secure.

Methods

The current study has adopted qualitative approach with explorative descriptive orientation in order to assess the susceptibility of university students to phishing activities as experienced in the online banking environments, especially with these activities facilitated by use of social media like WhatsApp, SMS and email. Since there is a necessity to clarify subjective experience and thoughts of students, their unstructured ways of responding behaviorally to phishing events, which are often dictated by the situational social cues and the forces of interpersonal relationships, a qualitative design was selected. Since the current extensive empirical literature provides little details of the mechanism of online banking phishing interpretations among populations of young adults through the informal social context, the explorative descriptive research design was appropriate. The respondents were 11 students of a university in various campuses in Indonesia; all were seen as active customers of digital banking service providers and had been targeted by at least one phishing attempt. Purposive sampling method was used to ensure that only those with first time personal experience which is directly relevant to the objectives of the study was used. This criterion-based selection approach allowed the researchers to focus on the participants who could present detailed, thoughtful reports of genuine phishing incidents, incidents that are supported or originated during social communication situations.

The collection of data was done through semi-structured in-depth interviews. This format helped the researchers to be consistent on the major themes whereas having the participants with certain freedom to talk about their own experiences, perceptions and actions. In the interview guide, the following several dimensions have been explored by using open-ended questions: (1) how frequently and in what form the digital banking is used; (2) what kind of platforms phishing attacks are received via; (3) how students decide to take action to address these attacks; and (4) whether they pay attention to risks in dealing with phishing attacks, and how they protect themselves. The interviews were held over the internet through safe video chat rooms, where the participants could answer the questionnaire in various geographical locations, without any access restriction, and audio-recorded with their tacit agreement. The interviews took 30-60 minutes.

In order to combine the information provided by the participant during the interview, the author organized a limited behavioral observation of the participants in the online sessions where he/she asked participants to describe and demonstrate their behavior related to the use of the digital banking application and answering unsolicited messages, which they usually use. Even though these observations were unstructured and lacked a systematic coding, they provided some background to the interview data, especially about the habitual encounters of the students with mobile interface and social messaging tools. Secondary was also secondary data in form of documentation of related cases reports and institutional records of phishing trends to support and triangulate the primary findings. Thematic analysis of data took place and started with the transcription and reduction of data. Researchers isolated frequent appearance of codes, and divided them into wider themes, such as trends of platform-based deception, emotional reactions to phishing emails, and gaps in security awareness. They used constant comparison of themes to build similarities and individual differences among the participants to improve themes iteratively. Interest was on the awareness of how the social cues were reflected on the likelihood (by participants) to do as an instruction as fraudulent attempt requests, as that is defined by the familiarity of the sender names, informality of language as well as the trust in platform-specific branding (i.e. availing branding logos of the banks on the WhatsApp platform).

Results and Discussion

This part displays the results of the research through the theme analysis of the in-depth interviews of eleven students of the university who actively use digital banking services and have already at least once faced an attempt of phishing. A data interpretation was inductively coded using both iterations of coding and comparative pattern detection and was based on an interest not only in the structural mechanics of phishing mechanisms, but the social, psychological, and behavioral contexts that present students as vulnerable in the digitally mediated environments of financial transactions. Instead of the statistic generalization, the analysis is done at the depth and complexity of student experiences to unpack how phishing is misusing daily habits, platform infrastructures, emotional reflex, and overwhelmed cybersecurity processes.

The data derived four major themes. The former is the extreme reliance of the students on online banking in their ordinary dealings and how this familiarization has minimized critical awareness. The second one investigates the operation of the social communication channel (especially WhatsApp and SMS) as a trusted channels of deception by phishers.The third one examines the elements of psychological manipulation and the emotion-based decision-making process, whereby the defense of users is destroyed by cognitive insights, emotional pressure, and urgency. The last theme brings out discrepancy of knowledge and proper security conducts as awareness of phishing dangers most times does not convert to good discipline. In combination, these themes highlight a paradigm of a multifaceted interaction that resists shortcuts of user ignorance and in its place spotlights an ecology of vulnerability.

Depending on Digital Banking Everyday Transactions Heavily Relying on Digital Banking Daily Transactions

The most uniform tendency was seen across the interviews where the use of digital banking turned out to be a highly ingrained and usually unexplored habit in the everyday life of students. What comes out of it is not only a practically contingent dependence on banking technology but, rather, an expanded socio-technical embeddedness in which the practices of digital financial behavior become little dispirited, emotional flat, and cognitively mechanized. Such integration instigates infrastructural trust and constructs certain kind of digital subjectivity which is operationally as well as structurally exposed and vulnerable.

> *"I basically use mobile banking every day transferring money to friends, paying for food deliveries, sometimes even splitting bills during group work."(Participant 2)*

Seemingly banal, such a statement indexes one of the key conditions: financial micro-transactions in the digitally mediated social routine of students have already become normalized. What the student is not making a description of is a specialised financial activity of banking but a naturalization of a stratum of social interaction in everyday life. In this case, the banking platform can be regarded as a tool as well as the infrastructural element of relational life. As the financial exchange becomes part of the comfortable societal rhythms and ways, e.g., the costs sharing with the peers, it stops being labeled a high-stakes and the high-attention behavior. Such is the state of affairs phishing actors exploit: banking used to be an event, it now became a habit. This routine decreases the critical threshold of the user, who will not check since they will feel that this is familiar.

> *"I keep my banking app open most of the time, and I don't even log out because it's faster that way when I need to make quick payments."(Participant 5)*

This quotation indicates a more basic economy of time and emotion in terms of speed, timeliness, and collision-free communication. This is because traditionally, the priorities of digitally native users are the area of convenience not touching on the aspects of procedural security, perhaps what Kurkovsky & Syta (2010) would refer to as the logic of smoothness of the interface. Focusing on unhindered access, the student externalizes the trust to the device and the platform thereof, under the assumption of the persistence of security established without the direct involvement of the user. This is an indication of structural dependence on platform reliability where vigilance on the part of the user is made less important. Furthermore, maintaining the session in an active state provides the student with an additional point of attack that may be exploited by the phishers in the context of their social engineering attacks that may either provide the impression of a sense of urgency or imminent vulnerabilities (e.g., late night messages). The platform is not perceived as a gateway, but as an ambient utility, a reliable one constantly at the disposal of the user, which breaks down the critical stance of the user.

> *"I often get notifications that look like bank alerts, and I don't really question them. I just assume they're real because I use the app so much anyway." (Participant 7)*

Such acknowledgement announces the degradation of semiotic choice of authentic and inauthentic digital signals. With daily, genuine alerts, the students emerge with a habituated cognitive schema a blueprint of expectation on which new alerts will be audited. Phishers take advantage of this mental model by creating spoofed signals that gels with such expectations. Trust, in this sense, is no longer something that is earned and verified: trust is routinely assumed towards anything that could be even remotely similar to the earlier forms of communication. This is the disintegration of verification as a vigorous mental operation, and the entrance of passive epistemology of interface routine as the substitute of scrutiny by understanding. Not the content is trusted so much as the pattern of the signal, a hazardous slippage in an environment full of mimicks.

> *"Even when I get messages about my bank account from unknown numbers, I sometimes believe them because I just expect banking info to come via my phone anyway." (Participant 4)*

This is an alarming might conflation of device and institutional level legitimacy. The mobile device assigned to the student becomes a convergent node, i.e., a place where all formal interactions (i.e., the communication with the institutions) are received, as well as all informal ones (social interactions). In this way, the phone turns into a representative seat of legitimacy: it is delivered through the phone, it gains presumable legitimacy. This would qualify as a textbook exercise in what cybersecurity scholars would refer to as contextual trust leakage (Kirlappos et al., 2012) through which the context in which users placed their trust (the banking app) has led to them extending the concept of trust applied to a specific domain (trusting the banking app) to other domains (SMS, WhatsApp) simply because of the fact that they operate within the same platform. The consequence of this is what has been denoted as an epistemic flattening by which the channel validates the message itself, authentication of the sender aside. With this state, it is the platform that will be made a guarantor, even in cases that the platform does not provide verification mechanism.

> *"My friends and I even share screenshots of our bank transfers in the group chat when we reimburse each other. It's just normal." (Participant 10)*

In this case, financial information is not only operative but also social performative. Photo-sharing of what people describe as a presumably intimate and sensitive act, i.e. banking screenshots, is also normalized by their peers and forms transactional transparency. However this normalization is very serious. First, it indicates the social spread of security norms: where the limits of privacy are lowered with trusted groups, users can apply the lowered norms to other situations, such as situations put on by the attackers. Second, it creates an avenue to peer imitation in phishing tactics. Each hacker who hacks into social areas or impersonates known senders can under the weight of the topicality of sharing screenshots solicit counterparts to help make the same types of disclosures. The micro-behavior of sharing is therefore a micro-habit that the student demonstrates whose scale can be utilized as a behavioral template. Financial information, which used to be strictly contained in institutional interfaces, has become social content Maurer -- redrawing the line of vulnerability.

Phishing Tactics Leveraging Social Communication Channels

The results of the interviews also revealed a compelling fact that phishing actors use social communication platforms deliberately to create an impression of sincerity, urgency and closeness. Participants have received phishing messages over and over again not in formal banking applications, but informal and socially saturated: WhatsApp, SMS, and once or twice via email where the communication style was close to real daily communication with peers or an institution. Being peripheral to the formal banking infrastructure, these platforms became the main channels of manipulation of the trust based on the fact that they are integrated into social life and their semiotic landscapes are of a hybrid nature.

> *"Most of the phishing messages I got were through WhatsApp. They looked like regular messages from a customer service number, with a bank logo as the profile picture." (Participant 1)*

This quotation represents the use of visual symbolics, as well as the choice of the platform structure and design, as utilized by those conducting an attack to create an illusion of the real, of actually existing. Adoption of a profile image that imitates a bank logo portrays the recognition of the cognitive mindset of users associating visual branding with legitimacy institutions. These visual markers take on an epistemic load in WhatsApp where avatars and simple display names can be used instead of official identification; they can make impossible attributions. This is true to what Zuboff (2019) would term as symbolic capture, whereby, attackers may not imitate the actual institution, but the mental model of what legitimacy should be according to the user. Since, in informal communication, WhatsApp does not structurally distinguish between business accounts, interface merges formal and informal into one communicational space, and is subject to misrecognition.

> *"They told me there was a system upgrade and sent a link via SMS. I didn't even think much because banks usually send updates through texts too." (Participant 3)*

This quotation unveils one of the main strategies to use the continuity of the channel norms. Banks traditionally send OTPs and transaction notification via SMS. Phishers, being aware of the institutional history of this channel incorporate themselves within the residue of credibility. This reaction of the student, which involves action without thinking will give a clear illustration of how we apply cognitive shortcutting (heuristic) when we receive a familiar message through a familiar route. Behavioral script: This is triggered by the form (it is an instructional, terse SMS message) and is compliance. This exploit appeals to what was referred to by Hutchby (2001) as technological affordances, whereby SMS enables concise and urgent communication, and as such, becomes perfect to engage in socially engineered societies which are deceptive in nature.

> *"I got an email that looked like it was from BRI. The language was formal, and the link address even had 'bri' in it, so I thought it was real." (Participant 9)*

The experience of this participant depicts a linguistically more advanced phishing attack, the one that combines formality with semantic mimicry. Such portrayed legitimacy is not only visual, but discursive; the use of formal language, plausible syntax, and domain names that do their best to look like legitimate URLs. What we observe here is an attacker who works in the conditions of a post-authenticity economy, where superficial cues (such as an existence of bri in the link) suffice to cause perceived institutional affiliation. The student does not use verification procedures, but rather rough similarity as an evidence of judgement, which is commonly known as trust-by-similarity and was described by sociotechnical researchers. It is in that context that language is weaponized in order not to communicate but to pretend to be credible.

> *"The message said my ATM card would be blocked if I didn't update my data. It sounded urgent, and it came through WhatsApp, so I reacted quickly without checking anything." (Participant 6)*

This statement refers to the emotional framework of phishing. The medium (WhatsApp) already carries the connotation of interpersonal immediacy and, with content that induces a cause of fear (results in blocked account), generates what Ahmed (2004) describes as an affective economy, the movements of feelings around, adhering to signs (e.g. the word blocked) in the manner that modulates behavior. The response of the student is not at all cognitive; it is affected-reflexive. The speed of the social messaging services used by the attacker conditions to respond quickly and habitually rather than carefully and slowly. This is because WhatsApp as a social space of urgencies and responsiveness to each other is the ideal vehicle of carrying interpersonal deceptions in the form of urgency.

> *"I actually got the phishing message forwarded from a friend. He said he got it from a campus group chat. That made me trust it more, because I thought it was shared info." (Participant 8)*

It is here that one can detect perhaps the most devious source of deception: peer-to-peer spreading of phishing. As the deception is recirculated as a part of social trust networks, the deception is given a relational license. What the student believed in was not the content of that message, but the social direction of the message. It is a classic case of relational trust displacement: a situation in which epistemic trusted is shifted between conduit and source. Such recirculation systems are also present in social commerce and digital peer networks, where they are similar to the electronic word-of-mouth (eWOM) activity in products marketing except that in this case they are used as a fraud. The implication is that platform design and group dynamics enable not only communication, but the viral reproduction of deception.

Psychological Manipulation and Impulsive Behavior

Although certain participants were found to exhibit knowledge of the phishing methods on the abstract level, their feedback showed that they still lacked the way to transfer this information into real-time usage. This disjuncture between thought and behavior has much to do with the manner in which phishing agents design cognitive and time pressures, panic, urgency, fatigue, authority badges, and simulated legality to by-pass thinking and trigger heuristic-based impulsive judgment. What is defined as the vulnerable in this sense is not intellectual ignorance but psychological imbalance in the focus of attention and perception in emotionally heightened times.

> *"I got a call saying my account was being accessed from another city and that I had to secure it immediately. I panicked and gave the OTP code without thinking." (Participant 3)*

This quotation is an example of a classic phishing operation an appeal to apprehension and urgency in place of weighing. The attacker does not merely ask information; he/she now creates a threat scenario, which is bound to create a compliance through induction of panic. This would be theoretically applied using dual-process decision-making (Diederich & Trueblood, 2018), which indicates that, under stressful conditions, users switch towards the instinctive (System 1) processing rather than reflective (System 2) processing. Students are made to believe that their OTP should never be leaked yet here they surrender not due to ignorance but rather due to the confusion about the time and feelings. In this case, the an attacker does not outsmart the user, but he outruns his logical mind.

> *"It was late at night and I was already tired when I saw the message. I just wanted to get it over with, so I clicked the link and entered my info without really reading." (Participant 6)*

This quote indexes what can be called in the fatigue window phishing or a tactic in which an attacker exploits the impaired mental condition of the user, e.g. exhaustion or sleepiness outside regular office hours. Decision fatigue, looking at it behaviorally, diminishes the capacity of the user to resist coercive signaling being tired to uphold anomalous scrutiny. The fact that the student fails to elaborate on the idea but just wants to get it over with represents a task compliance heuristic, in which the major aim of compliance is closure as opposed to protection. The result of this state is exacerbated by the design of messaging platforms that proposal calls to action as activity that is effortless, reducing the financial (both psychologically and procedurally) of compliance.

> *"They spoke very formally and said they were from the fraud detection unit. I didn't want to argue, so I just followed the instructions." (Participant 7)*

Another level of manipulation identified in the response of the participant can be characterized as simulated authority and deference scripting. By using more formal language and taking on an institutional tone phishers trigger compliance heuristic regarding social standing and institutional authority. It agrees with the traditional social psychology literature, as in the case of Milgram obedience to authority, where people have a higher likelihood to follow the orders when there is a sense of authority suggesting that this is their official capacity. The remark of the student-- I had no wish to quarrel-- denotes nothing whatever like confusion but unwillingly submission, motive of an all-but where unpleasantness in social intercourse is equalized above all to devisement. This exposes the fact that phishing is also used to take advantage of the rules of interpersonal conflict avoidance which is especially important in cultures with deeply ingrained respect to authority.

> *"I actually knew about phishing, and I've warned others before. But when it happened to me, it was so convincing, and I was in a rush. I only realized afterward." (Participant 2)*

This quote shows the contradiction of awareness and lack of opposition. The participant has experience with phishing (she expresses her own responsibility as an educator of her peer), but succumbs to the situation. This implies that awareness is a stored mental process and not an aroused defense system, unless specified ecological as well as emotional pre-conditions are not prescribed. Reasoning was not lost to the student but put on hold by time pressure and plausibility. It speaks of the vulnerability of informationally-based campaigns that aim to build an awareness instead of shaping a basis of practicable reflexes and corporality of distrust within the real world setting.

> *"They asked me to confirm some data to avoid my account being locked. I didn't want to lose access, so I just went along. Only later I realized it was too easy to believe." (Participant 11)*

In this case, the student loses because of loss aversion a behavioral bias which has been well studied; humans are more driven by a desperate avoidance of an imagined loss than by the need to gain equivalence (Sokol-Hessner & Rutledge, 2019). Pre-emptive compliance is caused by the fear of account deactivation: students do something not because they believe the message, but because they do not want to pay the price of disobeying. The words I just went along highlights the passive nature of the decision making process which presented a natural response to action that followed the threat. The manipulation is here by-affectively a weak one but by strategy capable of a great deal: it shoves aside the note of rational doubt and substitutes the logic of safety first-better safe than sorry, however strenuous the provocation.

Phishing, then, is actually an actor-centered performance across these stories that has a unique balance of time and emotion, as much as an action that aims at inducing rules of engagement through disorientation, inducing compliance. Phishers know that information is not their main target rather it is attention in impaired circumstances. The vulnerabilities in question are the result of students being sensitized to institutional security logic and the failure in that logic to correspond to the human-level pace, fatigue, trust, and pressure conditions.

Irregular Awareness and Security Unresponsiveness

As all of the participants received increased exposure to the cybersecurity discourse and awareness campaigns, concerning the researcher, a dissonance between what they said and how they acted emerged. With this theme, it proves one crucial point, which is awareness, without behavioral discipline and context reflexivity does not amount to resilience. In many cases, students could discuss phishing mechanisms at the abstract level but lacked the ability to apply this information to real-life time-sensitive situations, especially when affected by emotional, social, or procedural interference and unable to think critically. Further, the research observed inconsistent practices of protective measures, like utilization of secure networks, implementation of two-factor authentication (2FA), or confirming of suspicious messages, which were carried out either occasionally or not at all because of the overconfidence or fatalism opinions.

> *"Yes, I know that banks never ask for OTPs, but in the moment I forgot. It was just a blur, and I gave it out before I could even think." (Participant 2)*

Such confession demonstrates the weakness of the declarative awareness, namely, the possibility to repeat a security principle and be incapable of applying this principle in a case of pressure. The subject obviously has the right knowledge, yet they do not lie attached to action due to the influence of contextual stress. The kind of awareness that is possessed in this case is not a reflexive action or practice. Behaviorally, this implicates cripplement of what Lejarraga & Pindard-Lejarraga (2020) terms as ecological rationality; that is, the capacity to make adaptive judgment in the real world situations. When engulfed with the phishing deception under the affective haze, the rule against sharing OTP becomes mechanically displaced cognitively to the context in which the rule itself should apply. This state of cognitive disjunction is what phishing malevolent users use towards their advantage and make abstract consciousness rather inactive.

> *"Sometimes I remember to check the sender's number or link, but not always. When I'm busy or distracted, I just trust it looks official enough." (Participant 4)*

This citation speaks about the situational plasticity of caution. The participant is not consistent in the instantiation of the verification behaviors but they are contingent upon cognitive availability and emotional bandwidth. An expression of a hazardous dependence upon apparent verisimilitude, in lieu of authentication, is conveyed in the phrase, we are just to trust, that it looks official enough. On platforms where visual design is readily copied and where users are encouraged by socialization to care less about aesthetic quality and to value speed and convenience above all, superficial cues (logos, tone, formatting) are usually over-emphasized in user perception. This dependence on aesthetic recognition, instead of technical certificate, leads the way to attackers exploring visual analogues as weapons. Again in this case the knowledge exists but is inconsistently applied through the filters of urgency in tasks and attention loads.

> *"I know 2FA is important, but I haven't activated it. It just seems like a hassle, and I don't think I'll be targeted anyway." (Participant 8)*

In this statement, we find what is known as a fatalistic optimism bias, i.e., the tendency to determine that people are susceptible to security cyber threats but that it cannot be one. Although the participant acknowledges the importance of two-factor authentication (2FA), he or she willfully avoids its application with the view of inconvenience and misjudgment of the level of his or her personal risk. It reflects cognitive asymmetry of perceived threat versus preventive action, with the benefit of security pre-commitment (penalty in friction) being more saliently perceived than the fantasy of the benefit of the committed security against the threat. It is also symptomatic of a larger trend in the digital risk culture in moving responsibility of security out of user hands as the premise of platform or provider security is high enough. This learned helplessness stance, which finds justification in the comfort factor, results in such important security functionalities being under-utilised even by otherwise knowledgeable users.

> *"I always tell my friends to be careful with strange messages, but sometimes I reply to them just out of curiosity. It doesn't feel serious until something happens." (Participant 6)*

The given quote reflects the fact that cybersecurity discourse and popular digital practice is separated by a cultural divide. The respondent plays the dual role of exhorting safety to the world, and acting recklessly behind the scenes. This would imply that cybersecurity among numerous users is yet to be discursively performative as opposed to being internalized. The statement that it feels not serious is an indication of absence of emotional gravity of potential danger. Phishing is a hypothetical risk until the damage is experienced per se. This pre images the notion introduced by Shiv et al. (2005) on the deferred affect wherein investment of emotions is merely attributed retroactively following loss. In these situations, the users are aware of what they are not supposed to do, yet the economy of their emotional online world does not reward them in taking preventive precautions.

> *"I've gotten so many warnings from my bank about phishing that I've started ignoring them. They just seem like spam now." (Participant 1)*

Paradoxically, the excessive awareness propaganda can be a source of desensitization, or rather the mental exhaustion to security propaganda. When warnings are repetitive and debilitated, they are not salient-particularly when they are not supported with precise and implementable actions or specifically aligned to the user contexts. The presence of this attitude is an indication of security fatigue that cybersecurity psychologists refer to as the tendency to avoid protective behavior under pressure of information overwhelm, repetition, or improper messaging (National Institute of Standards and Technology 2016). The threat is not denied by the participant but he/she gets desensitized to its expression which further leaves the scene open to effective deception. What this demonstrates is that the issue is not the absence of messaging, but its inability to be put in a context that matters to the users of their everyday digital world.

Social Mediation of Finance Vulnerability in Platform Ecosystems

The susceptibility of students to phishing attacks is caused by the epistemic dynamics of the social messaging platforms like WhatsApp and SMS, in which channel familiarity is used as a proxy about message verification. New research - Wang et al. (2009) - indicates that users that exhibit habitual messaging behavior use visual identifiers such as profile names and logos as statistics on performance of trust. Shalaby (2024) go one step further to demonstrate that chronic exposure to branded alerts within chat apps weakens the cognitive vigilance of users. On a similar note, Scissors et al. (2008) conclude that interface mimicry in messaging situations does reduce analysis scrutiny. When the respondents in this research referred to making trust possible simply because of receiving a banking message through WhatsApp, it was the exact cognitive shortcut that was observed in such studies (Miller, 2022). According to Unger et al. (2015), heuristic processing in messaging applications is provoked where the delivery channel is the condition of guaranteed security. These findings converge, and this is why we may discuss the way our participants did not pay attention to questioning suspicious messages but used patterns instead. These dynamics give credence to the fact that phishing takes the advantage of social trust mediated by platform arrangements, rather than ignorance or lack of knowledge.

The other fundamental revelation is in the aspect of contextual trust leakage. The article by Yousafzai et al. (2023) describes how the trust placed in a single sphere of the digital world is transferred to the other as a result of people thinking that banking warnings sent out on the trusted sites should be real. According to Harvey et al. (2024), evidence has been supplied that notifications via WhatsApp to financial institutions invoke compliance unverified. During our interviews, one of the students reported how ceding messages occurred due to assumptions that any bank alert sent through SMS or messengers was possible. Such phenomenon is called by Chemerinsky (2021) a failure of layered scrutiny caused by the accustomed credence to the medium. Lai et al. (2022) demonstrate that users bypass authentication protocols in most cases due to a strategy of using channels as legitimate sources. Through these, the effect that we find in our data reflects the psychological trend contained in such a study and demonstrates how platform loyalty develops deceptive susceptibility.

It is common to find screenshots or payment confirmations on groups where people of good faith with similar-minded people formed into a community. Jia et al. (2024) explain that in social commerce scenarios, peer endorsement increases the legitimacy between members of the groups. As mentioned by Stockinger (2011), forwarding a message implies the implicit authentication. In our research, students described examples when phishing messages sent by friends or group administrators on the campus seemed to be trustworthy only because of the social proximity of the sender. On the larger scale, Teng et al. (2017) discuss the role of eWOM dynamics in peer networks in the process of persuasion. It is not by coincidence that hackers are using this norm to their advantage by inserting phishing in group channels thus taking advantage of implicit trust. This trend is consistent with the results of London et al. (2022) which indicate that peer-to-peer deception seems plausible due to the fact that the users do not doubt messages sent by people with whom they have established contact. The effect is that it is not isolated vulnerability that is socially distributed.

The line between the area of social chat and financial interaction is nowadays becoming thin because of digital platforms. Wepener et al. (2021) demonstrate that contemporary messaging applications support transactional messaging content in informal chat styles. The study by Huang & Wang (2023) explains that phishers can simulate the conversational tone and narrative structure similar to the message claims of social commerce. Ingram Bogusz et al. (2019) point out that whether users perceive platform legitimacy is highly dependent on aesthetics and user interface prompts. Our statistics confirm that phishing emails usually take the common messaging patterns that people use with each other instead of being formal bank messages. According to Saberi Pirouz (2013), phishing training based on emails does not equip the users with skills to protect themselves against deceit built-in through social messaging medium. Prospected by Bhaskaran (2024), the considerations of interface dynamics are crucial to the perception of user trust in the awareness efforts. These observations place phishing not as a vulnerability in technology but in a semantic exploitation in hybrid social commercial sites.

Intervention is more effective when HMI mimics those of the messaging platfoms with vernacular and affordances. Kavitha et al. (2024) simulated alerts reminiscent of WhatsApp and showed a huge jump in the detection accuracy. Those findings are confirmed by Lim et al. (1996) who emphasize that interface familiarity training develops contextual recognition. Thomas et al. (2024) extended it and added group-based roleplay on a messaging format, making it more convincing and less likely to be clicked-through. Jeon (2020) define the term situational fluency to refer to the capacity to disintegrate deceptive patterns in life-like message environments. This argument is put forward by Lentenbrink (2018), according to whom training activities need to develop a reflexive awareness that is built within real-life communication settings and not idealized or desexualized ones. Our participants stated that they saw general cybersecurity tips as out of touch with real-life experiences of messages and did not help them be ready to be deceived through common social interfaces. These observations confirm that proper prevention requires platform level literacy with respect to the real threat environment and not a concept.

The importance of platform-mediated phishing to industry structure is also confirmed by quantitative data released in the recent industry reports. On the one hand, the analysis depicted by the 2025 Verizon Data Breach investigations report clearly shows that there are more than ninety percent major social engineering attacks on financial industries, and all those are associated with WhatsApp or SMS vectors. As the Meta Phish Study (2024) notes, phishing through a messaging application does not fall under standard email graphics. According to CyberSec Intelligence (2023), there is a growing number of socially delivered fraud financial losses. According to Alwanain (2020) and Gyaisey Research (2023), Gen Z users under the age of 25 and belong to the category of unavoidable social message users are more vulnerable to scams than their older generations are. KPMG Gen Z Fraud Report (2024) displays that the more reliant people are on messaging, the less skeptical they are. This kind of demographic and behavioural overlap with our study cohort affirms that the aspect of vulnerability comes about due to systematic interaction between user behaviour and platform structures. The statistics highlight the risk as being social, rather than errant as individuals.

The vulnerability of Preconsciousness and the boundaries of the behavioral rationality of the digital security

This gap between phishing awareness and successive inability to stand up to fraudulent prompts indicates that even though awareness can lastingly protect people online, it is not doing it the case of phishing. Research conducted by Butavicius et al. (2022) defines a phenomenon when under stress, people do not switch on protective action even in the situation of phishing tactics verbal recognition. The results obtained by Price & Norman (2008) show that in an emotionally stimulating environment (fear, urgency), people switch to intuitive thinking, not to conscious reasoning. Participants in our information clearly stated the right principles like never sharing OTP but gave in to pressure and gave up such sensitive information, the exact breakdown of the dual process outlined in that kind of research. Sephton (2013) also record that such formal knowledge is usually dormant until the time it is internalized into an embodied practice. What it explains is that behavioral vulnerability does not take place as a result of ignorance but because of heuristic overrode in situational overload.

The theory of loss aversion offers an insight on how threat framing hinders rational security behavior. Parker (2006) have found that the messages that threaten users with account suspension or the loss of earnings make users comply pre emptively compared to the incentives that are gain framed and urge behavior diligence. Hamm et al. (2003) demonstrate that even in the case of suspicions, users react faster on the loss scenarios. Respondents said that they often respond quickly to the messages stating data leakage or blocking accounts. This is in line with the results of Van Prooijen (2017) showing that emotional reflexes are enhanced by the urgency signals. In such an environment there is a breakdown of the rational calculus and users obey lest they are to face punishment, not because of the efforts to be authentic. These dynamics reflect the fact that phishing is sometimes effective by using emotions instead of using rationality to scam.

Cognitive fatigue heavily decrease vigilance and goes below par in decision making in phishing activities. Kavvadias & Kotsilieris (2025) demonstrate that mentality borsch or lowest housing hours are related to high rates of clicks on the phishing button. The main idea addressed by Eyal (2019) is that the user attention is a limited resource, which can become depleted. Responding to our interviews students said that end of the day or late night tiredness lower their capacity to scrutinize messages. This aligns with the idea put in Alkhalil (2021), who speak of the phishing fatigue window, at the end of which users prove vulnerable to rapid solution rather than thorough scrutiny. This proves that susceptibility is partly dependent on temporal and affective conditions, and therefore, prevention should consider tempo of a human being rather than rationally educating people only.

There was deferred skepticism in the circumstances that involved broadcast of warnings and denigration of threats by the participants simultaneously. Kuraku (2022) record the occurrence of what they call the problem of discourse-performative caution: people advise the interlocutor not to succumb to phishing but engage in trivial activities on their part via the curiosity effect of being too curious. According to Wolburg (2006), affective inertia lags precaution until harm is realized. It was noted in our data that students tended to disregard odd messages as harmless until the repercussions showed. This is a representation of deferred affect by Ganguly et al. (2017) to digital risk culture. The effect is that cybersecurity then develops into a theatrical language instead of being an existent habit, until catastrophe alters behaviour. The main obstacle to awareness to action is security fatigue. The study by Mirilla (2018) demonstrates that disengagement is in place where security pronouncements are repeated without contextual actionability. Kass (1991) note that a repeated exposure to the same advisories also makes a user more likely to ignore it. Our interviewees reported having been desensitized to the high frequency of alerting e-mails sent by the bank with regard to phishing. This is similar to Stewart & Martin (1994) who proved general rejection of generic warnings. When these messages are turned into perfunctory messages, vigilance fails. The psychological cost of constant vigilance of caution prompts a resignation rather than precaution indicating that awareness messaging deprived of any experiential context can have a weakening effect on resilience.

Successful training should not only instill an informational knowledge, but a good one should be dealt with that produces reflexive habits as well. According to Delhomme et al. (2009), the success of interventions lies in their duplication of real messaging environments and putting the users in the conditions of emotional-realistic environment. As depicted by Damon (1984), integration of peer role play in group training leads to preservation and doubt. According to Islind et al. (2020), when the subject undergoes platform-context training, he/she becomes more resistant when pressed with urgency. The concept of situational fluency elaborated by Saarni (2001) needs an experience of repetition in the context of message delivery to develop emotional reflexes in the cognitive domain. Our findings support these directions. Participants said abstract advice lacked resonance during deceptive events. Cohesively this analysis insists that phishing prevention must evolve beyond awareness as doctrine to awareness as culturally and contextually embodied response.

Architecture of Digital Vulnerability

This research study was not merely aimed at finding out how university students can be victims of phishing attacks but to question the underlying social and behavioral frameworks that cause such vulnerability to be in the first place. The results have clearly indicated that phishing is not a technological foggy-ness nor it involves inadequate vigilance on the part of individuals. Rather, it is imbedded in the everyday logics of digital life in which one does not gain trust by passing through institutional rigor but rather by a social familiarity and regular engagement with interfaces and communicative immediacy. Phishing does not constitute breaking in the pathway of platform behavior but rather the symptom of the way platforms themselves negotiate credibility in their own relations.

What came out of the accounts of the participants is not only an image of misjudgment but a topology of trust informed by platform infrastructures. The inability to distinguish deception cannot be equaled to ignorance. It could better be defined as a logical reaction in an illogical design. As students execute acts based on messages sent via trusted messaging platforms, they are not failing to observe security precinct but obeying the epistemic grammar that is taught by the platform. They are reacting according to the affordances, cues and relationship norms that are naturalized within their digital practices.

The current research makes the case that digital vulnerability is a systemic result rather than an aberration that has to be adjusted. The attempt at solving the problem which does not consider the structural way of how deception is embedded in channels familiar to us will be superficial. It is not only a lack of information but an excess of familiarity that is the problem. It is not a want of ratiocinative power, but a surfeit of relation habit. Security awareness programs which consider users as independent cognitive subjects fail to acknowledge the social and embedded character of deception. Similarly, designing superficial friction as a means of engineers trust by platform designers denies larger cultural economy within the contests of trust is staged and evicted. The change, in this case, must be conceptual and practical. We have to stop thinking of users as the weakest point in a security chain and start seeing that they are local actors in adversarial but mundane contexts whose imperative conflicts with other such imperatives. Platform responsibility cannot be considered an optional add-on: it must be viewed as a critical design ethic. Awareness is not a transfer of information, but it has to be seen as a transformation of practice. But, most importantly, we have to acknowledge that any attempt at securing the users cannot succeed unless it addresses the systems that have conditioned users to act so unnaturally with respect to security.

This paper does not purport to come up with the ultimate answers. Nevertheless, it states confidently that our future is not teaching people not to fall victims to a lure but creating a space in which trust is not equivalent to green light on malicious intent. Whoever knows how to live, socialize, and normalize vulnerability will have the future of digital security in their hands, not those better able to write more effective defenses. On the one hand, therefore, to study phishing is not to study error. It is to examine the daily structures of the belief. And it is to inquire how it is possible to re-make those infrastructures.

Conclusion

The researched paper has demonstrated that the circumstances in which digital financial users become the victims of phishing are not accidental or can be reduced to ignorance. Rather they are developed in a system of routine, platform facilitated communication that habitualizes trust, mechanizes reaction, and disguises risk under the guise of ease. The problem of phishing is not an exception in the realm of digital money. It is a structural opportunity that is plausible as a result of the environments installed to promote access efficiency and instantaneity. What is visible through the findings of this study is a morbid choreography where vulnerability takes place not at digital life margins but at its core and is instantiated by repetitions of trusts people get to know through daily platform usage. This study of students described their accounts of deceit, reluctance, and eventual submission to show that the failure of cybersecurity is not cognitive but cultural. Phishing is not effective because users fall victims due to lack of information. These are designers that fall victims because the platform architecture instructs them on how to be confident in what appears familiar, do things too fast under the name of functionality, and to trust security to security interfaces, instead of institutions. In this kind of environment, even people with a lot of information are easily susceptible not despite their literacy, but because speed, responsiveness, and social conformity become heavier than reasoning. The point of this is not that people do not think, but that the environment itself has trained them to think in non-thinkable ways.

The meaning of this is that it is no longer sufficient to use the traditional methods of digital security in terms of education, technical obstacles, or the fault of a user. The solution should start with a change of ideas: to see vulnerability not as an issue that lies with the user but as a result of the systems that envelop them. This means recognizing trust as infrastructural, not optional. It means designing messaging environments that do not reward automation of belief. It means moving beyond awareness campaigns that treat users as information processors and toward pedagogies of attention, habit, and relational caution. And it demands that platforms take responsibility not simply for delivering content securely but for shaping the interpretive frameworks through which users assess legitimacy.

References

Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). Phishing happens beyond technology: The effects of human behaviors and demographics on each step of a phishing process. *IEEE Access*, *9*, 44928-44949. http://dx.doi.org/10.1109/ACCESS.2021.3066383

Agusthin, I. D., Nada, D. C., & Putri, N. A. (2024). Legal Protection of Customers from Phishing Crimes in Digital Banking Services in Indonesia. *Deposition: Journal of Legal Science Publications*, *2*(4), 132-148. https://doi.org/10.59581/deposisi.v2i4.4214

Ahmed, S. (2004). Affective economies. *Social text*, *22*(2), 117-139. http://dx.doi.org/10.1215/01642472-22-2_79-117

Akeiber, H. J. (2025). The Evolution of Social Engineering Attacks: A Cybersecurity Engineering Perspective. *Al-Rafidain Journal of Engineering Sciences*, 294-316. https://doi.org/10.61268/r9c49865

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

Alwanain, M. I. (2020). Phishing awareness and elderly users in social media. *International Journal of Computer Science and Network Security*, *20*(9), 114-119.

Anindyaa, T. D., Sasmitaa, G. M. A., & Pratama, I. P. A. E. (2024). Edukasi Bahaya Social Engineering Menggunakan Media Belajar Quizizz Untuk Meningkatkan Kesadaran Keamanan Informasi Nasabah Perbankan. *Jitter: Jurnal Ilmiah Teknologi Dan Komputer*, *4*(3), 2056.

Arif, M. N. R. Al. (2010). *Basics of Islamic Bank Marketing*. Alfabeta.

Batubara, M. C. A., & Anggraini, T. (2022). Analisis pengaruh layanan digital terhadap minat generasi Z dalam menggunakan produk perbankan syariah. *Jurnal Masharif Al-Syariah: Jurnal Ekonomi Dan Perbankan Syariah*, *7*(2), 706-725.

Bhaskaran, V. (2024). Designing for Trust: The Crucial Role in Digital User Experiences. *Journal of User Experience*, *19*(2), 53-59.

Butavicius, M., Taib, R., & Han, S. J. (2022). Why people keep falling for phishing scams: The effects of time pressure and deception cues on the detection of phishing emails. *Computers & Security*, *123*, 102937. http://dx.doi.org/10.1016/j.cose.2022.102937

Chemerinsky, A. (2021). Tears of Scrutiny. *Tulsa L. Rev.*, *57*, 341.

Chou, F. K. Y., Chen, A. P. S., & Lo, V. C. L. (2021). Mindless response or mindful interpretation: examining the effect of message influence on phishing susceptibility. *Sustainability*, *13*(4), 1651. https://doi.org/10.3390/su13041651

CyberTalk. (2022). *Phishing Prevention Ebook: What To Know About Upgrading Your Strategy*. Cybertalk.Org.

Damon, W. (1984). Peer education: The untapped potential. *Journal of applied developmental psychology*, *5*(4), 331-343. https://psycnet.apa.org/doi/10.1016/0193-3973(84)90006-6

Darics, E. (2012). *Instant messaging in work-based virtual teams: the analysis of non-verbal communication used for the contextualisation of transactional and relational communicative goals* (Doctoral dissertation, Loughborough University).

Delhomme, P., De Dobbeleer, W., Forward, S., & Simões, A. (2009). Manual for designing, implementing, and evaluating road safety communication campaigns: Part I. *Brussels: Belgian Road Safety Institute*.

Diederich, A., & Trueblood, J. S. (2018). A dynamic dual process model of risky decision making. *Psychological review*, *125*(2), 270. https://psycnet.apa.org/doi/10.1037/rev0000087

Eyal, N. (2019). *Indistractable: How to control your attention and choose your life*. BenBella Books.

Financial Services Authority Regulation Number 12/POJK.03/2021 of 2021 concerning Commercial Banks, peraturan.bpk.go.id (2021).

Ganguly, S., Harreis, H., Margolis, B., & Rowshankish, K. (2017). Digital risk: Transforming risk management for the 2020 s. *McKinsey & Company*.

Gyaisey, A. P. (2023). *The Effect of Mobile Payment Technology Fraud Perception on Customer Intention to Continously Use the Service: A Study Moderated by Generation X, Y, and Z from a Developing Economy* (Doctoral dissertation, University of Ghana).

Hamm, A. O., Schupp, H. T., & Weike, A. I. (2003). Motivational organization of emotions: Autonomic changes, cortical responses, and reflex modulation. *Handbook of affective sciences*, 187-211.

Harvey, R. H., Leotta, M. J., & Sachdev, G. (2024). Why depository institutions, with or without affiliated securities firms, can and should manage employee use of personal devices for work-related communications. *Journal of Financial Compliance*, *8*(2), 154-166.

Hollebeek, T., & Waltzman, R. (2004, September). The role of suspicion in model-based intrusion detection. In *Proceedings of the 2004 workshop on New security paradigms* (pp. 87-94). https://doi.org/10.1145/1065907.1066041

Huang, Y., & Wang, W. (2022). When a story contradicts: Correcting health misinformation on social media through different message formats and mechanisms. *Information, Communication & Society*, *25*(8), 1192-1209. https://psycnet.apa.org/doi/10.1080/1369118X.2020.1851390

Hutchby, I. (2001). Technologies, texts and affordances. *Sociology*, *35*(2), 441-456. http://dx.doi.org/10.1017/S0038038501000219

Ingram Bogusz, C., Teigland, R., & Vaast, E. (2019). Designed entrepreneurial legitimacy: the case of a Swedish crowdfunding platform. *European Journal of Information Systems*, *28*(3), 318-335. https://doi.org/10.1080/0960085X.2018.1534039

Islind, A. S., Norström, L., Vallo Hult, H., & Olsson, S. R. (2020). Socio-technical interplay in a two-sided market: the case of learning platforms. In *Digital Transformation and Human Behavior: Innovation for People and Organisations* (pp. 33-53). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-47539-0_4

Jeon, W. (2020). *Resonance, a step towards a fluency for complexity: The science, language, and epistemology of Gregory Bateson* (Master's thesis, The University of Western Ontario (Canada)).

Jia, Y., Liu, L., & Lowry, P. B. (2024). How do consumers make behavioural decisions on social commerce platforms? The interaction effect between behaviour visibility and social needs. *Information Systems Journal*, *34*(5), 1703-1736. http://dx.doi.org/10.1111/isj.12508

Kass, R. (1991). Building a user model implicitly from a cooperative advisory dialog. *User Modeling and User-Adapted Interaction*, *1*(3), 203-258. http://dx.doi.org/10.1023/A:1011145532042

Kavitha, P., Anand, A., Sreenivasan, S., Mohammed S, H., Borah, N., & Saikia, D. (2024). The development of early flood monitoring and a whatsapp-based alert system for timely disaster preparedness and response in vulnerable communities. *Engineering Proceedings*, *62*(1), 18. https://doi.org/10.3390/engproc2024062018

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. https://doi.org/10.3390/app15042236

Kirlappos, I., Sasse, M. A., & Harvey, N. (2012, June). Why trust seals don’t work: A study of user perceptions and behavior. In *International Conference on Trust and Trustworthy Computing* (pp. 308-324). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007%2F978-3-642-30921-2_18

Kuraku, S. (2022). *Curiosity Clicks: The Need for Security Awareness*. University of the Cumberlands.

Kurkovsky, S., & Syta, E. (2010, June). Digital natives and mobile phones: A survey of practices and attitudes about privacy and security. In *2010 IEEE International Symposium on Technology and Society* (pp. 441-449). IEEE. http://dx.doi.org/10.1109/ISTAS.2010.5514610

La Torre, A., & Angelini, M. (2025). Cyri: A Conversational AI-based Assistant for Supporting the Human User in Detecting and Responding to Phishing Attacks. *arXiv preprint arXiv:2502.05951*. http://dx.doi.org/10.48550/arXiv.2502.05951

Lai, C., Ma, Y., Lu, R., Zhang, Y., & Zheng, D. (2022). A novel authentication scheme supporting multiple user access for 5G and beyond. *IEEE Transactions on Dependable and Secure Computing*, *20*(4), 2970-2987. http://dx.doi.org/10.1109/TDSC.2022.3198723

Lejarraga, J., & Pindard-Lejarraga, M. (2020). Bounded rationality: Cognitive limitations or adaptation to the environment? The implications of ecological rationality for management learning. *Academy of Management Learning & Education*, *19*(3), 289-306. https://psycnet.apa.org/doi/10.5465/amle.2019.0189

Lentenbrink, J. W. (2018). *The Desexualization of Contemporary Psychoanalysis*. Pacifica Graduate Institute.

Lim, K. H., Benbasat, I., & Todd, P. A. (1996). An experimental investigation of the interactive effects of interface style, instructions, and task familiarity on user performance. *ACM Transactions on Computer-Human Interaction (TOCHI)*, *3*(1), 1-37. http://dx.doi.org/10.1145/226159.226160

London Jr, J., Li, S., & Sun, H. (2022). Seems legit: An investigation of the assessing and sharing of unverifiable messages on online social networks. *Information Systems Research*, *33*(3), 978-1001. http://dx.doi.org/10.1287/isre.2021.1095

Margie, L. A., Prihatni, R., & Gurendrawati, E. (2024). Determinants of Digital Banking Service Usage: A Systematic Literature Review. *Innovation: Scientific Journal of Management Science*, *11*(2), 604-614. https://doi.org/10.32493/Inovasi.v11i2.p604-614.45249

Maseko, A. E. (2023). *Remedies to reduce user susceptibility to phishing attacks* (Doctoral dissertation, University of the Western Cape).

Miller, J. R. (2022). *Financial inclusion through WhatsApp banking in Johannesburg* (Master's thesis, University of the Witwatersrand, Johannesburg (South Africa)).

Mirilla, D. F. (2018). *Slow incident response in cyber security: The impact of task disengagement in security operations centers*. Pace University.

Msallati, A. (2021). Investigating the nexus between the types of advertising messages and customer engagement: Do customer involvement and generations matter?. *Journal of Innovations in Digital Marketing*, *2*. http://dx.doi.org/10.51300/jidm-2020-31

Muda, N. R. S. (2024). Design and Build Plastic Waste Processing Robots in Indonesia to Support Sustainable Environmental Management. *International Journal of IJNRSM*, *4*(7), 200-210.

Muftiadi, A., Agustina, T. P. M., & Evi, M. (2022). *Studi kasus keamanan jaringan komputer: analisis ancaman phising terhadap layanan online banking. Hexatech: Jurnal Ilmiah Teknik, 1 (2), 60-65*.

Nur, F. (2023). Penegakan hukum terhadap kejahatan digital perbankan. *Innovative: Journal Of Social Science Research*, *3*(6), 3234-3249.

Okoli, J. (2021). Improving decision-making effectiveness in crisis situations: developing intuitive expertise at the workplace. *Development and Learning in Organizations: An International Journal*, *35*(4), 18-20. http://dx.doi.org/10.1108/DLO-08-2020-0169

Parker, C. (2006). The “compliance” trap: The moral message in responsive regulatory enforcement. *Law & Society Review*, *40*(3), 591-622. http://dx.doi.org/10.1111/j.1540-5893.2006.00274.x

Price, M. C., & Norman, E. (2008). Intuitive decisions on the fringes of consciousness: Are they conscious and does it matter?. *Judgment and Decision making*, *3*(1), 28-41. http://dx.doi.org/10.1017/S1930297500000140

Saarni, C. (2001). Cognition, context, and goals: Significant components in social-emotional effectiveness. *Social Development*, *10*(1). https://psycnet.apa.org/doi/10.1111/1467-9507.00152

Saberi Pirouz, A. (2013). *Securing email through online social networks* (Doctoral dissertation, Concordia University).

Scissors, L. E., Gill, A. J., & Gergle, D. (2008, November). Linguistic mimicry and trust in text-based CMC. In *Proceedings of the 2008 ACM conference on Computer supported cooperative work* (pp. 277-280). http://dx.doi.org/10.1145/1460563.1460608

Sephton, K. A. (2013). *Decision-making under information overload: Visual representation and 'fast and frugal'heuristics as strategies for dealing with information overload* (Doctoral dissertation, Stellenbosch: Stellenbosch University).

Shalaby, A. (2024). Classification for the digital and cognitive AI hazards: urgent call to establish automated safe standard for protecting young human minds. *Digital Economy and Sustainable Development*, *2*(1), 17. http://dx.doi.org/10.1007/s44265-024-00042-5

Shiv, B., Loewenstein, G., Bechara, A., Damasio, H., & Damasio, A. R. (2005). Investment behavior and the negative side of emotion. *Psychological science*, *16*(6), 435-439. https://doi.org/10.1111/j.0956-7976.2005.01553.x

Simatupang, S., Sinaga, O. S., Manurung, S., Ambarita, M. H., & Mokodongan, E. N. (2024). Digital Bank and Consumer Trust. *Satyagraha Scientific Journal*, *7*(2), 156-164. https://doi.org/10.47532/jis.v7i2.1090

Sokol -Hessner, P., & Rutledge, R. B. (2019). The psychological and neural basis of loss aversion. *Current Directions in Psychological Science*, *28*(1), 20-27. https://psycnet.apa.org/doi/10.1177/0963721418806510

Stewart, D. W., & Martin, I. M. (1994). Intended and unintended consequences of warning messages: A review and synthesis of empirical research. *Journal of Public Policy & Marketing*, *13*(1), 1-19. http://dx.doi.org/10.1177/074391569401300101

Stockinger, T. (2011). Implicit authentication on mobile devices. In *The Media Informatics Advanced Seminar on Ubiquitous Computing* (Vol. 8).

Tasri, E. S., Karimi, K., & Muslim, I. (2021). *Community Economic Vulnerability and Resilience to Environmental Damage*. Sukabina Press.

Teng, S., Khong, K. W., Chong, A. Y. L., & Lin, B. (2017). Persuasive electronic word-of-mouth messages in social media. *Journal of Computer Information Systems*, *57*(1), 76-88. http://dx.doi.org/10.1080/08874417.2016.1181501

Thomas, J. S., Chen, C., & Iacobucci, D. (2022). Email marketing as a tool for strategic persuasion. *Journal of Interactive Marketing*, *57*(3), 377-392. http://dx.doi.org/10.1177/10949968221095552

Unger, N., Dechand, S., Bonneau, J., Fahl, S., Perl, H., Goldberg, I., & Smith, M. (2015, May). SoK: secure messaging. In *2015 IEEE Symposium on Security and Privacy* (pp. 232-249). IEEE. https://doi.org/10.1109/SP.2015.22

Valiansyah, R., Matulessy, A., & Pratitis, N. (2023). Impulse Buying in College Students: What is the Role of Intepersonal Influence *Vulnerability*? *INNER: Journal of Psychological Research*, *2*(4), 539-549.

Van Prooijen, J. W. (2017). *The moral punishment instinct*. Oxford University Press.

Wang, J., Chen, R., Herath, T., & Rao, H. R. (2009). Visual e-mail authentication and identification services: An investigation of the effects on e-mail use. *Decision Support Systems*, *48*(1), 92-102. http://dx.doi.org/10.1016/j.dss.2009.06.012

Wepener, C., Johnson, E., & Bornman, J. (2021). Text messaging “Helps Me to Chat”: exploring the interactional aspects of text messaging using mobile phones for youth with complex communication needs. *Augmentative and Alternative Communication*, *37*(2), 75-86. http://dx.doi.org/10.1080/07434618.2021.1928284

Wolburg, J. M. (2006). College students’ responses to antismoking messages: Denial, defiance, and other boomerang effects. *Journal of Consumer Affairs*, *40*(2), 294-323. https://psycnet.apa.org/doi/10.1111/j.1745-6606.2006.00059.x

Yano, N., Ishii, T., & Irie, R. (1975). Modification of the Disk Assay Method for Detection of Antibiotics by Direct Seeding of Spores of Bacillus stearothermophilus. *Food Hygiene and Safety Science (Shokuhin Eiseigaku Zasshi)*, *16*(2), 105-109_1. https://doi.org/10.3358/shokueishi.16.105

Yousafzai, S. Y., Pallister, J. G., & Foxall, G. R. (2003). A proposed model of e-trust for electronic banking. *Technovation*, *23*(11), 847-860. http://dx.doi.org/10.5267/j.msl.2015.8.008

Zuboff, S. (2019, January). Surveillance capitalism and the challenge of collective action. In *New labor forum* (Vol. 28, No. 1, pp. 10-29). Sage CA: Los Angeles, CA: Sage Publications.