Scientific Research Publishing

Journal of Information Security, 2026, 17(2), 149-166
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Cyber Deception and Theft: A Critical Review

Paul Danquah, Stephen Bekoe

Council for Scientific and Industrial Research-Institute for Scientific and Technological Information (CSIR-INSTI), Accra, Ghana
Email: pauldanquah@yahoo.com, sbekoe2000@gmail.com

How to cite this paper: Danquah, P. and Bekoe, S. (2026) Cyber Deception and Theft: A Critical Review. *Journal of Information Security*, **17**, 149-166.
https://doi.org/10.4236/jis.2026.172008

Received: February 21, 2026
Accepted: April 17, 2026
Published: April 20, 2026

Abstract

Cyber deception and theft is the utilization of technology to perpetrate deception and enable theft. Theft typically denotes the act of unlawfully appropriating money or property, including credit card information, intellectual property, or digital content. The necessity for cyber deception and theft prevention is escalating, and the increased standardization and optimization of these measures is crucial for enhancing countermeasures. This paper aimed to present optimal mitigation strategies for cyber deception and theft by conducting a complete and systematic review of relevant literature, utilizing the PRISMA paradigm for systematic literature review technique. The results demonstrate that technical controls alone are inadequate for the industry. The incorporation of predictive analytics will yield more proactive preventative models. The results indicate that cyber deception and theft are systemic issues rather than individual incidents, necessitating coordinated, multi-faceted solutions. Comprehensive strategies that include behavioral awareness, multi-tiered security frameworks, forensic capabilities, regulatory alignment, and global cooperation are necessary. The research findings underscore the necessity for standardized risk-of-bias frameworks in cybercrime investigations to improve comparability and methodical synthesis in subsequent evaluations. Mitigation measures are proposed in relation to the identified phases of cyber deception and theft. Ultimately, it is advised that policy must synchronize technical regulation with behavioral risk reduction and international cooperation.

Keywords

Cyber Deception, Cyber Theft, Phishing, Online Fraud, Social Engineering

1. Introduction

Through the evaluation and analysis of the written, physical, and digital behaviours that were present in each attack, [1] research on cybercrime typologies led to the classification of computer and technology-related offences. This classifica-

tion was accomplished through the evaluation and analysis of the behaviours. Furthermore, [2] asserts that examining the intrusion from a criminal perspective is a significant aid to the investigator in appreciating the reasons behind an offender's actions. As a consequence of this, [3] created a taxonomy of cybercrime that included the following three categories: cyber-trespass, cyber-deceptions and theft, cyber-pornography, and cyber violence. Cybertrespass is a type of cybercrime that involves infringing upon the property of other people and/or causing harm to them when they are online. Users are typically authenticated and approved with particular access rights and privileges to resources on systems or networks. Additionally, they are subject to set boundaries. In general, all users are authenticated and authorized. Cyber trespass is the phrase used to describe unauthorized access to resources that are located beyond existing boundaries. Hacking, defacement, and the spread of viruses are all examples of offences that fall under the category of cyber harassment. There is a type of cybercrime known as cyber-deception and theft, which is characterized by the use of technology to commit deception and enable theft. In most cases, theft refers to the act of stealing money or stealing property. This can include acts like stealing credit card information, stealing intellectual property, or stealing music. Cyber-pornography includes activities that contravene laws pertaining to obscenity and decency, which vary from country to jurisdiction; nonetheless, there are fundamental legal principles that are applicable everywhere. One example that is commonly used is child pornography. Inflicting psychological pain or inciting physical harm against others through the use of the internet and other linked technology is cyber violence, which is a violation of laws that are designed to protect personal safety. Hate speech, cyberbullying, and denial-of-service attacks are all examples of various forms of cyber violence [3] [4].

Theft and deceit committed online frequently have socioeconomic repercussions, such as monetary loss, lost time, damage to one's reputation, and a decrease in one's sense of self-worth.

According to the findings of [5], the following are the processes that constitute the modus operandi of socially engineered cyber deception and theft.

1) Attract Attention: The perpetrator sends the victim a message via email, text message, or chat in order to get their attention.

2) Information Collection and Exchange: The perpetrator engages in a process of exchanging information with the potential victim over the course of a certain amount of time.

3) Build Cordial Relationship: The criminal forms a rapport with the victim by persistent contact, which gradually develops into a convivial friendship. The third step is to cultivate a cordial friendship based on this relationship.

4) Establish Trust: Trust is developed after the development of a friendly connection, which can be accomplished through a variety of means. The most common of these methods is the buying of gifts for the victim, as well as the introduction of the victim to close friends and relatives.

5) Trigger a bait/Access Victim: Initiate a lure or gain access to the victim: If the victim has been able to establish trust with the offender, they are more likely to be willing to give the offender with various forms of assistance or concessions.

6) Commit Offense: The sixth step is to carry out the offence, which is often the best time for the perpetrator to begin the assault.

7) Clear Tracks (Optional): Some criminals may disappear from the cyber sphere after the offence, while others continue to exist until their victims are no longer able to benefit from their actions [6].

Theft and deceit on the internet are two of the most significant security concerns of the twenty-first century. At the same time as it has broadened opportunities for economic innovation, the rapid digital transformation of commerce, governance, communication, and financial institutions has also fostered an environment that is conducive to criminal conduct that is driven by technology. In contrast to cyber theft, which refers to the unlawful acquisition of digital assets, credentials, financial resources, or intellectual property through the use of online technologies, cyber deception is the intentional manipulation of information, identities, and communication systems with the intention of misleading victims.

Cyber deception, in contrast to traditional criminal activity, operates within unbounded networks and makes use of anonymity, automation, and scalable attack frameworks. A number of factors, including cognitive biases, reliance on trust, poor authentication procedures, and inherent weaknesses within socio-technical systems, are utilized by those who commit crimes. The economic structure of criminal activity has been transformed because of the combination of social engineering, digital fraud markets, phishing automation, cryptocurrency laundering, and transnational networks. Cyber Fraud Prevention Framework is becoming increasingly necessary and its further standardization and optimization are equally important to make countering more robust and usable [6] [7].

In view of this, the purpose of this work is to provide optimal mitigation measures for cyber deception and theft through a comprehensive and systematic review of cyber deception and theft related literature using the PRISMA paradigm. Within the scope of this review, criminological theory, behavioural research, technical security studies, forensic technique, organizational governance frameworks, and victimological analysis are all incorporated. This analysis conducts a thorough evaluation of the empirical and theoretical contributions made by fourteen, detailed in **Figure 1**, analyses the strengths and limitations of the methodology, and formulates analytical conclusions for the sake of future research, practice and policy formulation.

2. Methodology (PRISMA Systematic Literature)

To guarantee transparency, replicability, and scientific rigour, this study makes use of the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework. Database searches were carried out utilizing combinations of keywords. They were conducted across Scopus, Web of Science, IEEE Xplore, and ACM Digital Library, as well as databases pertaining to criminal justice.

Figure 1. Risk of bias assessment for study.

2.1. Defining the Research Question

The research question (RQ), guided by the SLR process outlined in [5] and recent insights from [8], was as follows. RQ: What are the optimal mitigation measures for cyber deception and theft?

2.2. Keywords and Core Concepts

The keywords defined were "cyber deception," "cyber theft," "phishing," "online fraud," "social engineering," "digital forensics," and "cybercrime theory".

2.3. Search String Development

Keywords were integrated using Boolean operators, wildcards, and controlled vocabulary.

2.4. Subject and Database-Specific Adaptation

The databases searched were Scopus, Web of Science, IEEE Xplore, ACM Digital Library, Criminal Justice Abstracts and Google Scholar (supplementary search). Details are provided below:

Core Cyber Deception String

("cyber deception" OR "online deception" OR "digital deception"

OR "social engineering" OR phishing OR "advance fee fraud"

OR "online fraud" OR "internet scam")

AND

("cyber theft" OR "identity theft" OR "credential theft"

OR “financial fraud” OR “electronic fraud”)
Criminological Theory String
(“cybercrime theory” OR “routine activity theory”
OR “crime opportunity theory” OR “organized fraud”
OR “crime profiling” OR “cybercrime networks”)
AND
(“digital environment” OR cyberspace OR internet)
Behavioral & Psychological Susceptibility String
(“phishing susceptibility” OR “privacy calculus”
OR “cognitive bias” OR “human factors”
OR “user vulnerability” OR “social phishing”)
AND
(“online security” OR “information disclosure” OR “trust online”)
Technical & Forensic Investigation String
(“digital forensics” OR “IP tracing”
OR “spoof detection” OR “authentication security”
OR “cyber investigation” OR “fraud detection systems”)
AND
(“cyber theft” OR phishing OR “online fraud”)
Victimology & Impact String
(“cyber fraud victims” OR “impact of cybercrime”
OR “financial loss online” OR “psychological impact of phishing”)
AND
(“reporting behavior” OR “underreporting” OR “victimization”)

Database-Specific Finalized Search Queries

Scopus/Web of Science
(“cyber deception” OR “cyber fraud” OR “online fraud” OR “phishing”
OR “social engineering” OR “cyber theft” OR “advance fee fraud”)
AND (detection OR mitigation OR prevention OR susceptibility OR “crime analysis”)
AND (LIMIT-TO (LANGUAGE, “English”))
AND (PUBYEAR > 2000)
IEEE Xplore
(“phishing detection” OR “intrusion detection” OR “machine learning”
OR “authentication” OR “digital identity”)
AND (“cyber fraud” OR “cyber theft”)
ACM Digital Library
(“phishing” OR “social engineering”)
AND (“user study” OR “warning effectiveness” OR “susceptibility”)
Google Scholar (Grey Literature & Books)
“cyber fraud prevention framework” OR
“digital identity guidelines” OR
“cybercrime transformation” OR
“organized fraud”

2.5. Inclusion and Exclusion Criteria

For inclusion, the following criteria were considered:

1) Direct relevance to cyber deception or cyber theft.

2) A contribution that was either theoretical, empirical, or technical.

3) A publication in the English language.

4) A source that has been peer-reviewed or published in an academic journal.

The criteria for exclusion included duplicate records, cyber offences that were unrelated to the topic at hand, criticism that was entirely based on opinion, and internet content that could not be verified.

2.6. Search Execution and Results

A systematic filtering was achieved as a result of the PRISMA process, which began with identification and continued through screening, eligibility, and the final inclusion stages. The details are outlined in Table 1 below.

Table 1. PRISMA flow.

Stage	Number of Records
Identification: Records identified through database searching	n = 188
Screening: Records after duplicates removed	n = 150
Eligibility: Full-text articles assessed	n = 82
Included: Studies included in qualitative synthesis	n = 14

2.7. Search Date Range

Search period covered (publication years): 2001-2025.

Search execution date: 15-29 February 2026.

The range was selected to capture foundational cybercrime theory (early 2000s), the emergence of phishing and social engineering research (mid-2000s), behavioural susceptibility models (2010s), and contemporary fraud prevention frameworks (2020s).

2.8. Selection Process

The screening comprised three phases: 1) Evaluation of title and abstract, 2) Review of introduction and conclusion, 3) Comprehensive text and quality assessment. Twenty-one studies fulfilled the methodological criteria.

2.9. Data Extraction

A systematic spreadsheet documented the metadata, findings, methodologies, procedures, deficiencies, aims, and context of each study, facilitating synthesis, gap detection, and quality evaluation.

2.10. Screening and Selection Process of Studies

The screening and selection method adhered to PRISMA 2020 guidelines [9] and

was executed in three systematic phases: title screening, abstract screening, and full-text evaluation. All phases of screening and data extraction were performed by two independent reviewers. Both reviewers possessed previous research experience in cybersecurity and information systems. A third non-author reviewer served as an adjudicator when required.

Screening Process: During the screening of titles and abstracts, each reviewer separately evaluated eligibility according to established inclusion and exclusion criteria (relevance to cyber deception or theft; empirical, theoretical, or technological contribution; English language; publishing between 2001 and 2025). Studies considered irrelevant by both reviewers were eliminated. In cases with ambiguous eligibility, the study advanced to a comprehensive text review.

During the full-text phase, both reviewers separately evaluated methodological rigour, contextual significance, and contributions to detection, prevention, behavioural analysis, or socio-technical mitigation.

Disagreement Resolution: Disputes were initially addressed by organized dialogue between the two evaluators. If consensus was not reached, the third reviewer rendered the ultimate decision. Less than 10% of research necessitated adjudication at the full-text phase.

Data extraction was conducted autonomously via a standardized template, succeeded by cross-verification to guarantee precision and comprehensiveness.

2.11. Risk-of-Bias Assessment

Bias was assessed across five domains via the Cochrane tool. The domains utilized in the evaluation (Selection Bias, Performance Bias, Detection Bias, Reporting Bias, and External Validity) were derived from recognized systematic review and evidence appraisal frameworks frequently employed in health, social science, and transdisciplinary research. Despite the interdisciplinary nature of cyber deception studies encompassing criminology, information systems, and computer science, structured bias areas are relevant for assessing methodological rigour and evidentiary strength [9].

The structure conceptually corresponds with the Cochrane Risk of Bias framework, which assesses selection, performance, detection, and reporting biases in empirical studies [10]. The domains were expanded to encompass External Validity, highlighting the significance of generalizability in cybercrime research, as results frequently rely on jurisdiction, technological context, or demographic sample. This adaptation aligns with PRISMA-guided systematic review protocols that advocate for a transparent evaluation of research quality and bias across diverse evidence categories.

The diagram was created via Matplotlib, a prominent scientific visualization package in Python. Matplotlib facilitates the creation of high-resolution, publication-quality figures and is frequently employed in academic research for systematic review visualizations, statistical graphics, and risk-of-bias plots.

Domains Utilized in the Evaluation:

1) Selection Bias: Evaluates the potential limitations in representativeness due to study samples, case selection, or theoretical framing.

2) Performance Bias: Assesses methodological rigour, the robustness of research design, and the consistency of implementation.

3) Detection Bias: Assesses the reliability and objectivity of result measurement (e.g., experimental controls vs self-reports).

4) Reporting Bias: Assesses the thoroughness of reporting, transparency, and possible selective interpretation.

5) External Validity: Evaluates the generalizability of results across various contexts, populations, or jurisdictions.

Figure 1 shows the traffic light plot indicating low (green), moderate (yellow), high (red), or unclear (blue) bias levels. Figure 2 presents the weighted overall assessment, ensuring transparency and aiding reliability evaluations.

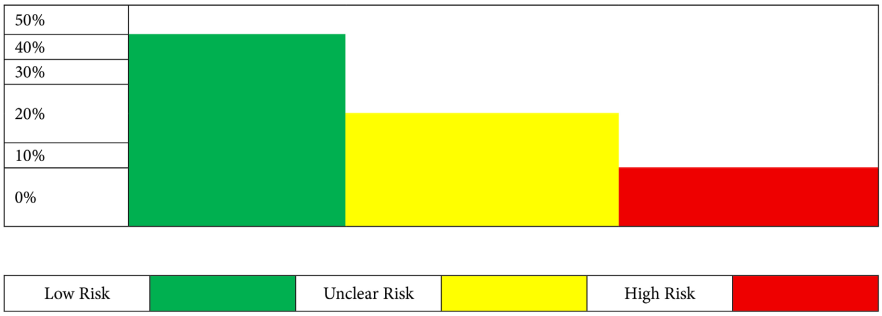

Figure 2. Overall weighted risk-of-bias summary.

3. Results and Discussion

3.1. Results

Foundational Concepts in Criminology:

Within digital ecosystems, motivated offenders, suitable targets, and the absence of capable guardians interact, according to the routine activity theory that has been applied to cyberspace [3]. Despite the fact that technical tools are relatively new, the novelty debate in cybercrime implies that the fundamental motivations and opportunity structures are nonetheless comparable to those commonly associated with traditional criminal activity [3].

The research on fraud organizations sheds light on organized criminal networks that operate on a global scale [11], while the profiling and investigative approaches provide insights into the behavioural patterns of offenders [1] [12].

The cyber fraud marketplaces function as economic ecosystems that are semi-formalized and are driven by scalability and low entry barriers [13].

Susceptibility to social engineering and behavioural manipulation:

Relying primarily on psychological cues such as urgency, authority, and reciprocity, phishing and deception are both forms of social engineering.

The results of experimental studies show that there are measurable demographic differences in phishing susceptibility [14], and the results of social phish-

ing trials reveal that personalisation approaches are effective [15].

In spite of being aware of the potential risks, individuals continue to divulge sensitive information, according to the privacy calculus theory [5].

Perspectives from the Technical and Forensic Fields:

Authentication validation, spoof detection, and encryption protocols are examples of technical defences that continue to be essential components of cyber defence architectures [16] [17]. The use of digital forensic approaches enables attribution through the examination of metadata, the tracking of intellectual property, and the recovery of artefacts [16], which complements investigations into the origins of advance service fraud [18].

Violent Crime and Its Effects:

Cyber fraud results in damage to a company's finances, psychological well-being, and reputation [2]. For a variety of reasons, including stigma and underreporting, victims may endure secondary victimization. On the internet, deception-based offences are classified as a predominant subgroup of online criminal behaviour, according to various taxonomies of internet crime [3].

FS-ISAC [8], were instructive in proposing a peculiar framework for the financial sector with the following five stages as the framework for cyber fraud prevention within the financial sector.

"Phase 1—Recon: The threat actor's passive or active actions to determine their target, collect information, set up infrastructure, and plan for attempted fraud. Recon ends at the entry point into the attack.

Phase 2—Initial Access: The threat actor's actions to gain an initial foothold for fraud against a consumer, financial services institution, or other entity (e.g. third-party vendor or a vendor's sub-service provider).

Phase 3—Positioning: The threat actor's attempts to change and/or collect account information that will be forwarded to the controlled infrastructure.

Phase 4—Execution: Process that converts stolen data to money, typically executed within business procedures that send fraudulent/unauthorized funds to the threat actor.

Phase 5—Monetization: The method of payment in which stolen funds are transferred to the threat actor."

This five-phase framework is applicable to several situations, including application fraud, account takeover, and economic offences such as money laundering and sanctions evasion.

The systematic review demonstrates that cyber deception and theft are best understood as socio-technical crimes operating at the intersection of criminology, behavioral science, and cybersecurity engineering. Five major findings emerge from the combined literature. The systematic review included eighteen fundamental sources across criminology, cybersecurity engineering, behavioural science, digital forensics, and victimology. The results demonstrate that cyber deception and theft function as interconnected socio-technical phenomena rather than solely technological crimes. Five predominant themes emerged from the analyzed

literature: adaption of criminological theory, organizational fraud frameworks, behavioural vulnerability, technology attack vectors, and investigative/forensic responses.

Criminological literature indicates that conventional theoretical paradigms are still relevant in digital environments. Routine activity theory elucidates cyber deception via the intersection of motivated offenders, appropriate online targets, and inadequate digital guardianship. The "novelty" discussion asserts that although cybercrime tools are technologically sophisticated, the fundamental motivations profit, anonymity, and minimal perceived risk reflect traditional criminal behaviour. Systematic fraud investigations further disclose organized, interconnected criminal syndicates utilizing web frameworks for expansive operations.

First, criminological theory remains highly applicable in digital contexts. Routine activity theory explains cyber deception through the convergence of motivated offenders, suitable online targets, and weak digital guardianship structures [19] [20]. This confirms that cybercrime reflects adaptation rather than complete theoretical novelty.

Second, organized and networked fraud structures underpin large-scale cyber theft operations. Fraud is increasingly coordinated, scalable, and transnational, functioning within semi-formalized criminal ecosystems [11] [21]. These structures leverage digital infrastructures to maximize profit while minimizing risk. Behavioural and psychological studies consistently demonstrate that deception primarily succeeds through cognitive exploitation. Research on phishing and social engineering demonstrates that urgency cues, authority framing, personalization, and familiarity markedly enhance compliance. Privacy calculus models indicate that victims do not behave irrationally; rather, they evaluate perceived advantages (convenience, speed, trust) against abstract risks, frequently underestimating the likelihood of threats. This underscores deceit as a tactical adjustment of perceived risk-reward assessments.

Third, technological evaluations identify phishing, spoofing, advance fee fraud, and credential harvesting as prevalent methods of cyber theft. Automation, botnets, anonymization services, and bitcoin laundering augment scalability and diminish criminal traceability. Engineering research prioritizes multi-layered defences, encompassing authentication validation, encryption, spoof detection mechanisms, and zero-trust architectures. Behavioral susceptibility is central to cyber deception success. Social phishing research shows that personalization and social cues significantly increase victim compliance [15]. This supports broader evidence that deception exploits cognitive heuristics such as authority, urgency, and familiarity.

Fourth, privacy calculus theory explains why individuals disclose sensitive information despite awareness of risk [4]. Victims often engage in rational cost–benefit assessments that undervalue abstract security threats relative to perceived convenience or trust.

Fifth, cyber theft generates substantial victim harm extending beyond financial

loss.

Victimological research documents psychological distress, reputational damage, and systemic underreporting [2], highlighting the broader societal impact of deception-based offenses.

Collectively, these findings indicate that cyber deception and theft are sustained by structural opportunity, organized criminal networks, cognitive manipulation, and rationalized risk-taking behaviors. Effective mitigation therefore requires integrated socio-technical responses rather than purely technological countermeasures. The research on digital forensics indicates that attribution and investigation are achievable however intricate. IP tracing, metadata analysis, and artefact reconstruction facilitate investigative endeavours; yet, cross-border jurisdictional issues and anonymization technologies hinder enforcement.

Ultimately, the findings indicate that cyber deception is maintained by a system of behavioural manipulation, technological capabilities, economic motivations, and restricted oversight capacity.

3.2. Discussion

The results affirm that cyber deception and theft should be seen as adaptive, ecosystem-driven phenomena rather than discrete criminal acts. The examined literature indicates a convergence between criminological theory and cybersecurity engineering, implying that successful prevention necessitates interdisciplinary integration. Cyber deception arises not only from technological vulnerabilities but also from the inherent trust entrenched in digital infrastructures.

A crucial observation arising from the synthesis is the importance of human cognition. Although organizations frequently emphasize technology safeguards, evidence indicates that social engineering constantly circumvents just technical defences. Behavioural susceptibility is influenced by urgency framing, authority signalling, and personalization elements that function independently of system architecture. Consequently, preventative systems must encompass more than just firewalls and encryption; they should also integrate behavioural training, enhancements in interface design, and tactics for risk communication.

Below in Table 2 is description of deduced themes and the respective core insights and key contributions with supporting citations.

Table 2. Thematic insights from literature review.

Theme	Core Insight	Key Contributions	Supporting Citations
Criminological Foundations	Cyber deception reflects adaptation of traditional crime theories to digital environments.	Routine activity theory explains offender-target-guardian convergence; profiling supports offender behavioral analysis.	[1] [12] [14] [19]

Continued

Organized Fraud & Criminal Ecosystems	Cyber theft operates within scalable, networked, transnational structures.	Fraud markets function as semi-formalized economic systems with low entry barriers and distributed actors.	[3] [11] [13]
Behavioral Susceptibility & Social Engineering	Deception exploits cognitive biases such as urgency, authority, and familiarity.	Social phishing experiments show personalization increases compliance; demographic variation in susceptibility identified.	[6] [14] [15]
Privacy & Risk Perception	Victims engage in rationalized cost-benefit decisions when disclosing information.	Privacy calculus explains information disclosure despite awareness of risk.	[4] [8]
Technical Mechanisms of Deception	Phishing, spoofing, credential harvesting, and authentication bypass dominate attack vectors.	Engineering studies emphasize layered security, spoof detection, and trust validation mechanisms.	[16] [17]
Digital Forensics & Attribution	Investigative capabilities rely on metadata, IP tracing, and artifact reconstruction.	Technical tracing supports fraud origin analysis; cross-border attribution remains challenging.	[18]
Victimology & Impact	Cyber theft produces financial, psychological, and reputational harm.	Underreporting and secondary victimization are persistent issues.	[2] [7]
Governance & Prevention Frameworks	Effective mitigation requires integrated socio-technical controls.	Layered security, behavioural training, regulatory coordination, and international collaboration recommended.	[2] [13] [14] [17]

The economic aspect of cyber theft complicates action further. Online fraud marketplaces function with minimal entry barriers, worldwide accessibility, and scalable automation. Strategies aimed at disrupting individual offenders may yield minimal long term effects unless infrastructure, financial pathways, and supportive ecosystems are considered. Tracing cryptocurrency, infiltrating markets, and implementing coordinated international enforcement may constitute more effective systemic responses.

The assessment also exposes methodological deficiencies in current studies. Although experimental phishing investigations demonstrate robust internal validity, numerous criminological and market assessments depend on qualitative or conceptual frameworks. Victimization research frequently experiences underreporting bias and sampling limitations. Enhanced longitudinal and cross-national empirical research is essential to assess long-term impact and policy efficacy.

The synthesis indicates that cyber deceit flourishes in contexts marked by unequal knowledge, inadequate guardianship, and disjointed regulatory monitoring. A comprehensive response incorporating criminological profiling, digital forensics, organizational governance, behavioural science, and regulatory alignment is essential.

In summary, cyber deception and theft constitute dynamic, hybrid threats influenced by technological advancement, economic motivations, and human psychology. Effective mitigation requires coordinated socio-technical methods instead of separate technological approaches.

3.3. Deductions from Review

The thorough synthesis offers a number of important deductions for consideration. To begin with, it is important to note that cyber deception is mostly socio-technical in nature, rather than solely technological. Criminals take advantage of human intellect just as well as they exploit software flaws. The second point is that cyber theft occurs inside scalable economic ecosystems, which suggests that disruption methods should focus on infrastructure and financial incentives rather than on single players. Third, the vulnerability of victims is not exclusively a result of ignorance; rather, it is a logical cost-benefit assessment that is impacted by perceived convenience and trust [4]. In the fourth place, it is imperative that the capacity for investigation incorporates criminological profiling, forensic analytics, and collaboration across international borders [1] [12] [18]. Finally, to lessen the impact of systemic exposure, preventative frameworks should combine layered security, behavioural training, privacy-by-design principles, and regulatory harmonization.

3.4. Mitigation Measures

The proposed mitigation measures in Cyber Deception and Theft are proposed based on the criteria effectiveness, scalability, cost-efficiency, sector fit, and evidence strength.

Effectiveness refers to the measurable reduction in successful deception attempts, phishing click-through rates, credential compromise, or financial loss. Interventions should demonstrate statistically significant impact across real-world or controlled evaluations.

Scalability assesses whether the measure can be deployed across diverse organisational sizes and infrastructures without disproportionate complexity. Solutions relying on automation, adaptive learning systems, or cloud-based deployment typically score higher.

Cost-efficiency evaluates implementation, maintenance, and training costs relative to risk reduction outcomes. Measures that combine technological controls (e.g., AI-driven anomaly detection) with low-cost behavioural nudges may yield higher value ratios.

Sector fit examines contextual relevance financial institutions, healthcare, edu-

cation, and government sectors face distinct threat profiles and regulatory obligations; mitigation must align with operational realities.

Evidence strength prioritizes peer-reviewed studies, longitudinal analyses, and replicated field experiments over anecdotal or vendor-reported claims.

Applying these criteria consistently supports the conclusion that optimal mitigation is socio-technical: integrating behavioural training, cognitive-aware interface design, adaptive technical controls, and coordinated policy frameworks. Measures that score highly across all five criteria rather than excelling in only one dimension should be prioritized in strategic cyber defence planning.

Subject to the above, the suggested mitigation measures for cyber deception and theft are detailed below;

First, continuous behavioural security training, coupled with simulated phishing exercises, effectively diminishes susceptibility and enhances security awareness [22] [23]. These programs are scalable via automated systems and cost-effective compared to breach cleanup expenses, rendering them appropriate across many sectors.

Secondly, AI-powered anomaly detection and behavioural analytics improve the early identification of suspicious activities by recognising anomalies in user and network behaviour. Empirical studies validate the efficacy of machine learning in intrusion detection systems [24] [25]. Despite potentially elevated deployment costs, scalability in cloud and business settings enhances long-term value.

Third, multi-factor authentication (MFA), especially phishing-resistant techniques, offers significant safeguarding against credential theft and account breach [26] [27]. MFA demonstrates consistent performance across several areas, particularly in finance and healthcare.

Fourth, the implementation of secure interface design that includes effective warning signals and anti-urgency messaging directly counters cognitive manipulation strategies [28]. These measures are economical and extremely scalable.

Interventions that combine behavioural, technical, and organisational controls, supported by robust empirical evidence, constitute the most effective socio-technical mitigation techniques.

Figure 3 below shows the mapping of mitigation measures to attack phases/vectors. Below is an explanation of the mapping.

Attract Attention: During the attention phase, mitigation emphasises cognitive-aware interface design, anti-urgency warning signals, spam filtration, and ongoing behavioural training to assist users in identifying misleading initial contact indicators prior to interaction.

Information Collection and Exchange: In the course of information exchange, privacy-by-design measures, data minimisation strategies, and phishing-resistant multi-factor authentication limit the volume and applicability of sensitive data that can be acquired, thereby diminishing the advantage for attackers, even at the onset of interaction.

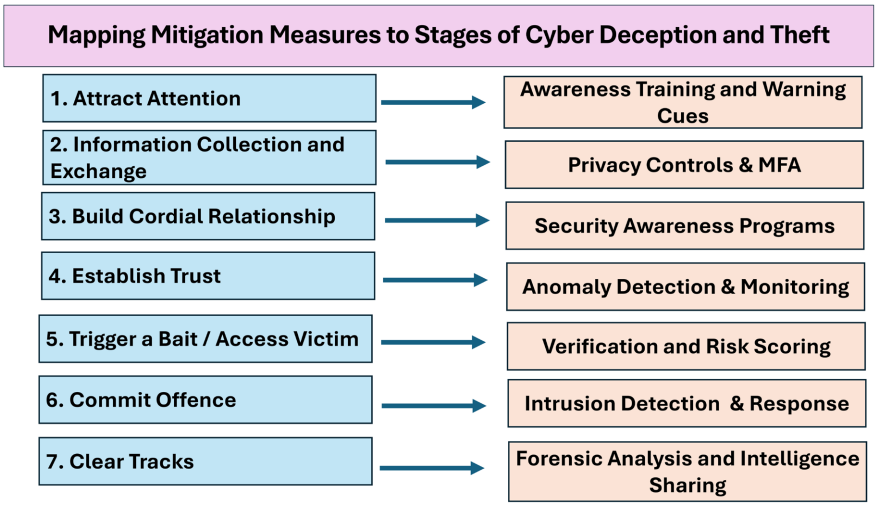

Figure 3. Mapping of mitigation measures to attack phases/vectors. Source: authors.

Build Cordial Relationship: As rapport strengthens, continuous security awareness initiatives adjust risk perception and highlight manipulation strategies, including familiarity, authority signalling, and emotional connection, thereby averting the normalisation of dubious communication behaviours.

Establish Trust: During the consolidation of trust, layered security measures—such as behavioural analytics and anomaly detection—observe aberrations in access patterns, ensuring that trust-based manipulation does not automatically confer system-level privileges.

Trigger a Bait/Access Victim: During the bait phase, transaction verification protocols, enhanced authentication, and automated risk assessment impede high-risk activities, diminishing the efficacy of enticements that depend on urgency or emotional manipulation.

Commit Offence: The execution of an offence is mitigated by real-time intrusion detection, financial monitoring systems, and quick incident response frameworks, which limit harm and enhance economic scalability.

Clear Tracks: Ultimately, forensic analytics, audit recording, and intersectoral intelligence sharing enhance attribution and deterrence, mitigating systemic vulnerabilities beyond isolated occurrences.

3.5. Implications for Research

This review highlights the need for deeper interdisciplinary integration across criminology, cybersecurity engineering, behavioural science, and economics. Future research should prioritize longitudinal and cross-national empirical studies to measure evolving patterns of cyber deception and theft. While experimental phishing research provides strong internal validity, broader ecological validity is required through real-world behavioural datasets. Greater methodological rigor in victimology studies is necessary to address underreporting bias and demographic sampling gaps. Additionally, research should explore AI-driven deception (e.g., generative phishing content), adversarial machine learning risks, and auto-

mated fraud markets. The integration of predictive analytics with criminological theory could enable more proactive prevention models. Finally, standardized risk-of-bias frameworks for cybercrime studies would enhance comparability and systematic synthesis in future reviews.

3.6. Implications for Policy

The findings suggest that cyber deception and theft are systemic rather than isolated offenses, requiring coordinated, multi-layered policy responses. Governments should strengthen cross-border legal cooperation and harmonize cybercrime legislation to address jurisdictional challenges. Regulatory frameworks should mandate stronger authentication standards, secure-by-design principles, and data protection enforcement across sectors. Public awareness campaigns must move beyond general advice to evidence-based behavioral interventions targeting cognitive vulnerabilities. Policy should also address financial infrastructure abuse, including cryptocurrency tracing and fraud market disruption. Improved victim reporting mechanisms and support services are essential to reduce stigma and secondary victimization. Ultimately, policy must align technological regulation with behavioural risk mitigation and international collaboration.

3.7. Implications for Industry

For industry, the research underscores that technical controls alone are insufficient. Organizations must adopt integrated socio-technical security strategies combining layered authentication, phishing-resistant architectures, behavioural training, and real-time anomaly detection. Zero-trust frameworks and continuous verification models should replace perimeter-based assumptions. Firms should invest in user-centred security design that reduces cognitive overload and mitigates deception cues. Regular phishing simulations, behavioural analytics, and threat intelligence sharing can strengthen resilience. Additionally, industry collaboration through information-sharing alliances can disrupt fraud ecosystems more effectively than isolated responses. Recognizing cyber deception as both a human and technological risk will enable organizations to build adaptive, resilient security cultures capable of responding to evolving threats.

4. Conclusion

Cyber deception and theft constitute intricate, adaptable risks integrated into modern digital environments. This review illustrates that these offences are not merely technical exploits, but socio-technical phenomena influenced by criminological opportunity structures, organized fraud networks, cognitive manipulation, and systemic trust dependencies. The intersection of motivated offenders, expandable digital infrastructures, and inadequate guardianship results in enduring vulnerabilities in online settings. Behavioural study demonstrates that deception leverages predicted cognitive biases, whilst technical studies emphasize that automation and anonymization enhance cybercriminal activities. The data implies that effective

mitigation cannot depend solely on technology measures. Integrated methods that encompass behavioral awareness, layered security architectures, forensic capabilities, regulatory coordination, and international collaboration are essential. With the ongoing acceleration of digital transformation, the complexity and magnitude of cyber deception are expected to rise. Future policy and research must consequently embrace interdisciplinary frameworks that can tackle both the human and technology aspects of cyber-enabled stealing. Additionally, it is recommended that future studies investigate artificial intelligence-driven detection models, adversarial machine learning concerns, and bitcoin tracing techniques. It is essential to conduct longitudinal victim studies to evaluate the different patterns of psychological rehabilitation and economic restitution. An evaluation of the harmonization of enforcement across different jurisdictions should be included in cross-national regulatory analysis. To make significant progress in the development of predictive prevention models and adaptive governance techniques, it will be essential for researchers in the fields of criminology, behavioural science, computer science, and policy research to work together across scientific disciplines.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Ainsworth, P.B. (2001) Offender Crime Profiling and Crime Analysis. Willan Publishing.

[2] Button, M. and Cross, C. (2017) Cyber Frauds, Scams and Their Victims. Routledge.

[3] Yar, M. (2005) The Novelty of "Cybercrime". *European Journal of Criminology*, **2**, 407-427. https://doi.org/10.1177/147737080556056

[4] Dinev, T. and Hart, P. (2006) An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, **17**, 61-80. https://doi.org/10.1287/isre.1060.0080

[5] Danquah, P. and Longe, O. (2011) Cyber Deception and Theft—An Ethnographic Study on Cyber Criminality from a Ghanaian Perspective. *Journal of Information Technology Impact*, **11**, 169-182.

[6] Longe, O.B., Danquah, P. and Ebem, D.U. (2012) De-Individuation, Anonymity and Unethical Behaviour in Cyberspace—Explorations in the Valley of Digital Temptations. *Computing Information Systems Journal*, **16**, 46-55.

[7] FS-ISAC (2025) Leveling Up: A Cyber Fraud Prevention Framework for Financial Services. FS-ISAC Cyber Fraud Prevention Framework Working Group.

[8] Wall, D.S. (2024) Cybercrime: The Transformation of Crime in the Information Age. 2nd Edition, Polity.

[9] Page, M.J., McKenzie, J.E., Bossuyt, P.M., *et al.* (2021) Updating Guidance for Reporting Systematic Reviews: Development of the PRISMA 2020 Statement. *Journal of Clinical Epidemiology*, **134**, 103-112.

[10] Higgins, J.P.T., Altman, D.G., Gotzsche, P.C., Juni, P., Moher, D., Oxman, A.D., *et al.* (2011) The Cochrane Collaboration's Tool for Assessing Risk of Bias in Randomised Trials. *BMJ*, **343**, d5928. https://doi.org/10.1136/bmj.d5928

[11] Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F. and Downs, J. (2010) Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Atlanta, 10-15 April 2010, 373-382. https://doi.org/10.1145/1753326.1753383

[12] Levi, M. (2008) Organized Fraud and Organizing Frauds. *Criminology & Criminal Justice*, **8**, 389-419. https://doi.org/10.1177/1748895808096470

[13] Leukfeldt, E.R. (2014) Cybercrime and Social Ties. Phishing in Amsterdam. *Trends in Organized Crime*, **17**, 231-249. https://doi.org/10.1007/s12117-014-9229-5

[14] Herzberg, A. and Gbara, A. (2004) TrustBar. Cryptology ePrint Archive.

[15] Johnson, T.A. (2005) Forensic Crime Investigation. CRC Press.

[16] Gruschka, N. and Lo Iacono, L. (2009) Vulnerable Cloud. 2009 *IEEE International Conference on Web Services*, Los Angeles, 6-10 July 2009, 625-631.

[17] Casey, E. (2011) Digital Evidence and Computer Crime. 3rd Edition, Academic Press.

[18] Schmalleger, F. and Pittaro, M. (2009) Crimes of the Internet. Pearson Prentice Hall.

[19] Anderson, R. (2008) Security Engineering. 2nd Edition, Wiley.

[20] Danquah, P., Longe, O.B., Lartey, J.D. and Tobbin, P.E. (2020) Towards a Theory for Explaining Socially-Engineered Cyber Deception and Theft. In: *Advances in Information Security, Privacy, and Ethics*, IGI Global, 44-58. https://doi.org/10.4018/978-1-7998-3149-5.ch003

[21] Jagatic, T.N., Johnson, N.A., Jakobsson, M. and Menczer, F. (2007) Social Phishing. *Communications of the ACM*, **50**, 94-100. https://doi.org/10.1145/1290958.1290968

[22] Jansson, K. and von Solms, R. (2013) Phishing for Phishing Awareness. *Behaviour & Information Technology*, **32**, 584-593. https://doi.org/10.1080/0144929x.2011.632650

[23] Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2014) Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, **42**, 165-176. https://doi.org/10.1016/j.cose.2013.12.003

[24] Buczak, A.L. and Guven, E. (2016) A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys & Tutorials*, **18**, 1153-1176. https://doi.org/10.1109/comst.2015.2494502

[25] Sommer, R. and Paxson, V. (2010) Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. 2010 *IEEE Symposium on Security and Privacy*, Oakland, 16-19 May 2010, 305-316. https://doi.org/10.1109/sp.2010.25

[26] Bonneau, J., Herley, C., Oorschot, P.C.v. and Stajano, F. (2012) The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. 2012 *IEEE Symposium on Security and Privacy*, San Francisco, 20-23 May 2012, 553-567. https://doi.org/10.1109/sp.2012.44

[27] Grassi, P.A., Garcia, M.E. and Fenton, J.L. (2017) Digital Identity Guidelines (NIST Special Publication 800-63B). National Institute of Standards and Technology.

[28] Egelman, S., Cranor, L.F. and Hong, J. (2008) You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Florence, 5-10 April 2008, 1065-1074. https://doi.org/10.1145/1357054.1357219