Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

Theorizing the Occurrence of Internet Fraud Victimisation: Based on Two Systems in Decision-Making and Reasoning

Adebukola Oluwatosin OHUNENI;[1] Taiwo Jesutofunmi ASHAOLU;[2] Adetayo Olaniyi ADENIRAN;[3] Chinasa Racheal UGWU;[4] Olayemi David BABATUNDE [5]

[1,2,3] University of Ilesa, Nigeria
[4]Emboyi State University;
[5]Federal University of Agriculture, Abeokuta
[1] bukola_ohuneni@gmail.com; https://orcid.org/0009-0002-6842-1728
[2] ashaolujesutofunmi9@gmail.com; https://orcid.org/0009-0005-8507-3958
[3] adetayo_adeniran@unilesa.edu.ng; https://orcid.org/0000-0002-6870-1212
[4]chinasaogbonnia@gmail.com; https://orcid.org/0009-0009-1540-4079;
[5] babatundeolayemi28@gmail.com; https://orcid.org/0009-0004-9333-6044

Correspondence: Chinasa Racheal UGWU

Abstract

Studies have been carried out on the influencing factors of internet fraud which can be categorized under psychology, experience, susceptibility information, and demography. Although there is not much study on the psychological underpinnings of online fraud victimisation, what is known offers a fresh angle on the subject. This study relied on theories and the empirical reviews surrounding those theories. It was discovered that earlier studies consistently held the opinion that the systematic processing mode was useful in identifying and detecting fraud and that the heuristic processing mode was associated with vulnerability to online fraud. This summary was not disproved based on the overall findings, but more work has to be done to validate and explain the relationships between this inherent causes. Furthermore, there is disagreement about whether psychological traits like personality have a mediating role in the risk of online fraud when it comes to the heuristic-systematic model (HSM), with the attribute of suspicion being the exception. It has been discovered that objective knowledge and experience in particular domains might lead to this path. More information is needed to understand how habits and equipment influence network victimisation through the heuristic processing system,

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

even if this information is starting to surface. Lastly, the heuristic-systematic model's defensive tactics include deliberate analysis like simulated scene training and content-based cue recognition technologies.

Keywords: ***Internet Fraud Victims; Heuristic-Systematic Model; Defence Strategies***

1. Introduction

Communication is key in any society (Akinloye 2025). Also, fraud is not a new aberrant occurrence; it has occurred since the beginning of human history and is otherwise classified as a criminal offence. Communication and fraud are two distinct activities that are connected to each other. The definition and repercussions of fraudulent acts on victims have remained constant (Smith, 2007), with the exception that the expansion of the Internet has allowed for the growth of online fraud capabilities (Falola & Heaton, 2008; Ilugbami *et al*., 2025). Internet fraud is defined as any intentionally deceptive activity involving the use of a combination of Internet components, such as email, chat rooms, and websites, to offer illegal and non-existent goods or services to members of the virtual community, thereby falsely representing such illegal and non-existent goods or services to consumers.

Online fraud is the act of making money by deception utilising network communication technology, or the act of issuing fraudulent invitations to potential victims or carrying out fraudulent transactions using the internet, according to Tade and Aliyu (2011), Whitty (2019); Gao (2021), and others. Internet fraud, often known as phishing, typically entails sending victims an email that appears to be from a reputable business or individual (Frauenstein & Flowerday, 2020). Due to the availability of modern communication technologies, especially mobile devices, internet fraud occurs not just through email but also through text messages, social networking sites (SNSs), and phone calls (Vishwanath, 2015; Aleroud & Zhou, 2017; Frauenstein & Flowerday, 2020).

Phishing and other forms of internet fraud rank sixth among security incident causes and have the greatest success rate of any attack vector (Verizon, 2019). In 2017, a phishing operation that mimicked a major Asian manufacturer fooled Facebook and Google out of over $100,000 (United States Department of Justice, 2017). A meta-

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

analysis revealed that roughly 2.7 billion dollars in economic damages were incurred by online fraud in the US in 2018. According to Norris *et al*. (2019), internet fraud is the crime that is expanding the quickest in the United Kingdom, with 3.25 million individuals falling victim to it annually. Online scammers started using people's fear and anxiety in the early stages of the COVID-19 epidemic in 2020 as a springboard for phishing attempts (Muncaster, 2020; Omigbodun & Akinloye, 2026). According to Burges *et al*. (2017) and Modic *et al*. (2018), internet fraud has grown in importance as a social governance issue and is receiving more and more attention from academics.

Problem

It might also include the transmission of such victims' cash, accessing gadgets, or obtaining possession of other valuable objects without the victim's informed consent (US Federal Bureau of Investigation, 2003). The reputation of Nigerian cyber-fraudsters known as the Yahoo boys has constantly placed Nigeria among the world's biggest cybercrime hotspots. Indeed, various international organisations and law enforcement agencies, including the United Nations Office on Drugs and Crime (UNODC), the International Criminal Police Organisation (INTERPOL), and the Federal Bureau of Investigation (FBI), have attested to Nigerian cyber fraudsters criminal ingenuity and the devastating transnational socioeconomic impacts over time (This Day, 2016; Aderinto & Ojedokun 2017).

Yahooboyism, a phrase that first appeared in Nigeria in the early 2000s, is now used to characterise a criminal subculture of young people interested in online fraud (Ajayi 2019; Ojedokun 2010). The illegal activities of Yahoo boys have not only been recognised as a severe problem by the federal government of Nigeria, but they have also become a major source of concern for other internet users worldwide (Ojedokun & Eraye 2012; This Day 2016). The FBI apprehended a Nigerian cybercrime gang in the United States of America in August 2019 after it scammed its victims of around $3 billion through fraudulent wire transfers, business email compromise (BEC) crimes, and dating/romance scams (Oladimeji, 2019; Premium Times, 2019).

Similarly, in June 2020, the Dubai Police arrested a suspected cybercriminal group led by a Nigerian for allegedly plotting and carrying out a global cyber scam of AED 1.6 billion ($435 million) (Vanguard, 2020). Furthermore, according to the Nigeria Deposit Insurance Corporation's (NDIC) 2014 study, fraud in the Nigerian banking

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

sector's e-payment platform surged by 183% between 2013 and 2014 alone (This Day, 2016). Even though the online criminal activities of Nigerian cyber-fraudsters have received a great deal of scholarly attention (Jegede, Elegbeleye, Olowookere, and Olorunyomi 2016; Ogunleye, Ojedokun, and Aderinto 2019), there is a scarcity of empirical data on their success factors.

Beyond the commonly documented forms of internet fraud, this study draws attention to how perpetrators deliberately construct credibility and manipulate trust before financial exploitation occurs. Perpetrators may present themselves as genuine and trustworthy individuals, provide false personal or professional information, assume fabricated identities, or develop seemingly genuine personal or romantic relationships with potential victims. Through such strategies, they may influence how victims perceive information, evaluate credibility, and make decisions (Button *et al*., 2014). This study therefore extends existing discussions by examining internet fraud victimisation as a process involving credibility construction, trust manipulation, and decision-making, thereby providing a cognitive perspective on how deceptive online interactions may progress from initial contact to successful victimisation.
Hence, a study of this nature is significant because it will explore the theoretical standpoints on the factors influencing the success of Yahoo boys in conducting internet fraud. This study will employ social learning theory, strain theory, routine activity theory (RAT), theory of deception, the elaboration likelihood model (ELM), and the heuristic-systematic model (HSM). This study will employ a literature approach in the study.

2. Literature Review

The Yahoo boys in Nigeria

The growth of the Yahoo boys is inextricably linked to the arrival of the Internet. Nigeria had its first Internet connection in 1995, thanks to the UNESCO-sponsored Regional Informatics Networks for Africa (Internet eXchange Point of Nigeria, n.d.). Access was difficult to spread in the early years due to the Abacha administration's self-proclaimed attempts to eradicate 419. Following Nigeria's democratic transition in 1999, Internet and cellular phone technologies became more popular in Nigerian culture (Smith, 2007). In 2002, it was predicted that 350,000 Nigerians own a mobile phone (Falola and Heaton, 2008). By June 2013, the country has over 120 million active mobile phone customers (Nigeria Communications Commission, 2013).

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

The internet was introduced in the late 1990s, “98, 99, and the year 2000.” Yahoo, an American multinational Internet firm best known for its search engine, online portal, and email service, was the global market leader at the time (Seodotcom, 2011; Wall, 2013). Because Yahoo! was the primary Internet service provider in Nigeria for many years, the term “Yahoo” became a Nigerian slang term for the Internet. According to the informant, “in Nigeria, the illiterates refer to Internet, anything online, Internet as Yahoo.” You want to browse, you want to Yahoo, anything Yahoo.” As a result of the subsequent surge in Nigerian Internet fraud, “Yahoo” and “Yahoo Yahoo” became words for Internet fraud, and people who committed these sorts of fraud were known as “Yahoo boys.”

In contemporary Nigeria, "Yahoo boys" has also come to describe young men perceived to have acquired wealth through online fraud, especially when the source of their wealth is unknown. They are associated with conspicuous consumption, such as lavish spending, expensive clothing, and exotic cars (Lazarus, 2018). This visibility has affected how young people are perceived: those who earn their wealth legitimately may sometimes be mistaken for "Yahoo boys" on appearance alone. Meanwhile, the perceived rewards of internet fraud draw some youths towards quick wealth rather than legitimate work (Tade & Aliyu, 2011). The growing social acceptance of illicit wealth may also reshape young people's ideas of success, encourage materialistic aspirations, and weaken disapproval of fraud (Lazarus, 2018; Ndubueze, 2013).

3. Theoretical Review

Social Learning Theory

The premises of Ronald L. Akers' social learning theory served as the theoretical foundation for this study. Akers and Jennings (2016) define social learning theory as a hybrid of differential association and behavioural learning theories. It contends that crime is a learned behaviour caused by the combination of four major components: differential association, definitions, differential reward, and imitation. The theory's differential association component implies that people's contacts with others vary in frequency, duration, priority, and intensity, with the most important interactions being intimate personal groupings such as family and friends.

Thus, connections that occur early in childhood (priority), endure longer (duration), occur more frequently (frequency), and/or include persons to whom the individual has a strong attachment (intensity) have a stronger impact on an individual's

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

definitions and subsequent behaviour (Akers & Sellers, 2013; Akinloye, 2024a). Definitions include the meanings, attitudes, values, and orientations that people associate with crime and deviance, as well as conforming behaviour, whereas differential reinforcement focuses on the balance of the perceived, experienced, or anticipated reward(s) and punishment(s) that would likely accompany or follow the display of a specific type of behaviour (Akers & Jennings, 2016; Akinloye, 2024b). As a result, behaviours that are regularly displayed and frequently rewarded (and strongly reinforced) are ones that people are most likely to continue to practice (Akers & Jennings, 2016).

Imitation is described as engaging in behaviour after observing another person engaging in a related activity (Holt, Burruss & Bossler, 2012). Individuals are more likely to choose criminal behaviour over conforming behaviour when they associate differently with those who expose them to deviant patterns when deviant behaviour is differentially reinforced over conforming behaviour when they are more exposed to deviant compared to conforming models, and when their definitions favour committing deviant acts (Akers & Sellers, 2013).

Therefore, the idea posits that deviation and conformity have a bidirectional relationship since they are both impacted by the modelling and reinforcing process. Yahoo boys are not only reliant on their offline and online contacts for knowledge and information on cyber fraud techniques, but they are also reliant on their social networks for the acquisition of critical tools and resources used to facilitate their illegal acts in cyberspace.

Robert K. Merton's Anomie/Strain Theory

Merton (1968) claimed that deviation, in whatever shape it takes, is a consequence of society's culture and structure. This idea is founded on the functionalist concept of value consensus, which refers to shared values held by society's members. Thus, deviation happens when the ideals that society accepts do not match or cannot be accomplished in culturally accepted ways. According to Merton (1968), members of society share key aims or values, such as success, which is generally measured by wealth and material goods. Educational credentials, hard effort, ability, skill, dedication, and ambition, on the other hand, are institutionalised ways of achieving such goals (Jegede & Olowookeere, 2014).

In a normal and balanced society, the focus should be on both cultural aims and institutionalised methods. An imbalanced society, on the other hand, will result in a condition of anomie in which individuals of the society disregard the rules of the game to attain the goals. When the norms are no longer followed, deviation in any

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

form is encouraged. However, people in society do not all react the same way to this scenario. Merton, in reality, identifies five unique approaches, which are listed below:

a) Conformity: The most usual reaction. Members of society here conform to cultural ideals and adhere to institutionalised means. They seek to attain these objectives through normative or approved ways. This is the most widespread, and it serves as the foundation for the society's continuity and stability.

b) Innovation: This is the reaction that piqued the researcher's interest in this study. It entails rejecting conventional methods of success and turning to deviation. In other words, innovators accept cultural values but pursue alternative techniques of reaching them that provide higher returns than institutionalised approaches.

c) Ritualism: Those who answer in this group are considered aberrant since they forego societal success objectives in favour of institutionalised methods of reaching such goals. According to Merton, this occurs because individuals have been socialised to such standards and ideals yet have little chance of achieving them.

d) Retreatism: This refers to pariahs, vagabonds, outcasts, and vagrants who are unable to attain success despite internalising both cultural aspirations and institutionalised methods. As a result, individuals resolve this issue by forsaking both, a condition analogous to "dropping out" of society.

e) Rebellion: The rejection of cultural aims as well as institutionalised means. In addition to rejection, there is an endeavour to replace them with other aims and means to establish a new society.

Merton defines the causes of deviance as individual responses to contemporary society's structural and social aims and conflicts. Economic success is described as being accessible and attainable by everybody, and this premise serves as the foundation for cultural goals established for all members of society. The tools to achieve such aims, however, are not equally available to all members of society (Muraina & Muraina, 2015). As previously stated, this societal disjunction causes varied pressures at the individual level, particularly when the lower class recognises the impediments of traditional ways to achieve such cultural ideals (Tade, 2013). Merton also stated that economic riches are a prominent objective in society and that education is the traditional way of achieving such wealth.

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

Strains occur when methods fail to fulfil goals, such as when the availability of employment inside the country can no longer serve as a means of reaching the cultural aim of riches, putting pressure on adolescents, who respond in a variety of ways. Other research on the elements that encourage young people to engage in Internet fraud and other criminal behaviours, particularly in Nigeria, supports the feasibility of the Anomie/Strain Theory (AST) for the topic. According to Jegede *et al*. (2016), the failure of the government and society at large to provide legally acceptable and institutionalised means of achieving cultural goals such as economic success has led younger members of society to choose either attitudinal apathy or deviant innovation. Makinde (2005) agrees, stating that youngsters are continually inventing to adapt to the tough political and economic climate. As several studies have identified poverty (Okeshola & Adeta, 2013; Tade & Aliyu, 2011), unemployment, and underemployment (Adesina, 2017) as major motivators for involvement in cybercrime, it is clear that young adults in society face significant barriers to achieving economic success through traditional means.

In this aspect, Merton's Innovation strain looks to be an intriguing theoretical framework for explaining young people's engagement in Internet fraud. However, it is worth noting that some studies, such as Tade and Aliyu (2011), used the Institutional Anomie Theory (IAT) as the theoretical framework for their research. While the study acknowledges the IAT's usefulness as a theoretical framework, Robert Merton's Anomie/Strain Theory is more appropriate since innovation is considered a consequence of strain. For a more thorough analysis, future studies may combine both theories.

Routine Activity Theory

According to routine activity theory, victimizations are caused by appropriate targets, motivated offenders, and ineffective guardianship (Cohen & Felson, 2010). Cunning is a tool used by motivated criminals to deceive victims. Six fundamental characteristics of persuasion are usually used by fraudsters; they are reciprocity, social proof or conformity, commitment or consistency, authority, likeability, and scarcity (Cialdini, 2018).

For instance, the receiver reacts to information about scarcity to prevent missing out on possibilities (Bullée *et al*., 2015). Regarding effective guardianship, fighting and preventing cyber fraud is a top priority for all nations. Strict legal action against offenders, educating and recalling possible victims, and technological techniques of interception are common strategies (Chen & Yang, 2022). When considering why so many individuals fall victim to online fraud attempts daily, one must adjust their focus to the right victim or target.

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

There are three primary avenues in which researches were carried out on possible online scam victims:

a) Firstly**,** research conducted on demographics such as age, income, education, gender, and race of people who fall prey to online fraud is the first area of focus (Holtfreter *et al*., 2006; Salthouse, 2012; Burnes *et al*., 2017; Gavett *et al*., 2017). It was revealed in those research that men are more prone than women to become victims of personal crimes like computer fraud, according to research by Carcach *et al*. (2001). Many academics have focused their study and attention on age, and the idea that older persons are more susceptible to fraud has been developed by the rising ageing phenomenon and the dissemination of anecdotal evidence, such as news articles.

Research has been carried out to examine various aspects of victims of online fraud and it was discovered that, in contrast to other forms of criminal activity, older persons are more susceptible to falling victim to consumer fraud (Carcach *et al*., 2001). According to Burnes *et al*. (2019), the elderly are more easily cheated, which is related to their high experiences of loneliness and slow cognitive processing. Furthermore, James *et al*. (2014) discovered a correlation between the education level and income of fraud victims and their susceptibility to deception. According to many Federal Trade Commission (FTC) research, non-Hispanic white Americans are less likely than African Americans, Hispanic Americans, and Aboriginal Americans to become victims of fraud (Anderson, 2004; Anderson, 2013).

b) Secondly, in terms of psychological traits, studies have mostly focused on the variables that influence a person's vulnerability to online fraud. These include the perception of danger (Moody *et al*., 2017), personality (Ashton & Lee, 2009), trust (Wright & Marett, 2010), suspicion (Harrison *et al*., 2016), and self-control (Modic & Lea, 2012). According to Holtfreter *et al*. (2008), there is a greater chance of deception among populations who exhibit poor self-control.

This is mostly because those who lack self-control want to get what they want right away. They could comply with a con artist's instructions to get a promise. Researchers discovered that not all personality variables indicate sensitivity to fraud in their investigation of the connection between personality and susceptibility to online fraud. Alseadoon *et al*. (2012) used 200 college students to participate in a fraud simulation and discovered that extraversion and openness might increase the likelihood of responding to emails, but no other personality qualities were shown to have a predictive influence. Scholars have also explored the link between victims'

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

online experience, security knowledge, and vulnerability to online fraud in the research of personality variations and susceptibility to online fraud (Larcom & Elbirt, 2006; Wright & Marett, 2010).

c) Thirdly, in terms of the psychological mechanism's orientation, fraud is fundamentally opposed to social interaction, which calls for cognitive resources, by interpersonal deception (Buller & Burgoon, 1996). According to Johnson *et al*. (2001), deception is effective when the perpetrator exploits the target's incapacity to comprehend information and employs strategies to hinder the target's cognitive efforts during communication. Put another way, the victim is the result of either a cognitive inability to recognise fake information a deficit in information processing, or both.

According to earlier research, consumers' cognitive processing plays a significant role in their vulnerability to online fraud (Vishwanath *et al*., 2011). The theory of deception, the elaboration likelihood model (ELM), and the heuristic-systematic model (HSM) are related theories.

Heuristic-Systematic Model (HSM) and Elaboration Likelihood Model (ELM)

The heuristic system, which is based on intuition, and the analytical system, which is based on logic, are the two information processing modalities included in the HSM model (Evans, 2003). The Heuristic System is more dependent on intuition since parallel processing is quick and uses little or no psychological energy. Serial processing is sluggish, requires more mental energy, and is more dependent on reason in the Analytic System. Trumbo (2002) discovered that heuristic processing results in a reduced risk assessment, which eventually causes individuals to fall victim to fraud as it is harder for them to recognise the red flags in fake material. By tricking the intended victim into making a snap judgement about the usefulness of the material, phishing assaults typically enhance their success rate (Luo *et al*., 2013).

The Elaboration Likelihood Model (ELM) differentiates between two methods in which people process information, making it another dual process model. While the peripheral processing route does not take into account every aspect of the message, the central processing route carefully considers the information that is offered utilising comparisons and experience (Petty & Cacioppo, 1986). While there are theoretical similarities between the HSM and the ELM, the HSM stresses the possibility of two different ways of thinking about information, whereas the ELM proposes that information processing happens on a continuum (Frauenstein & Flowerday, 2020).

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

Petty and Cacioppo (1986) claim that the two subprocesses of information processing are attention and elaboration:

According to Vishwanath *et al*. (2011), attention is the initial step of information processing and describes the degree of mental concentration applied to particular aspects of an event or object. According to Perse (1990) and Vishwanath *et al*. (2011), elaboration is the process by which people consciously draw connections between the cues they encounter and their past knowledge. According to Jakobsson's (2007) findings, the target was likely duped because they failed to recognise several telltale signs of a phishing email address, such as the email address. Fraud detection users can apply prior experience and knowledge for evaluation (ELM's elaboration process) and pay attention to illogical cues (ELM's attention process).

Theory of Deception

The detecting deception model is another name for the theory of deception. It describes how people recognise fraud by analysing discrepancies between anomalies and their prior knowledge; so, clue processing is better clarified (Johnson *et al*., 2001).

According to the detection deception model, the process of identifying fraud can be divided into four stages:

a) Activation and anomaly detection of fraudulent data.

b) Formulating hypotheses, analysing anomalous hints, and raising suspicions.

c) Evaluation of the hypotheses: This involves comparing the ideas generated in the previous step with a set of standards.

d) A comprehensive analysis, amalgamation, and general appraisal of recognised hints.

The elaboration process is comparable to these four phases of cognitive effort (Eveland *et al*., 2003; Vishwanath *et al*., 2011). When Grazioli examined the legitimacy of the trading site in 2004 using eighty MBA students, he discovered that proficiency in assessing the theory of deceit was a significant determinant of successful and failed detection. There is disagreement about the findings of a considerable body of prior research on the correlation between psychological characteristics, online fraud, and demography.

Regarding demographic characteristics, Button *et al*. (2009) suggested that there is no demographic feature that predisposes someone to internet fraud more or less.

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

After doing a thorough evaluation of the literature, Shang *et al*. (2022) concluded that older adults were not a sensitive population and that the influencing factors previously examined were unsustainable. Research on trust and other psychological characteristics has produced mutually incompatible results (McKnight *et al*., 2004; Judges *et al*., 2017). Studies on online fraud ought to look at victims' decision-making processes when presented with false information (Norris *et al*., 2019).

Although the ELM distinguishes between the central processing route (system 1) and the peripheral processing route (system 2) in principle, there is no measurement or categorization of these two systems in actuality, according to a description of the decision-making process of victims of network fraud. Scholars primarily concentrate on the connection between online fraud and the attention and elaboration subsystems of ELM (Vishwanath *et al*., 2011; Harrison *et al*., 2016).

It's common knowledge that attention and elaboration are signs of HSM processing (Frauenstein & Flowerday, 2020; Gao, 2021). Using the heuristic systematic model to gather and explore previous studies and their findings regarding the victimisation process and promotion, a study of the literature was done on the decision-making process of victims of online fraud.

Heuristic-analytic processing mode and victims of Internet fraud

Heuristic processing uses straightforward factors or messages (i.e., heuristic cues) to conduct a quick effectiveness evaluation. According to Petty and Cacioppo (1986), users' attitudes, perceptions, and actions about certain information may be influenced by their propensity to process information in different ways.

Based on cognitive resource economics, studies have demonstrated that people favour heuristic processing over effort when evaluating information (Sundar, 2008). Heuristic processing, however, also appears to result in a reduced risk assessment, which makes it harder for people to spot scam traps in false material and puts them at risk of fraud (Wang *et al*., 2012; Jones *et al*., 2015; Vishwanath *et al*., 2016). According to the HSM, for individuals to feel satisfied with their judgements after performing a validity evaluation, their confidence in the evaluation must either achieve or be above the adequacy threshold (the extent people aim to attain when making decisions) (Eagly & Chaiken, 1993).

Recipients are likely to resort to systematic processing when heuristic processing is insufficient to help them meet the sufficiency criterion (Luo *et al*., 2013). According to Vishwanath *et al*. (2016), heuristic processing significantly increases the likelihood that someone will fall victim to phishing attacks via email and Facebook, while systematic processing significantly reduces the likelihood that someone will

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

become a victim of fraud. Furthermore, a high degree of systematic processing might reduce the effectiveness of heuristic processing and potentially lead to conclusions that contradict or limit heuristic processing, by the weakening principle of the HSM (Watts & Zhang, 2008). It is simpler for people to recognise online fraud when they turn on system processing to find and analyse fraud information (Grazioli, 2004).

The included research consistently shows a relationship between the heuristic decision-making model and being a victim of online fraud. Attackers who use phishing techniques are aware of the shortcomings in human information processing and want to increase the success rate of their scams by encouraging victims to think heuristically rather than systematically (Chen & Yang, 2022). Just three studies offered data analysis in terms of specific demonstrations; other documents examined the relationship between victimisation and HSM subsystems or the factors that influence the HSM. These studies primarily illustrated information processing models (the heuristic vs. systematic processing modes) and whether or not subjects were vulnerable to online fraud. According to social psychology studies on phishing, a primary factor contributing to personal victimisation is a cognitive process that is not functioning well (Vishwanath *et al*., 2016).

How can fraudulent information increase people's susceptibility to fraud by causing the HSM to generate erroneous cognition? According to researchers, the two distinct subprocesses of information processing, attention and elaboration, are thought to be markers of systematic processing (Friedenstein and Flowerday, 2020; Gao, 2021). Diverse levels of focus and in-depth analysis of data eventually result in varying vulnerabilities to becoming victims of fraud.

The first step in the processing of information is attention. Because of this interest, some people can feel pressured to read the email carefully, look for further hints, compare the hints to what they already know, decide if the email is relevant, and eventually come to the conclusion that it is a hoax (Jakobsson, 2007). The results of the study indicate a strong relationship between elaboration and attention level.

There is more elaboration among those who focus more on information aspects (Harrison *et al*., 2016b). For instance, suspicious issues regarding typos, grammar, and website URLs in phishing emails may prompt the development of a more thorough message, leading to systematic processing and a decrease in the chance of falling victim to phishing (Toma & Hancock, 2012). Naturally, the emphasis of the attention is on quality rather than quantity. In contrast to popular perception, Grazioli (2004) discovered that successful detection ignores deception cues no more than failure detection.

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

Elaborate information processing happens in the second stage of the information processing-elaboration process when people use a central (systematic) processing path to tie these information items to past knowledge and experience. On the other hand, information components are ignored or no elaboration processing is done for the information elements that are detected when the peripheral (heuristic) processing method is used (Gao, 2021). Compared to those who merely focus on clues, individuals who expound on clues are more likely to comprehend, absorb, retain, and later recall knowledge (Eveland *et al*., 2003). According to Harrison *et al*. (2016), elaboration is a predictor of individual phishing and is associated with a decreased chance of falling victim to phishing. The possibility of being duped is decreased by the development and processing of information content (i.e., by using systematic processing).

Factors related to the selection of the heuristic-analytic processing mode

As was said in the introduction, psychological characteristics, demography, and other elements are being studied as the factors that influence online fraud. Within the context of the HSM, this section's explanation clarifies the variables that might affect a person's information processing style and result in network fraud. This inductive research reveals that the cognitive processing mode for online fraud (the start of the heuristic system mode or analytic system mode; See Figure 1) may be influenced by psychological variables, knowledge and experience, tools, and habits.

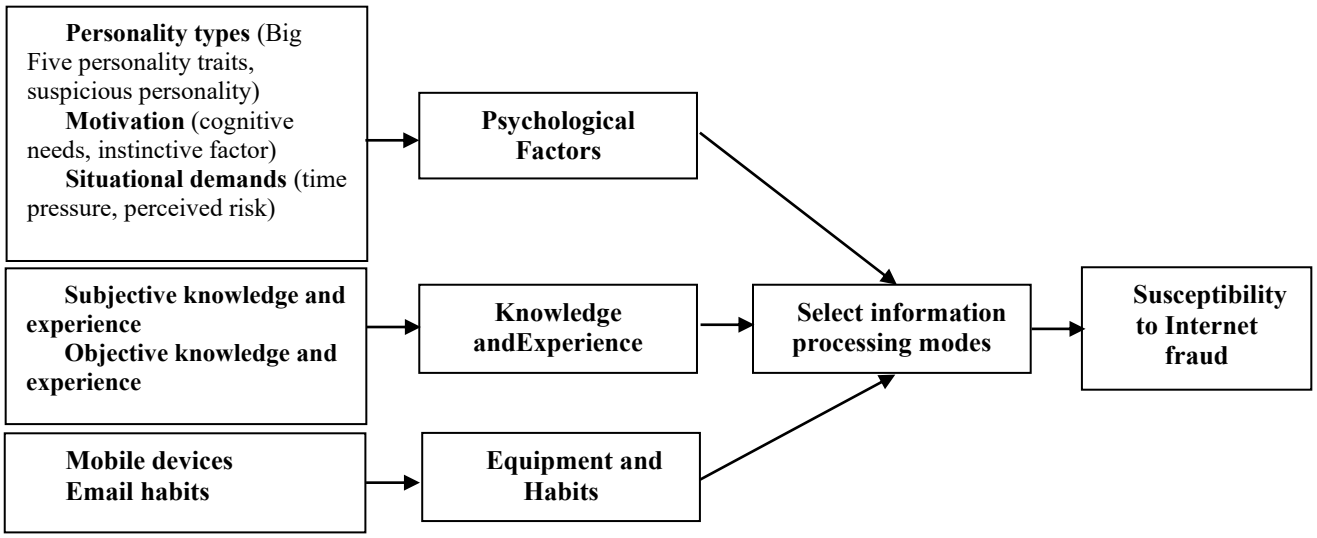

Figure 1: Influencing factors of susceptibility to Internet fraud under a framework of the HSM model

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

Adapted and modified from Norris *et al*. (2019)

Psychological Factors

Personality type

The Big Five personality characteristics and suspicious personality are the core subjects of personality type research. Research has been done on the connection between the Big Five personality qualities and the chance of being a victim of online fraud (Norris *et al*., 2019). Alseadoon *et al*. (2012), for instance, discovered that those who exhibit high levels of agreeableness, openness, and extraversion are particularly vulnerable to information available online; nevertheless, this study did not come to a consistent result. According to Cho *et al*. (2016), neuroticism and agreeableness were highly predictive of the chance of falling victim to online fraud. Only the study of Frauenstein and Flowerday (2020) was located inside the HSM framework.

These authors examined the relationship between the Big Five personality model and the heuristic-systematic model of information processing for the first time, showing how heuristic processing increased susceptibility to phishing assaults. They found that extraversion was not statistically correlated with either heuristic or systematic processing, agreeableness, neuroticism, and openness all had effects with both, and conscientiousness was statistically correlated with heuristic processing but had no effect with systematic processing. Heuristic and systemic processing may be operating simultaneously while processing information, as evidenced by the notable correlation between the impacts of both processes and personality traits (such as neuroticism and agreeableness).

Generalised communicative suspicion (GCS; Levine and McCornack, 1991) is a form of persistent personality characteristic that refers to an individual's propensity to be suspicious of the intentions of others. There have been two phases of research on the connection between GCS, the HSM, and network fraud susceptibility:

Stage 1 treated the relationship between GCS and the HSM as separate dependent variables,

Stage 2 established the relationship between GCS and the HSM, whereas.

This study mostly discusses Stage 2. From the perspective of the HSM and internet fraud victimisation, network users' starting the heuristic system during information processing is the primary cause of their inability to recognise fraud and eventual victimisation (Luo *et al*., 2013; Huang *et al*., 2022). Information insufficiency was

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

presented by Harrison *et al*. (2016) as a mediator between the GCS and the HSM. They discovered that a high GCS raises uncertainty and encourages a demand for additional information before making a decision. The need for more information results in the methodical assessment of the data that is already accessible and in the more precise identification of phishing deception.

Motivation

Unmotivated people typically spend less time and mental energy, according to the HSM (Luo *et al*., 2013). People who are motivated to digest information focus on the salient details of arguments before engaging in more in-depth thought processes. On the other hand, unmotivated people could concentrate on signals that are not related to the primary argument and could be convinced by noncontent signals (Stamm & Dube, 1994). The degree of information elaboration depends on the recipients' incentive to pay attention.

According to Langenderfer and Shimp (2001) and Wang *et al*. (2012), network users who are more inclined to contemplate a scam are also more likely to thoroughly study the intricacies of the material, which might result in the discovery of leaked evidence about the scam and the avoidance of victimisation. Additionally, Langenderfer and Shimp (2001) discovered a possible inverse relationship between motivation and susceptibility to fraud victimisation, and they hypothesised that a deficiency in motivation may be one of the causes of a dearth of reviews.

Nonetheless, some academics contend that highly motivated people tend to understate the benefits and drawbacks of making decisions, ignore potential issues, and process information related to making decisions and related decisions less well (Fischer *et al*., 2008). Research by Ariely *et al*. (2009) demonstrated that when decisions involve amounts above people's typical experience levels, decision-making quality declines. The quest for cognitive and instinctual components of motivation is necessary in light of these contradictory results. The HSM states that behavioural expectations that an individual has for themselves are the foundation for the incentive to devote cognitive resources (cognitive requirements; Chaiken, 1987).

According to Vishwanath (2015), perceived information deficiency is a strong predictor of system processing, and the higher one's cognitive demands, the more processing power is required. Higher cognitive needs individuals are less vulnerable to heuristic processing and are hence less likely to be deceived (Luo *et al*., 2013). However, there are situations where people might fall victim to deception despite having strong motivation. This might have to do with instinct, which frequently leads

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

to careless choices; in other words, those who are influenced by instinct typically don't think through the repercussions of their own choices (Loewenstein, 1996).

People overlook clear indicators of fraud in the attention process when they are very eager to receive the reward offered by false information or to avoid the risk contained in fraudulent information (Langenderfer & Shimp, 2001). Therefore, instinctive variables may function as a moderator of the effect of motivation on the susceptibility to deception. Strongly motivated people are more likely to overlook cues in the information and concentrate more on winning or avoiding losses when instinct is strong, but people with weaker instincts might decide to carefully consider the information's specifics as opposed to the reward itself (Whitty, 2013; Jones *et al*., 2015).

Situational demands: perceived danger, time constraints, etc. Shah *et al*. (2004) discovered that recipients of phishing emails tend to pay undue attention to urgent cues and disregard other important details like spelling, grammar, and source (Jakobsson, 2007). When people are under time constraints, they tend to depend more on urgent signals or employ fewer product qualities when making decisions, which eliminates the systematic processing that takes time and cognitive resources (Rothstein, 1986). Paying attention to urgent cues can also create a sensation of urgency and pressure. Phishing-generated content with urgent indications slows down cognitive processing and prevents the systematic processing of additional clues that can point to fraudulent sources of information.

According to Harrison *et al*. (2016), phishers anticipate that by emphasising emotional reactions, these urgent indications would steer users away from more logical decision-making processes. According to Luo *et al*. (2013), adding greater time pressure to phishing communications may lessen the influence of argument quality and boost the influence of source legitimacy and the herd effect, which would enhance heuristic processing and affect a person's vulnerability to being a victim of fraud. Nonetheless, certain research has indicated that the attributes of emails, such as the requirement for prompt decision-making, do not impact the way online users interpret phishing emails (Harrison *et al*., 2016).

When people consider risk-related behaviours, risk-related beliefs are the most often employed cognitive framework (Gryphon *et al*., 2002). Individuals modify their actions in response to perceived threats by considering the potential harm and associated risks (Grothmann & Reusswig, 2006). People undergo systematic processing when they expect their actions to have dire repercussions, which heightens their uncertainty (Workman, 2008). Cyber-risk views are favourably

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

correlated with systematic processing and negatively correlated with heuristic processing, according to research by Vishwanath *et al*. (2016).

People who have strong opinions about cyber risk are better at spotting online fraud. This contrasts with the results of Das *et al*. (2003), who hypothesised that the presence of threat elements in information may have a unique effect on information processing; consequently, resources for information processing are allocated unevenly, and the acceptability of convincing information rises. Research has demonstrated that the fear-induced perceived risk does not affect the elaboration process. Additionally, some researchers have confirmed through trials that an increased perceived danger did not reduce the probability that an individual would fall for a phishing email.

This is because some individuals with higher perceived risks when it comes to online fraud may be afraid of the repercussions of making a mistaken decision and may be less inclined to recognise deception cues due to potential social and financial ramifications (Harrison *et al*., 2016).

Knowledge and experience

Certain knowledge and experience-related characteristics can be used to predict the information elaboration processing stage. Individuals without the requisite expertise or comprehension to comprehend a given argument typically depend on incidental cues in the data, which prompts heuristic processing and may result in erroneous conclusions (Chen and Chaiken, 1999). Wright and Marett (2010) discovered that in the context of phishing, network experience and security knowledge can make it easier for users to spot and recognise fraudulent hints in phishing emails, raise the likelihood that the information will be noticed and elaborated upon, and ultimately lower the likelihood that they will become victims of phishing.

Harrison *et al*. (2016) also discovered that elaboration is predicted by expertise in certain disciplines rather than being impacted by message characteristics. Adults are less dependent on heuristic processing than children are since they can critically examine pertinent information due to the development of acquired knowledge and cognitive abilities. Even in a time-constrained environment, knowledgeable participants may engage in and effectively complete deception detection (Grazioli, 2004). Understanding email fraud draws attention to telltale signs of phishing schemes and decreases response probability (Wang *et al*., 2012). Information receivers are better able to comprehend and absorb pertinent concerns when they have a greater level of prior professional knowledge. This enhances the possibility

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

of elaboration and decreases reliance on peripheral signals (Ratneshwar and Chaiken, 1991).

Harrison and colleagues (2016) discriminated between objective and subjective knowledge, concluding that only the latter was linked to increased attention to emails. Reduced attention resources are also required to elicit professional information when one is more knowledgeable. Nonetheless, it has also been suggested that such past knowledge may present a biased view of information obtained externally since stored knowledge is frequently skewed towards the original viewpoint (Crocker *et al*., 1984). Subjective knowledge, or false information, can also give rise to a false sense of confidence and result in a lack of focus and detail on the particular details in phishing emails that could point to deceit (Harrison *et al*., 2016).

Equipment and habits

According to a recent study, using mobile devices like smartphones can improve heuristic processing, increasing the likelihood that consumers would fall into online fraud traps. Users will be more receptive to the heuristic indications in phishing emails if they would rather analyse emails on their phones than on desktops (Kim and Sundar, 2015; Vishwanath, 2016). Since smartphones are primarily touch-based devices with smaller screens than desktops, the material must fit into a constrained amount of space (Sundar, 2008). Smartphone layouts and designs prioritise rich graphical cues over textual content. Rich presentation improves heuristic processing by depleting the limited cognitive capacity and resources required to absorb persuasive material (Kim and Sundar, 2015).

Additionally, the cognitive resources available for system processing are diminished while using a multitasking processing mode (Chaiken, 1987; Ratneshwar and Chaiken, 1991). According to experimental data, smartphones with large screens and video modes encourage heuristic processing, whereas smartphones with tiny screens and text modes encourage systematic processing (Kim and Sundar, 2015). Nonetheless, some research indicates that cognitive heuristics and email habits both individually and combined influence the likelihood of falling victim to online fraud. Instead of altering cognitive functioning, mobile gadgets like smartphones increase habitual susceptibility to fraud (Sundar, 2008; Vishwanath, 2016). According to LaRose and Eastin (2004), a habit is an automatic behaviour pattern or reaction that is prompted by external stimuli and carried out without conscious thought. Habits follow a regular cognitive pattern.

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

According to studies, habitual response patterns (such as replying right away when one wakes up) can limit one's ability to respond to phishing emails. In other words, people respond to relevant emails without actively considering them (Vishwanath *et al*., 2011). Habitual email activity that is formed subconsciously is distinct from conscious behaviour that requires some level of thought, according to the concept of habit (Aarts *et al*., 1998). Stated differently, responding to reports of online fraud entails a disregard for and underdevelopment of the HSM. Three primary approaches exist within the HSM framework for email habits to impact victims of online fraud:

Email habits are negatively correlated with suspicion, heuristic processing is negatively correlated with suspicion, and systematic processing is positively correlated with suspicion (Vishwanath *et al*., 2011). Additionally, email habits are parallel to the heuristic-systematic model (Vishwanath *et al*., 2016). These patterns of media usage, which represent an extreme value of involvement that is positively correlated with the level of elaboration, when combined with a high-level email load that is negatively correlated with the level of elaboration, have a strong and significant impact on the likelihood of individuals being phished.

Measures of the heuristic-analytic processing mode, influencing factors and likelihood of internet fraud victimisation

Under the HSM framework, measures of the probability of being a victim of internet fraud are carried out using the experimental approach. In the course of these experiments, researchers give victims fraud materials, such as financial statements (Grazioli and Wang, 2001), phishing emails (Luo *et al*., 2013), and shopping websites (Grazioli, 2004). These materials may be created by the researchers specifically for the study or they may be actual fraud materials. The possibility of being duped is estimated based on the subject's evaluation of the veracity of these materials or if the subject answers. For instance, Wang *et al*. (2012) used a genuine phishing email as a stimulus to study 321 students at a major institution in the northeastern United States.

The researchers identified themselves as an email team, informed users of a website update, requested user name, password, and other information, and asked users to confirm the details associated with their email accounts. Users were warned that their email accounts would be permanently deleted if they failed to submit the needed information within the allotted seven days. The email said, “UPGRADE YOUR EMAIL ACCOUNT NOW.” in its headline. Subjects in the Wang *et al*. study ran the risk of being duped if they replied to emails and gave information, but not if they didn't.

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

The method used to measure systematic and heuristic processing is self-reporting following studies. Various researchers have created objects with varying amounts and contents; studies have utilised three items (Vishwanath *et al*., 2011), four items (Gryphon *et al*., 2002), and six items (Schemer *et al*., 2008). The Vishwanath *et al*. (2011) scale has been frequently cited: three items, namely "I thought about the action I took based on what I saw in the Facebook message" and "I skimmed (i.e., moved quickly) through the Facebook message" are examples of heuristic processing; the other three are examples of systematic processing. All of the measures used a five-point Likert scale, even though their contents and item counts varied.

Self-reports have also been used to gauge the attention to and elaboration of the HSM subsystems, however, the precise techniques of assessment used were different. A few research works have made use of the Eveland *et al*. (2003) or Eveland and Dunwoody (2002) scale. Alternative methods for measuring have been utilised in certain research. Harrison *et al*. (2016), for instance, employed response length (word count) as a metric to assess the degree of elaboration, while an open-ended question asking participants to justify their actions or inactions was used to gauge the amount of elaboration. The researchers used correct recollection of email components to gauge participants' attention to those items. They discovered a strong correlation between elaboration and attention, meaning that those who elaborated the message more also paid greater attention to its components.

Some examples of existing measures that can be used to measure influencing factors are the BFI personality trait scale (John & Srivastava, 1999), the suspicion scale (Lyons *et al*., 2011), the suspicion of humanity scale (Wright and Marett, 2010), the cyber-risk beliefs scale (Vishwanath *et al*., 2016), the risk beliefs scale (Wright and Marett, 2010), the perceived risk scale (Drolet & Morrison, 2001), the domain-specific knowledge scale (Vishwanath *et al*., 2011), the subjective e-mail knowledge and experience scale (Harrison *et al*., 2016), the web experience scale (Everard and Galletta, 2005), and the email habits scale (Verplanken & Orbell, 2003).

Defence strategies under the HSM

Technology, education, and simulated scene training are the key remedies against susceptibility to online fraud within the theoretical framework of the heuristic-systematic model.

Technology

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

According to Huang *et al*. (2022), human flaws including inattention may play a role in online fraud. They created a human-technical solution that creates adaptable visual aids (ADVERT) based on eye-tracking data to focus users' attention on the email content rather than on unimportant distractions. In a case study based on a human experimental dataset from New York University, they reported success. In addition, Chen and Yang (2022) created an enhanced deep attention collaboration filter that was successfully evaluated in a case study centred around an educational institution. This filter helps users examine social information directly or indirectly to detect spam.

Furthermore, prior research has discovered that device affordance may impact heuristic processing by encouraging users to decrease their cognitive resource investment, relax their cognitive participation in information processing, and perform heuristic processing on cognitive information, thereby increasing their susceptibility to online fraud (Kim & Sundar, 2015; Vishwanath, 2016). Positive outcomes have also been seen in the use of technology, such as spam blockers (Vishwanath *et al*., 2011), fraud risk identification systems (Frauenstein & Flowerday, 2020), and anti-phishing software and toolbars (Wright & Marett, 2010), to protect against fraud attacks mediated by intelligent devices.

Education

Those in these high-vulnerability groups typically have low-risk awareness and little experience with network security. Education may improve people's perceptions of risk and their knowledge base about network security. According to Wright and Marett's (2010) findings, education appears to be the most effective strategy for thwarting phishing attacks. Network security knowledge education should be improved to put educational measures into action. Examples of this include user training initiatives (Luo *et al*., 2013), legal initiatives to combat internet deception (Grazioli, 2004), and training and education on email deception detection (Harrison *et al*., 2016).

Lack of domain expertise makes it harder for people to recognise false information; instead, they often process information only peripherally and depend on small hints found in emails, which leads to poor decisions and online fraud (Vishwanath *et al*., 2011). Education may enhance awareness and elucidate information, make it easier for individuals to see fraud indicators, and lessen the chance that they will fall victim to phishing (Harrison *et al*., 2016). Furthermore, educational initiatives including cyber-risk belief education (Vishwanath *et al*., 2016), security awareness education courses (Frauenstein & Flowerday, 2020), and scam awareness training (Wang *et al*., 2012) should be used to enhance people's capacity to perceive risk.

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

Simulated scene training

A type of embedded education known as "simulated scene training" exposes users to several scenarios as they role-play on a fictitious email inbox. Participants can experience the outcomes of both suitable and incorrect reactions after being exposed to various forms of email phishing (Wright & Marett, 2010). This measure has received official recognition. For instance, organisations like the New York State government have implemented contextual training to prevent phishing. Upon completion of the study, users receive materials on preventing phishing and are sent simulated emails with malicious attachments (Wright and Marett, 2010). Network users engaged in the simulated network fraud environment may successfully increase their feeling of network self-efficacy by actively, intuitively, and vividly experiencing relevant anti-fraud information through lifelike interaction. In the end, this lowers the possibility that they will react to information about network fraud by giving them greater confidence while processing information about network fraud in reality.

---

4. Discussion

The heuristic system and internet fraud victimisation

The reviewed literature appears to concur that the identification of fraud in networks is done through the analytic processing mode and is associated with heuristic processing. This is because the analytic system relies more on logic, processes information more slowly, and has a lower mistake probability than the heuristic system, which depends more on intuition, rapid parallel processing, and judgement errors that are more common (Chaiken, 1980; Evans, 2003). The theory of deception and the theory of interpersonal deceit have both supported this result (Johnson *et al*., 2001).

The supporting data is not strong, nevertheless, notwithstanding the heuristic-analytic system's experimental outcomes and susceptibility to online fraud. First, only the three studies presented by Vishwanath *et al*. (2016), Harrison *et al*. (2016), and Frauenstein and Flowerday (2020) have direct empirical investigations in the literature. Secondly, the idea that the HSM is the victim of online fraud is not entirely supported by these three pieces of research. For instance, Frauenstein and Flowerday (2020) found that systematic processing and phishing susceptibility did not significantly correlate. Third, the separation of the two systems in the process of thinking and decision-making is contested by some academics.

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

For instance, Moshman (2000) proposed that the analytic system is automated, but the heuristic system is implicit, and that the separation of the two systems is insufficient to include the decision-making and reasoning process as a whole. It is challenging to enable the heuristic processing forecast of the probability of network fraud victimisation in the absence of a dual system division. Not to mention, it might not be accurate to assume that the intuitive heuristic system is inferior to the rational analytical system.

Gigerenzer, working with the ABC Research Group, found and suggested the "Fast and frugal heuristics" (Gigerenzer, 2008; Gigerenzer *et al*., 2008; Liu, 2009) based on the principles of limited rationality and ecological rationality. Numerous research demonstrated that "Fast and frugal heuristics" were sensible and effective cognitive techniques for knowledge retention. For instance, Gigerenzer and Gaissmaier (2011) discovered that, in cases of poor predictability and small samples, omitting certain information might result in more accurate conclusions than adding all the information and weighting it. Given the existence of these ambiguous or debatable opinions, a more thorough study is needed to prove that network fraud and heuristic information processing modes are related.

As per the opinions of the academics involved in our investigation, attentiveness and elaboration are considered subsystems of the HSM (Gao, 2021) and the ELM (Frauenstein and Flowerday, 2020). The impact of attention and elaboration on the vulnerability to online fraud is further supported by empirical research (Vishwanath *et al*., 2011; Toma and Hancock, 2012). It's crucial to remember that the standard of the clues rather than their quantity is what counts when evaluating online fraud. According to theory, cognitive busyness or cognitive laziness (Petty and Wegener, 1999), insufficient adjustment (Epley and Gilovich, 2004), and intuitive confidence (Simmons and Nelson, 2006) account for the HSM.

Nevertheless, none of the recent research that uses the HSM to explain vulnerability to online fraud has proposed these methods. Furthermore, ten types of "Fast and frugal heuristics" have been compiled by Gigerenzer (2008a). These include recognition heuristics, which determine which of the two or more options has a higher validity value if one is recognised, and adoption of the best heuristics, which search for a clue based on its validity and stop searching when a clue that can distinguish the two options is found. To determine which "quick thrift heuristic" is connected to victims of online fraud, further data is required.

The aforementioned conversation does not intend to refute the connection between the heuristic-analytic system and victims of online fraud. More evidence is required despite studies on the link between the two processing systems and vulnerability to

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

online fraud, or the relationship between the two processing systems' explanation mechanism (the subsystems) and susceptibility to online fraud.

Factors related to the selection of the heuristic-analytic processing mode

Rather than only examining the influencing elements of vulnerability to online fraud, our research explored the influencing factors within the HSM framework. Psychological variables are unstable throughout analysis, and the findings of many research contradict one another. In the field of motivation studies, for instance, people who are motivated to process information typically focus on important information arguments before engaging in elaboration processing (Luo *et al*., 2013). However, choices get worse when there is more information involved than people typically have access to (Ariely *et al*., 2009).

Uncertainty in risk perception under situational demands may result from varying interpretations of what constitutes danger. People who have strong opinions about cyber risk may be able to engage in systematic processing to better detect online fraud if risk perception is seen as a permanent personality trait (Vishwanath *et al*., 2016). However, if the information creates a state of anxiety due to threat factors, it may make people more susceptible to deception (Das *et al*., 2003) or have no effect at all (Das *et al*., 2003; Wright & Marett, 2010).

Furthermore, more research is required to understand the process behind personality characteristics' application to the HSM framework, as they have done for the first time (Frauenstein & Flowerday, 2020). Unlike the previously mentioned criteria, a high GCS raises uncertainty, which encourages methodical information processing and improves the accuracy of phishing detection (Harrison *et al*., 2016). This result is in line with earlier research (Wright & Martt, 2010). Does the choice of heuristics and analytical systems depend on any other psychological factors?

Forgas and East (2008) discovered that consumers' emotions influence their capacity to recognise deceit. Users are better at detecting sadness when they are depressed. The ELM states that similar to other factors, emotions may influence attitudes through a variety of low-effort processes while thinking under relatively low-thinking situations. Nevertheless, these same emotions can influence persuasion through other methods when thinking is relatively likely (Petty and Briñol, 2014). More research is required to determine if feelings influence the mediating role of the heuristic and systematic processing modes, hence impacting vulnerability to online fraud. According to Schonfeld and Chang (2017), building workers frequently reside distant from their families, which might eventually cause loneliness.

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

According to a poll, many decided to create online acquaintances in an attempt to get over their feelings of inadequacy and loneliness, which resulted in online dating fraud. The finding that knowledge and experience, particularly the particular information and experience relevant to online fraud, are protective factors against online fraud is generally consistent within the framework of the HSM (Wright & Marett, 2010). According to Feeley *et al*. (1995), interpersonal deception research places experience at the core of the fraud detection process, since it can increase the accuracy of spotting misleading information. Those with pertinent knowledge and experience are better equipped to digest new information in detail when pertinent occurrences are readily available and preserved. This facilitates the creation of links between the information received and pertinent events.

It's important to remember two things:

(a) previous knowledge may contain a biassed evaluation of data that was obtained from outside sources (Crocker *et al*., 1984);

(b) knowledge may be split into subjective and objective categories, with a preference for objective knowledge (Harrison *et al*., 2016).

Research on the impact of device affordance and habits on the victimisation of online fraud is still in its infancy. According to earlier research, heuristic processing is aided by smartphones with big screens and video modes, whereas systematic processing is aided by smartphones with small screens and text modes (Kim & Sundar, 2015). Nonetheless, Vishwanath (2016) proposed that rather than altering cognitive processes, mobile technologies like smartphones reinforce habits, which may increase the vulnerability of fraud victims. This calls for a closer look at the issue of whether habits influence information processing processes. This research is incomplete and needs to be improved in terms of online fraud.

Measures of the heuristic-analytic processing mode, influencing factors and the likelihood of internet fraud victimisation

Although there exist scales to measure the heuristic and systematic processing modes (including attention and elaboration), the validity and reliability of the scales employed were not documented. The dynamics of gathering data were majorly through participant experience, attention span, loss when making poor judgements, and more (Jones & Towse, 2018; Gao, 2021).

Second, users' susceptibility to online fraud is measured by two factors: whether they click on links in phishing emails (Luo *et al*., 2013; Harrison *et al*., 2016) and whether they divulge the private information requested in phishing emails (Wang *et*

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

al., 2012). However, these factors are not the same as being deceived in the end. Third, rather than actual victims, the experiment subjects were regular individuals (Vishwanath *et al*., 2011). When actual victims are utilised as subjects, self-report bias may still exist, but in this case, the affecting elements are more realistic and objective.

Defence strategies under the HSM

Previous defensive methods in the non-HSM framework concentrated on two areas: technology and education, in contrast to the solutions put out in the literature that are included in our research. Though traditional technology emphasises internet fraud information blocking from the government, internet providers, shopping, and other related websites, defence technology for online fraud is more prominent in the HSM framework, helping potential victims to initiate the systematic processing mode. Huang *et al*. (2022), for instance, created a human-technical solution that produces adaptive visual aids (ADVERT) to focus the user's attention on the email content rather than on unimportant details. Researchers have suggested virtual scenario training as a way to teach while still emphasising the value of knowledge and experience (Kumaraguru *et al*., 2007; Sheng *et al*., 2007).

According to Williams and Noyes (2007), network users can enhance their perception of network risk and self-efficacy and avoid the cognitive load associated with extensive publicity and education by immersing themselves in a simulated network fraud environment through lifelike interaction that provides relevant anti-fraud knowledge and experiences it more actively, intuitively, and vividly. Simulated scenario training is not without its problems, though.

For instance, when phishing simulations are employed, subjects who reply to emails could experience embarrassment and distress as they exhibit the same susceptibility as actual victims (Jones *et al*., 2015). Some academics have proposed that after a certain amount of time, participants should undertake the online fraud attack test and engage in the simulation scenario in an educated manner. These issues might still arise, though, if individuals are put through an online fraud attack test after forgetting they signed up, and providing participants with complete information will lessen the likelihood that they would reply (Mack, 2014). Consequently, it will be essential to enhance the simulation method, the simulation scenario, and the simulation's educational impact in the future.

5. Conclusion

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

The two decision-making and reasoning systems are still in the early phases of explanation. These two systems suggest that victims of online fraud may have a connection to the weaknesses of humans in decision-making. When people handle information about online fraud using the heuristic processing mode, they may make themselves more vulnerable to victimisation. The defensive strategy under the HSM states that immersive simulated training and technological applications that draw users' attention to email content might potentially lead to a significant advancement in the fight against online fraud in the future. Nevertheless, to anticipate network fraud victimisation, the explanatory mechanism and influencing elements, as well as the verification of the heuristic and analytical processing modes, must be further explored.

Funding

This research received no external funding.

Conflicts of Interest

The author declare no conflict of interest.

References

Aarts, H., Verplanken, B., and Van Knippenberg, A. (1998). Predicting behaviour from actions in the past: repeated decision-making or a matter of habit? *J. Appl. Soc. Psychol.* 28, 1355-1374. doi: 10.1111/j.1559-1816.1998.tb01681.x

Aderinto, A. A., and Ojedokun, U. A. (2017). The cyber underground economy in Nigeria. In P. Ndubueze (Ed.), *Cyber criminology and technology-assisted crime control: A reader* (pp. 219-228). Ahmadu Bello University Press, Limited, Zaria.

Adesina, O. S. (2017). Cybercrime and poverty in Nigeria. *Canadian Social Science, 13*(4), 19-29.

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

Ajayi, T. M. (2019). Anti-language, slang and cyber scam subculture among urban youth in southwestern Nigeria. *International Journal of Cyber Criminology, 13*(2), 511-533.

Akers, R. L., and Jennings, W. G. (2016). Social learning theory. *The handbook of criminological theory*, 230-240.

Akers, R. L., and Sellers, C. S. (2013). *Criminological theories: Introduction, evaluation, and application* (6th edition). New York: Oxford University Press.

Akinloye, D. N. (2024a). Grandparent-Grandchild Communication: Synthesis of Integrative Model. Psychology Nexus, 1(1), 1-15

Akinloye, D. N. (2024b). Communication and Online Platforms: Pitfalls, Possibilities, and Pressures. Texas Tech University. Ttu-ir.tdl.org

Akinloye, D. N. (2025). Communication Pattern and the Influence of Social Media Contents on Young Adults' Wellbeing in Texas, United States of America. Journal of Communication, 6(2), 1-22.

Aleroud, A., and Zhou, L. (2017). Phishing environments, techniques, and countermeasures: a survey. *Comput. Secure.* 68, 160-196. doi: 10.1016/j.cose.2017.04.006

Alseadoon, I., Chan, T., Foo, E., and Gonzalez Nieto, J. (2012). Who is more susceptible to phishing emails?: A Saudi Arabian study. ACIS 2012 Proceedings, 21. Available at: https://aisel.aisnet.org/acis2012/21

Anderson, K. B. (2004). *Consumer fraud in the United States: An FTC survey*. Washington, DC: Federal Trade Commission.

Anderson, K. B. (2013). *Consumer fraud in the United States, 2011: The third FTC survey*. Washington, DC: Federal Trade Commission.

Ariely, D., Bracha, A., and Meier, S. (2009). Doing good or doing well? Image motivation and monetary incentives in behaving prosocially. *Am. Econ. Rev.* 99, 544-555. doi: 10.1257/aer.99.1.544

Ashton, M. C., and Lee, K. (2009). The HEXACO-60: a short measure of the major dimensions of personality. *J. Pers. Assess.* 91, 340-345. doi: 10.1080/00223890902935878

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

Bargh, J. A., and Gollwitzer, P. M. (1994). "Environmental control of goal-directed action: automatic and strategic contingencies between situations and behaviour," in *Integrative views of motivation, cognition, and emotion*. eds. W. D. Spaulding and H. A. Simon (London, LON: University of Nebraska Press), 71-124.

Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., and Hartel, P. H. (2015). The persuasion and security awareness experiment: reducing the success of social engineering attacks. *J. Exp. Criminology.* 11, 97-115. doi: 10.1007/s11292-014-9222-7

Buller, D. B., and Burgoon, J. K. (1996). Interpersonal deception theory. *Commun. Theory,* 6, 203-242. doi: 10.1111/j.1468-2885.1996.tb00127.x

Burnes, D., Henderson, C. R. Jr., Sheppard, C., Zhao, R., Pillemer, K., and Lachs, M. S. (2017). Prevalence of financial fraud and scams among older adults in the United States: a systematic review and meta-analysis. *Am. J. Public Health* 107, e13-e21. doi: 10.2105/AJPH.2017.303821

Burnes, D., Sheppard, C., Henderson, C. R. Jr., Wassel, M., Cope, R., Barber, C. (2019). Interventions to reduce ageism against older adults: a systematic review and meta-analysis. *Am. J. Public Health* 109, e1-e9. doi: 10.2105/AJPH.2019.305123

Button, M., Lewis, C., and Tapley, J. (2009). *Fraud typologies and the victims of fraud: A literature review*. London: National Fraud Authority.

Button, M., McNaughton Nicholls, C., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. Australian & New Zealand Journal of Criminology, 47(3), 391-408. https://doi.org/10.1177/0004865814521224

Carcach, C., Graycar, A., and Muscat, G. (2001). *The victimisation of older Australians* (Vol. *212*). Canberra, Australia: Australian Institute of Criminology.

Chaiken, S. (1980). Heuristic versus systematic information processing and the use of source versus message cues in persuasion. *J. Pers. Soc. Psychol.* 39, 752-766. doi:10.1037/0022-3514.39.5.752

Chaiken, S. (1987). "The heuristic model of persuasion," in *Social influence: The Ontario symposium*, vol. *5*. eds. M. P. Zanna, J. M. Olson and C. P. Herman (Hillsdale, NJ: Psychology Press), 3-39.

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

Chen, S., and Chaiken, S. (1999). "The heuristic-systematic model in its broader context" in *Dual-process theories in social psychology*. eds. S. Chaiken and Y. Trope (New York, NY: The Guilford Press), 73-96.

Chen, Y., and Yang, Y. (2022). An advanced deep attention collaborative mechanism for secure educational email services. *Comput. Intell. Neurosci.* 2022, 1-9. doi: 10.1155/2022/3150626

Cheung, M. W. L., and Vijayakumar, R. (2016). A guide to conducting a meta-analysis. *Neuropsychol. Rev.* 26, 121-128. doi: 10.1007/s11065-016-9319-z

Cho, J. H., Cam, H., and Oltramari, A. (2016). "Effect of personality traits on trust and risk to phishing vulnerability: Modeling and analysis," in *2016 IEEE International Multidisciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, 7-13.

Cialdini, R. B. (2018). Influence: the psychology of persuasion. *Gyan Manag. J.* 12, 69-70.

Cohen, L. E., and Felson, M. (2010). "Social change and crime rate trends: a routine activity approach (1979)," in *Classics in environmental criminology*. eds. M. A. Andresen, P. J. Brantingham and J. B. Kinney (New York, NY: Routledge), 203-232.

Cohen, L. E., Kluegel, J. R., and Land, K. C. (1981). Social inequality and predatory criminal victimization: An exposition and test of a formal theory. *Am. Sociology Rev.* 505-524. doi: 10.2307/2094935

Crocker, J., Fiske, S. T., and Taylor, S. E. (1984). "Schematic bases of belief change," in *Attitudinal judgment*. ed. J. Richard Eiser (New York, NY: Springer), 197-226.

Das, E. H., De Wit, J. B., and Stroebe, W. (2003). Fear appeals motivate acceptance of action recommendations: evidence for a positive bias in the processing of persuasive messages. *Personal. Soc. Psychol. Bull.* 29, 650-664. doi: 10.1177/0146167203029005009

Drolet, A. L., and Morrison, D. G. (2001). Do we need multiple-item measures in service research? *J. Serv. Res.* 3, 196-204. doi: 10.1177/109467050133001

Eagly, A. H., and Chaiken, S. (1993). *The psychology of attitudes*. Fort Worth, TX: Harcourt Brace Jovanovich College Publishers.

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

Epley, N., and Gilovich, T. (2004). Are adjustments insufficient? *Personal. Soc. Psychol. Bull.* 30, 447-460. doi: 10.1177/0146167203261889

Evans, J. S. B. (2003). In two minds: dual-process accounts of reasoning. *Trends Cogn. Sci.* 7, 454-459. doi: 10.1016/j.tics.2003.08.012

Eveland, W. P. Jr., and Dunwoody, S. (2002). An investigation of elaboration and selective scanning as mediators of learning from the web versus print. *J. Broadcast. Electron. Media* 46, 34-53. doi: 10.1207/s15506878jobem4601_3

Eveland, W. P. Jr., Shah, D. V., and Kwak, N. (2003). Assessing causality in the cognitive mediation model: a panel study of motivations, information processing, and learning during campaign 2000. *Commun. Res.* 30, 359-386. doi: 10.1177/0093650203253369

Everard, A., and Galletta, D. F. (2005). How presentation flaws affect perceived site quality, trust, and intention to purchase from an online store. *J. Manag. Inf. Syst.* 22, 56-95. doi: 10.2753/MIS0742-1222220303

Falola, T., and Heaton, M. M. (2008). A History of Nigeria. Cambridge, UK: Cambridge

University Press.

Feeley, T. H., de Turck, M. A., and Young, M. J. (1995). Baseline familiarity in lie detection. *Commun. Res. Rep.* 12, 160-169. doi: 10.1080/08824099509362052

Fischer, P., Schulz-Hardt, S., and Frey, D. (2008). Selective exposure and information quantity: how different information quantities moderate decision makers' preference for consistent and inconsistent information. *J. Pers. Soc. Psychol.* 94, 231-244. doi:10.1037/0022-3514.94.2.94.2.231

Forgas, J. P., and East, R. (2008). On being happy and gullible: mood effects on scepticism and the detection of deception. *J. Exp. Soc. Psychol.* 44, 1362-1367. doi: 10.1016/j.jesp.2008.04.010

Frauenstein, E. D., and Flowerday, S. (2020). Susceptibility to phishing on social network sites: a personality information processing model. *Comput. Security,* 94:101862. doi: 10.1016/j.cose.2020.101862

Frey, D. (1986). Recent research on selective exposure to information. *Adv. Exp. Soc. Psychol.* 19, 41-80. doi: 10.1016/S0065-2601(08)60212-9

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

Gao, Y. (2021). Influencing factors of college Students' susceptibility to online fraud. Master's thesis. Zhejiang University. Available at: https://kns.cnki.net/KCMS/detail/detail.aspx?dbname=CMFD202102andfifilename=1021610212.nh

Gavett, B. E., Zhao, R., John, S. E., Bussell, C. A., Roberts, J. R., and Yue, C. (2017). Phishing suspiciousness in older and younger adults: the role of executive functioning. *PLoS One* 12:e0171620. doi: 10.1371/journal.pone.0171620

Gigerenzer, G. (1996). On narrow norms and vague heuristics: a reply to Kahneman and Tversky. *Psychol. Rev.* 103, 592-596. doi: 10.1037/0033-295X.103.3.592

Gigerenzer, G. (2008a). Why heuristics work. *Perspect. Psychol. Sci.* 3, 20-29. doi:10.1111/j.1745-6916.2008.00058.x

Gigerenzer, G. (2008b). "Moral intuition=fast and frugal heuristics?" in *Moral psychology*. ed. W. E. Sinnott-Armstrong (Cambridge, MA: MIT Press), 1-26.

Gigerenzer, G., and Gaissmaier, W. (2011). Heuristic decision-making. *Annu. Rev. Psychol.* 62, 451-482. doi: 10.1146/annurev-psych-120709-145346

Gigerenzer, G., Hoffrage, U., and Goldstein, D. G. (2008). Fast and frugal heuristics are plausible models of cognition: reply to Dougherty, Franco-Watkins, and Thomas (2008). *Psychol. Rev.* 115, 230-239. doi: 10.1037/0033-295X.115.1.230

Goldstein, D. G., and Gigerenzer, G. (2002). Models of ecological rationality: the recognition heuristic. *Psychol. Rev.* 109, 75-90. doi: 10.1037/0033-295x.109.1.75

Grazioli, S. (2004). Where did they go wrong? An analysis of the failure of knowledgeable internet consumers to detect deception over the internet. *Group Decis. Negot.* 13, 149-172. doi: 10.1023/B:GRUP.0000021839.04093.5d

Grazioli, S., and Wang, A. (2001). "Looking without seeing: understanding unsophisticated consumers' success and failure to detect internet deception." in *ICIS 2001 Proceedings*. 23, 193-204. Available at: https://aisel.aisnet.org/icis

Griffin, R. J., Neuwirth, K., Giese, J., and Dunwoody, S. (2002). Linking the heuristic systematic model and depth of processing. *Commun. Res.* 29, 705-732. doi:10.1177/009365002237833

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

Grothmann, T., and Reusswig, F. (2006). People at risk of flooding: why some residents take precautionary action while others do not. *Nat. Hazards* 38, 101-120. doi: 10.1007/s11069-005-8604-6

Harrison, B., Vishwanath, A., and Rao, R. (2016). "A user-centred approach to phishing susceptibility: the role of a suspicious personality in protecting against phishing." in *2016 49th Hawaii International Conference on System Sciences (HICSS)*. pp. 5628-5634. IEEE.

Holt, T. J., Burruss, G. W., and Bossler, A. M. (2012). Social learning and cyber deviance: Examining the importance of a full social learning model in the virtual world. *Journal of Crime and Justice*, *33*(2), 31-61.

Holtfreter, K., Reisig, M. D., and Blomberg, T. G. (2006). Consumer fraud victimization in Florida: an empirical study. *St. Thomas L. Rev.* 18, 761-789.

Holtfreter, K., Reisig, M. D., and Pratt, T. C. (2008). Low self-control, routine activities, and fraud victimization. *Criminology* 46, 189-220. doi: 10.1111/j.1745-9125.2008.00101.x

Huang, L., Jia, S., Balcetis, E., and Zhu, Q. (2022). Advert: an adaptive and data-driven attention enhancement mechanism for phishing prevention. *IEEE Trans. Inf. Forensics Secur.* 17, 2585-2597. doi: 10.1109/TIFS.2022.3189530

Ilugbami, O. J., Omigbodun, O. T., Edim, E., Gbadegesin, A. A., & Odeyinka, Y. V. (2025). Cybercrime and Cyber-Security in Nigeria. Management Analytics and Social Insights, 2(3), 230-244.

Jakobsson, M. (2007). The human factor in phishing. *Priv. Sec. Cons. Info.* 7, 1-19.

James, B. D., Boyle, P. A., and Bennett, D. A. (2014). Correlates of susceptibility to scams in older adults without dementia. *J. Elder Abuse Negl.* 26, 107-122. doi: 10.1080/08946566.2013.821809

Jarvenpaa, S. L., Tractinsky, N., and Vitale, M. (2000). Consumer trust in an internet store. *Inf. Technol. Manag.* 1, 45-71. doi: 10.1023/A:1019104520776

Jegede, A. E., Elegbeleye, A. O., Olowookere, E. I., and Olorunyomi, B. R. (2016). Gendered alternative to cyber fraud participation: An assessment of technologically driven crime in Lagos State, Nigeria. *Gender and Behavior, 14*(3), 7672-7692.

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

Jegede, A. E. and Olowookere I. E. (2014). Cyber risks and fraud in Nigeria's business environment: A postmortem of youth crime: *Journal of Social and Development Sciences, 5*(4), 258-265.

Jegede, A. E., Olowookeere, I. E., and Elegbeleye, A. O. (2016). Youth identity, peer influence and internet crime participation in Nigeria: A reflection. *IFE PsychologIA: An International Journal, 24*(1), 37-47.

John, O. P., and Srivastava, S. (1999). "The big-five trait taxonomy: History, measurement, and theoretical perspectives," in *Handbook of Personality: Theory and Research*. eds. L. A. Pervin and O. P. John (New York, NY: Guilford Press.), 102-138.

Johnson, P. E., Grazioli, S., Jamal, K., and Berryman, R. G. (2001). Detecting deception: adversarial problem-solving in a low base-rate world. *Cogn. Sci.* 25, 355-392. doi: 10.1207/s15516709cog2503_2

Johnson, P. E., Grazioli, S., Jamal, K., and Zualkernan, I. A. (1992). Success and failure in expert reasoning. *Organ. Behav. Hum. Decis. Process.* 53, 173-203. doi:10.1016/0749-5978(92)90061-b

Jones, H. S., and Towse, J. (2018). "Examinations of email fraud susceptibility: perspectives from academic research and industry practice," in *Psychological and Behavioural Examinations in Cyber Security*. eds. J. McAlaney, L. A. Frumkin and V. Benson (Pennsylvania, PA: IGI Global), 80-97.

Jones, H. S., Towse, J. N., and Race, N. (2015). Susceptibility to email fraud: a review of psychological perspectives, data-collection methods, and ethical considerations. *Int. J. Cyber Behav. Psychol. Learn.* 5, 13-29. doi: 10.4018/IJCBPL.2015070102

Judges, R. A., Gallant, S. N., Yang, L., and Lee, K. (2017). The role of cognition, personality, and trust in fraud victimization in older adults. *Front. Psychol.* 8:588. doi:10.3389/fps.2017.00588

Kim, K. J., and Sundar, S. S. (2015). Mobile persuasion: can screen size and presentation mode make a difference in trust? *Hum. Commun. Res.* 42, 45-70. doi: 10.1111/hcre.12064

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., and Nunge, E. (2007). "Protecting people from phishing: the design and evaluation of an

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

embedded training email system." in *Proceedings of the SIGCHI conference on human factors in computing systems*. pp. 905-914.

Langenderfer, J., and Shimp, T. A. (2001). Consumer vulnerability to scams, swindles, and fraud: a new theory of visceral influences on persuasion. *Psychol. Mark.* 18, 763-783. doi: 10.1002/mar.1029

Larcom, G., and Elbirt, A. J. (2006). Gone phishing. *IEEE Technol. Soc. Mag.* 25, 52-55. doi: 10.1109/MTAS.2006.1700023

LaRose, R., and Eastin, M. S. (2004). A social cognitive theory of internet uses and gratifications: toward a new model of media attendance. *J. Broadcast. Electron. Media* 48, 358-377. doi:10.1207/s15506878jobem4803_2

Lazarus, S. (2018). Birds of a feather flock together: The Nigerian cyber fraudsters (Yahoo Boys) and hip hop artists. Criminology, Criminal Justice, Law & Society, 19(2), 63-80.

Levine, T. R., and McCornack, S. A. (1991). The dark side of trust: conceptualizing and measuring types of communicative suspicion. *Commun. Q.* 39, 325-340. doi:10.1080/01463379109369809

Liu, Y. F. (2009). Fast and frugal heuristics: the related debates and brief comments. *Adv. Psychol. Sci.* 17, 885-892.

Loewenstein, G. (1996). Out of control: visceral influences on behaviour. *Organ. Behav. Hum. Decis. Process.* 65, 272-292. doi: 10.1006/obhd.1996.0028

Luo, X. R., Zhang, W., Burd, S., and Seazzu, A. (2013). Investigating phishing victimization with the heuristic-systematic model: a theoretical framework and an exploration. *Comput. Security* 38, 28-38. doi: 10.1016/j.cose.2012.12.003

Lyons, J. B., Stokes, C. K., Eschleman, K. J., Alarcon, G. M., and Barelka, A. J. (2011). Trustworthiness and IT suspicion: an evaluation of the nomological network. *Hum. Factors* 53, 219-229. doi:10.1177/0018720811406726

Mack, S. (2014). *Reasoning and judgements are made in an online capacity. An exploration of how phishing emails influence decision-making strategies unpublished dissertation*. Lancaster University, Lancaster, UK.

Makinde, T. (2005) Problems of policy implementation in developing nations: The Nigerian experience. *Journal of Social Sciences, 11*(1), 63-69.

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

Malhotra, N. K., Kim, S. S., and Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. *Inf. Syst. Res.* 15, 336-355. doi: 10.1287/isre.1040.0032

McKnight, D. H., Kacmar, C., and Choudhury, V. (2003). "Whoops- did I use the wrong construct to predict e-commerce trust? Modelling the risk-related effects of trust versus distrust concepts." in *Proceeding of the thirty-sixth Hawaii international conference on social systems*.

McKnight, D. H., Kacmar, C. J., and Choudhury, V. (2004). Dispositional trust and distrust distinctions in predicting high-and low-risk internet expert advice site perceptions. *E-Service* 3, 35-58. doi: 10.2979/esj.2004.3.2.35

Merton, R. (1968). *Social theory and social structure.* Simon and Schuster: New York

Modic, D., Anderson, R., and Palomäki, J. (2018). We will make you like our research: the development of a susceptibility-to-persuasion scale. *PLoS One* 13:e0194119. doi: 10.1371/journal.pone.0194119

Modic, D., and Lea, S. E. (2012). How neurotic are scam victims? The Big Five and Internet scams. 2448130.

Modic, D., and Lea, S. E. (2013). Scam compliance and the psychology of persuasion. 2364464.

Moher, D., Liberati, A., Tetzlaff, J., and Altman, D. G.PRISMA Group* (2009). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *Ann. Intern. Med.* 151, 264-269. doi: 10.7326/0003-4819-151-4-200908180-00135

Moody, G. D., Galletta, D. F., and Dunn, B. K. (2017). Which phish gets caught? An exploratory study of individuals' susceptibility to phishing. *Eur. J. Inf. Syst.* 26, 564-584. doi: 10.1057/s41303-017-0058-x

Moshman, D. (2000). Diversity in reasoning and rationality: metacognitive and developmental considerations. *Behav. Brain Sci.* 23, 689-690. doi: 10.1017/S0140525X00483433

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

Muncaster, P. (2020). # COVID-19 drives phishing emails up 667% in under a month. Infosecurity Magazine. Online. Available at: https://www.infosecurity-magazine.com/news/covid19-drive-phishing-emails-667/

Muraina, M. B, and Muraina, K. O. (2015). Peer pressure, parental socioeconomic status, and cybercrime habit among university undergraduates in Southwestern Nigeria. *International Journal of Technology in Teaching and Learning, 11*(1), 50-59.

Norris, G., Brookes, A., and Dowell, D. (2019). The psychology of internet fraud victimization: a systematic review. *J. Police Crim. Psychol.* 34, 231-245. doi: 10.1007/s11896-019-09334-5

Ndubueze, P. N. (2013). Social values and the yahooboys' subculture in Nigeria: Towards a paradigm shift for national value re-orientation. The Nigerian Journal of Sociology and Anthropology, 11(1), 101-114.

Ogunleye, Y. O., Ojedokun, U. A., and Aderinto, A. A. (2019). Pathways and motivations for cyber fraud involvement among female undergraduates of selected universities in south-west Nigeria. *International Journal of Cyber Criminology, 13*(2), 309-325.

Ojedokun, U. A. (2010). *Cybercrime and changing lifestyle among students of some selected universities in southwestern Nigeria* (Unpublished master's thesis). University of Ibadan, Ibadan, Nigeria.

Ojedokun, U. A., and Eraye, M. C. (2012). Socioeconomic lifestyles of the yahoo-boys: A study of perceptions of university students in Nigeria. *International Journal of Cyber Criminology, 6*(2), 1001-1013.

Okeshola F.B. and Adeta A.K, (2013) The nature, causes and consequences of cybercrime in Tertiary Institutions in Zaria-Kaduna State, Nigeria *American International Journal of Contemporary Research, 3*(9), 98-114.

Oladimeji, R. (2019). Cyber fraud: Court orders Invictus Obi's 280m forfeited. *The Punch*. Available at: https://www.punchng.com/cyber-fraud-court-orders-invictus-obis-n280m-forfeited/

Omigbodun, T. O., & Akinloye, D. N. (2026). Context and Application of Agnew's General Strain Theory to Explain Crime. Journal of International Review of Research Studies, 1(06), 1-11. https://doi.org/10.66104/s04mz37

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

Perse, E. M. (1990). Audience selectivity and involvement in the newer media environment. *Commun. Res.* 17, 675-697. doi: 10.1177/009365090017005005

Petty, R. E., and Briñol, P. (2014). Emotion and persuasion: cognitive and meta-cognitive processes impact attitudes. *Cognit. Emot.* 29, 1-26. doi: 10.1080/02699931.2014.967183

Petty, R. E., and Cacioppo, J. T. (1986). "The elaboration likelihood model of persuasion," in *Communication and persuasion*. eds. R. E. Petty and J. T. Cacioppo (New York, NY: Springer), 1-24.

Petty, R. E., Cacioppo, J. T., and Goldman, R. (1981). Personal involvement as a determinant of argument-based persuasion. *J. Pers. Soc. Psychol.* 41, 847-855. doi: 10.1037/0022-3514.41.5.847

Petty, R. E., and Wegener, D. T. (1999). "The elaboration likelihood model," in *Current status and controversies in dual-process theories in social psychology*. eds. S. Chaiken and Y. Trope (New York, NY: Guilford Press), 37-72.

Ratneshwar, S., and Chaiken, S. (1991). Comprehension's role in persuasion: the case of its moderating effect on the persuasive impact of source cues. *J. Consum. Res.* 18, 52-62. doi: 10.1086/209240

Ross, L. (1981). "The "intuitive scientist" formulation and its developmental implications" in *Social cognitive development: Frontiers and possible futures*. eds. J. H. Flavell and L. Ross (London and New York: Cambridge University Press)

Rothstein, H. G. (1986). The effects of time pressure on judgment in multiple cue probability learning. *Organ. Behav. Hum. Decis. Process.* 37, 83-92. doi:10.1016/0749-5978(86)90045-2

Salthouse, T. (2012). Consequences of age-related cognitive declines. *Annu. Rev. Psychol.* 63, 201-226. doi: 10.1146/annurev-psych-120710-100328

Schemer, C., Matthes, J., and Wirth, W. (2008). Toward improving the validity and reliability of media information processing measures in surveys. *Commun. Methods Meas.* 2, 193-225. doi: 10.1080/19312450802310474

Schonfeld, I. S., and Chang, C. H. (2017). *Occupational health psychology: Work, stress, and health*. eds. D. Wang and Y. Hu (Trans. Shanghai: East China Normal University Press).

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

Schwarz, N., Frey, D., and Kumpf, M. (1980). Interactive effects of writing and reading a persuasive essay on attitude change and selective exposure. *J. Exp. Soc. Psychol.* 16, 1-17. doi: 10.1016/0022-1031(80)90032-3

Seodotcom. (2011). The History of Search [infographic]. Retrieved May 15, 2013, from

http://www.seo.com/blog/history-search-infographic/

Shah, D. V., Kwak, N., Schmierbach, M., and Zubric, J. (2004). The interplay of news frames on cognitive complexity. *Hum. Commun. Res.* 30, 102-120. doi: 10.1111/j.1468-2958.2004.tb00726.x

Shang, Y., Wu, Z., Du, X., Jiang, Y., Ma, B., and Chi, M. (2022). The psychology of the internet fraud victimization of older adults: a systematic review. *Front. Psychol.* 13:912242. doi:10.3389/fpsyg.2022.912242

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., *et al*. (2007). "Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish." *in Proceedings of the 3rd symposium on usable privacy and security*. pp. 88-99.

Simmons, J. P., and Nelson, L. D. (2006). Intuitive confidence: choosing between intuitive and nonintuitive alternatives. *J. Exp. Psychol. Gen.* 135, 409-428. doi: 10.1037/0096-3445.135.3.409

Sloman, S. A. (1996). The empirical case for two systems of reasoning. *Psychol. Bull.* 119, 3-22. doi: 10.1037/0033-2909.119.1.3

Smith, D. J. (2007). A Culture of Corruption: Everyday Deception and Popular Discontent in

Nigeria. Princeton, NJ: Princeton University Press.

Stamm, K., and Dube, R. (1994). The relationship of attitudinal components to trust in media. *Commun. Res.* 21, 105-123. doi: 10.1177/009365094021001006

Sundar, S. S. (2008). *The MAIN model: A heuristic approach to understanding technology effects on credibility* (pp. 73-100). Cambridge, MA: Mac Arthur Foundation Digital Media and Learning Initiative.

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

Sundar, S. S., Knobloch-Westerwick, S., and Hastall, M. R. (2007). News cues: information scent and cognitive heuristics. *J. Am. Soc. Inf. Sci. Technol.* 58, 366-378. doi:10.1002/asi.20511

Tade, O. (2013). A spiritual dimension to cybercrime in Nigeria: The Yahoo-plus phenomenon. *Human Affairs, 23*(4), 689-705.

Tade, O. and Aliyu (2011) Social organization of internet fraud among university undergraduates in Nigeria. *International Journal of Cyber Criminology, 5*(2), 860-875.

The Nigerian Communications Commission. (2013). Subscriber Data. Available at http://www.ncc.gov.ng/index.php?option=com_contentandid=125andItemid=73

This Day. (2016). Nigeria loses over N127bn annually through cybercrime. Retrieved from www.thisdaylive.com/index.php/2016/04/18/cyber-security-Nigeria-loses-over-n127bn-annually-through-cybercrime/

Toma, C. L., and Hancock, J. T. (2012). What lies beneath the linguistic traces of deception in online dating profiles? *J. Commun.* 62, 78-97. doi: 10.1111/j.1460-2466.2011.01619.x

Trumbo, C. W. (2002). Information processing and risk perception: an adaptation of the heuristic-systematic model. *J. Commun.* 52, 367-382. doi: 10.1093/joc/52.2.367

United States Department of Justice (2017). Lithuanian man arrested for theft of over $100 million in fraudulent email compromise scheme against multinational internet companies [Press release]. Available at: https://www.justice.gov/usao-sdny/pr/lithuanianman-arrested-theft-over-100-million-fraudulent-email-compromise-scheme

Valecha, R., Mandaokar, P., and Rao, H. R. (2022). Phishing email detection using persuasion cues. *IEEE Trans. Dependable Secure Comput.* 19, 1-756. doi: 10.1109/TDSC.2021.3118931

Verizon. (2019). 2019 data breach investigations report (DBIR). Available at: https://enterprise.verizon.com/resources/reports/2019-data-breach investigations-report.pdf

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

Verplanken, B., and Orbell, S. (2003). Reflections on past behaviour: a self-report index of habit strength. *J. Appl. Soc. Psychol.* 33, 1313-1330. doi: 10.1111/j.1559-1816.2003.tb01951.x

Vishwanath, A. (2015). Habitual Facebook use and its impact on getting deceived on social media. *J. Comput.-Mediat. Commun.* 20, 83-98. doi: 10.1111/jcc4.12100

Vishwanath, A. (2016). Mobile device affordance: explicating how smartphones influence the outcome of phishing attacks. *Comput. Hum. Behav.* 63, 198-207. doi: 10.1016/j.chb.2016.05.035

Vishwanath, A., Harrison, B., and Ng, Y. J. (2016). Suspicion, cognition, and automaticity model of phishing susceptibility. *Commun. Res.* 45, 1146-1166. doi:10.1177/0093650215627483

Vishwanath, A., Herath, T., Chen, R., Wang, J., and Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decis. Support. Syst.* 51, 576-586. doi: 10.1016/j.dss.2011.03.002

Wall, A. (2013). History of Search Engines: From 1945 to Google Today. Available at: http://www.searchenginehistory.com/

Wang, J., Herath, T., Chen, R., Vishwanath, A., and Rao, H. R. (2012). Research article phishing susceptibility: an investigation into the processing of a targeted spear phishing email. *IEEE Trans. Prof. Commun.* 55, 345-362. doi: 10.1109/TPC.2012. 2208392

Watts, S. A., and Zhang, W. (2008). Capitalizing on content: information adoption in two online communities. *J. Assoc. Inf. Syst.* 9, 73-94. doi: 10.17705/1jais.00149

Whitty, M. T. (2013). The scammer's persuasive techniques model: development of a stage model to explain the online dating romance scam. *Br. J. Criminol.* 53, 665-684. doi:10.1093/bjc/azt009

Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *J. Financ. Crime* 26, 277-292. doi: 10.1108/JFC-10-2017-0095

Williams, D. J., and Noyes, J. M. (2007). How does our perception of risk influence decision-making? Implications for the design of risk information. *Theor. Issues Ergon. Sci.* 8, 1-35. doi: 10.1080/14639220500484419

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/08/2026 - **Accepted:** 15/09/2026
Vol: 01.05
DOI: 10.66104/czvy6872
Pages: 1-43

Workman, M. (2008). A test of interventions for security threats from social engineering. *Inf. Manag. Comput. Security* 16, 463-483. doi: 10.1108/09685220810920549

Wright, R. T., and Marett, K. (2010). The influence of experiential and dispositional factors in phishing: an empirical investigation of the deceived. *J. Manag. Inf. Syst.* 27, 273-303. doi: 10.2753/MIS0742-1222270111

Author Responsibility Statement

AOO: Conceptualization, Writing - original draft; TJA: Introduction, Literature, Conclusion, Editing; AOA: Conceptualization, Writing - original draft, Editing; CRU: Introduction, Literature, Conclusion, Visualization; ODB: Writing - original draft, Editing. The author read and approved the final manuscript.

CC BY