RAIS Journal for Social Sciences | Vol. 10, No. 1, 2026
ISSN 2574-0245 (Print) | ISSN 2574-1179 (Online) | DOI:10.5281/zenodo.19661077

Malvertising as a Vector for Cognitive Hacking: Integrating Technical and Psychological Defense Using the DISARM Framework

Sharon L. Burton

Embry-Riddle Aeronautical University, USA, Burtons6@erau.edu

Abstract: Malvertising, which embeds malicious code and psychological manipulation in digital ads, has become a major cybersecurity problem as it converges with cognitive hacking and disinformation. In 2024, incidents rose 10% year-over-year, with 29% involving misleading product offers, up from 26% the prior year, reflecting more deceptive tactics. Mobile environments face growing risks, as adware accounted for 35% of mobile threat detections in 2024. This qualitative study uses thematic analysis of recent industry data and academic reports to evaluate adaptive attack tactics and defense frameworks, including DISARM (Disinformation Analysis and Risk Management). Findings expose major gaps in governance, threat intelligence sharing, and the integration of technical and psychological defenses. The research concludes that a multidisciplinary strategy is vital to strengthen digital advertising ecosystem resilience and improve user protection. This work will interest cybersecurity professionals, researchers, policymakers, and digital advertising leaders seeking effective responses to emerging online threats.

Keywords: Malvertising, Cognitive Hacking, DISARM Framework, Digital Advertising, Cybersecurity, Influence Operations

Introduction

The digital advertising ecosystem, foundational to the internet economy, has become a prime target for cybercriminals due to its vast scale and complexity. Malvertising is a deceptive tactic where cyber attackers embed malicious code within online advertisements that are delivered through legitimate ad networks, allowing the harmful content to appear on trusted websites, often without the knowledge of publishers or users, thereby exposing a broad audience without requiring them to visit suspicious sites (Mukherjee et al.,2025; SentinelOne, 2025; Sood & Enbody, 2011). This risk is exacerbated by increasing reliance on third-party ad platforms, which introduce vulnerabilities that attackers can exploit at scale (Benaroch, 2021). The crafty nature of malvertising enables it to bypass traditional security measures, frequently requiring no user interaction to execute an attack (Zeng, 2024). According to Jones (2020), risk is best understood as a multifactorial construct involving uncertainty, potential harm, and the need for proactive mitigation strategies. Recent industry data from GeoEdge (2024), Q1 2024 Malvertising Report, provided a detailed breakdown of attack types and trends, highlighting the evolving tactics of threat actors. In the first quarter of 2024, misleading product offers emerged as the most prevalent malvertising vector, accounting for 29% of all attacks, a notable increase from 26% in 2023 (GeoEdge, 2024). These campaigns typically lure users with enticing deals or discounts, redirecting them to fraudulent or malicious websites (GeoEdge, 2024). Auto-redirects, another major attack type, comprised 25% of malvertising incidents in Q1 2024, down slightly from 28% in 2023, but still represents a significant threat (GeoEdge, 2024).

These redirects often lead users to phishing sites or initiate malware downloads, with many linked to the notorious ScamClub VAST campaign. ScamClub VAST campaign refers to a malicious online advertising operation that uses the VAST (Video Ad Serving Template) protocol to distribute deceptive or fraudulent ads (Pedael, 2025). These campaigns typically hijack legitimate ad networks to show fake alerts, tech support scams, or redirect users to harmful websites (GeoEdge, 2024). The goal is to trick users into clicking or taking actions that result in financial gain for the scammers, such as subscribing to unwanted services, downloading malware, or providing sensitive information. ScamClub is the name associated with a group or operation behind such aggressive and misleading ad-based attacks (Confiant, 2025). As given by GeoEdge (2024), malicious extensions and add-ons also saw an uptick, constituting 16% of malvertising incidents in Q1 2024, compared to 13% in 2023. Also, these extensions, frequently impersonating as legitimate tools, compromise user privacy by harvesting sensitive data or injecting additional advertisements (Spadafora, 2024). Financial ad scams increased modestly from 13% in 2023 to 14% in the first quarter of 2024, while tech support scams experienced a notable rise from 2% to 6% over the same period (GeoEdge, 2024). These shifts indicate a diversification of tactics, with attackers adapting to detection efforts by targeting new vectors and exploiting user trust in different ways.

Moreover, the GeoEdge (2024) Q1 2024 Ad Quality Report offered that device targeting trends shifted in early 2024. Desktops became the primary target for malvertising, accounting for 57% of attacks, reversing the previous pattern where mobile devices were more frequently targeted (GeoEdge, 2024). The report noted that mobile attacks, now comprising 42% of incidents, predominantly involved pre-click redirects, while desktop campaigns focused on post-click scams using clickbait ads. This strategic adaptation suggests that malvertisers are refining their approaches to maximize impact across platforms and user behaviors.

The broader context of these trends is a 10% year-over-year increase in overall malvertising incidents, underscoring the persistent and growing threat to digital advertising environments (Vishwakarma & Dhakad, 2024). The infection rates on supply-side platforms (SSPs) varied, with some platforms experiencing spikes as high as 2.56% of all ads blocked for malicious content in Q1 2024, particularly those driven by financial scams and fake antivirus campaigns. Google Ads, while generally maintaining higher quality standards, still saw a marginal decrease in infection rates, dropping from 1.25% to 0.98% over the same period.

These evolving attack vectors and breach rates reflect the adaptability of threat actors and the ongoing arms race between malvertisers and defenders (Vishwakarma & Dhakad, 2024). The increasing sophistication of malvertising campaigns, particularly those leveraging clickbait and large-scale redirect schemes, highlights the need for continuous vigilance and innovation in security strategies (Bârgăoanu & Pană, 2024). The intersection of malvertising with cognitive hacking and disinformation further complicates the landscape, as malicious ads are not only used to deliver malware but also to manipulate public perception and erode trust in digital ecosystems (Bârgăoanu & Pană, 2024). Cognitive hacking refers to the deliberate manipulation of human perception, beliefs, or decision-making processes through digital means. This form of cyberattack exploits psychological vulnerabilities, using misinformation, disinformation, or persuasive content to influence individual or collective behavior. Rather than targeting technical systems directly, cognitive hacking aims to undermine trust, shape opinions, or disrupt organizational or societal functions by exploiting cognitive biases and emotional triggers.

Given this context, the central analytical question arises: How can defenders effectively counter malvertising given its technical sophistication and integration with broader cognitive hacking campaigns? This study argues that a comprehensive defense requires technological innovation and the adoption of frameworks that address the psychological manipulation inherent in malvertising. See Figure 1 for details.

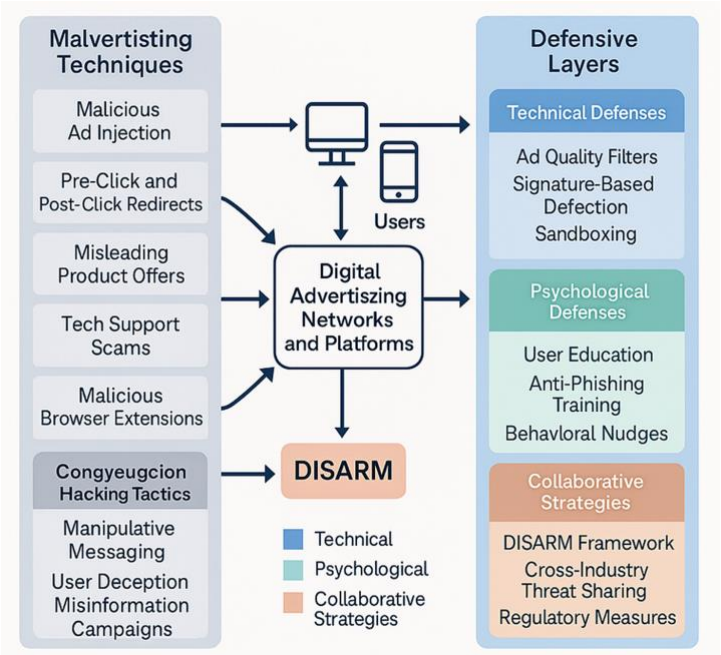

Figure 1. Integrated Model of Malvertising Attack Vectors and Multidisciplinary Defense Strategies

A comprehensive defense against malvertising must simultaneously advance technical solutions and adopt frameworks that directly address the psychological manipulation at the heart of modern attacks (Bârgăoanu & Pană, 2024). Consider how a modern advertising platform integrates advanced machine learning algorithms with a cognitive analysis framework like DISARM (Disinformation Analysis and Risk Management) to defend against malvertising and influence operations to illustrate the dual-layered approach (Kumar & Urwin, 2024). First, the platform continuously monitors all incoming advertisements using machine learning models trained to detect anomalous behaviors. This writing team notes that these machine learning models trained to detect anomalous behaviors flag suspicious patterns such as unusually rapid redirects, code obfuscation, or deviations from typical ad delivery sequences (Kumar & Urwin, 2024). For example, suppose an ad starts redirecting users to multiple domains in quick succession or contains encrypted JavaScript segments not commonly observed in legitimate campaigns. In that case, the system automatically marks it as potentially malicious (Bârgăoanu & Pană, 2024). Once a technical anomaly is detected, the flagged advertisement is subjected to further scrutiny using the DISARM framework. At this stage, DISARM analyzes the narrative content of the ad, examining the language, imagery, and contextual cues to determine whether manipulative messaging or psychological tactics are present (Bârgăoanu & Pană, 2024). The framework looks for indicators of disinformation, such as emotionally charged language, fabricated endorsements, or calls to urgent action that exploit cognitive biases.

Through this process, DISARM categorizes the psychological strategies being used (i.e., such as fear appeals, authority impersonation, or social proof manipulation) and assesses whether the ad is part of a coordinated disinformation campaign. If such tactics are identified, the platform can take immediate technical action by blocking or removing the ad, while also generating intelligence reports for longer-term strategic responses (Kumar & Urwin, 2024). These reports inform user education initiatives, policy updates, and collaborative efforts with other platforms to counter recurring influence operations. The following primary sections are included in this study: Background, Assumptions, Limitations, and Delimitations, Research Gap, Research Methodology and Design, Literature Review, Conceptual Framework, Conceptual Framework Critiques, Originality of the Text, Results, Discussion, and Conclusions.

Background

According to Zhou and Yang (2023), the shift from traditional to digital advertising has transformed the way businesses reach consumers, but it has also introduced new security challenges. Online ads are now delivered through complex networks that span multiple domains and technologies, making it challenging to ensure the integrity of every component (Vishwakarma & Dhakad, 2024). Attackers exploit this complexity by injecting malicious code into ads, which are then served to users via trusted platforms. This method enables broad distribution of malware with minimal effort, as even reputable sites can inadvertently become vectors for infection (Vishwakarma & Dhakad, 2024).

Malvertising tactics have evolved alongside advances in web technologies. Early attacks relied on simple redirects or pop-ups, but modern campaigns use sophisticated techniques such as exploiting widget vulnerabilities, hidden iframes, and compromised content delivery networks (Cybersecurity and Infrastructure Security Agency, 2024). These methods often bypass user awareness and traditional security controls, increasing the risk of widespread compromise.

The rise of programmatic advertising and real-time bidding has further complicated the landscape (Liua et al., 2022). Automated ad placement can inadvertently prioritize speed and reach over security, allowing malicious actors to infiltrate ad networks more easily (Cybersecurity and Infrastructure Security Agency, 2024). Additionally, the use of social engineering within ads (i.e., urgent calls to action or impersonation of trusted brands) blurs the line between technical and psychological exploitation.

According to Bârgăoanu and Pană (2024), recent research underlines the convergence of malvertising with cognitive hacking and disinformation campaigns. Malicious ads are increasingly used not just to deliver malware, but to manipulate public opinion, spread misinformation, and disrupt digital discourse (Bârgăoanu & Pană, 2024). Frameworks like DISARM have been developed to analyze and counter these multifaceted threats by enabling structured incident analysis and collaborative intelligence sharing (Cavaliere et al., 2024). The DISARM Framework is a collaborative, open-source resource developed to support organizations in detecting, understanding, and addressing disinformation and influence campaigns (Bârgăoanu & Pană, 2024; Cavaliere et al., 2024).

Despite advances in detection and mitigation, malvertising remains a persistent challenge due to the dynamic nature of online advertising and the adaptability of attackers. Addressing this threat requires a holistic approach that combines technical defenses, policy development, user education, and international cooperation (Cybersecurity and Infrastructure Security Agency, 2024; Sood & Enbody, 2011). Sustained collaboration between industry stakeholders and regulatory bodies is essential to keep pace with evolving tactics and to strengthen the overall resilience of the digital advertising ecosystem.

Assumptions, Limitations, and Delimitations

A rigorous examination of any research endeavor requires explicit acknowledgment of its underlying assumptions, inherent limitations, and the boundaries that define its scope (Braun & Clarke, 2025). Clarifying these elements is essential for contextualizing the findings, guiding the interpretation of results, and identifying avenues for future inquiry. In this research, the integration of technical, psychological, and governance perspectives in the analysis of malvertising defense necessitates a transparent articulation of the foundational premises, potential constraints, and deliberate exclusions that shape the research design and its conclusions.

Assumptions

This research is grounded in several key assumptions that shape its analytical approach and interpretation of findings. It is assumed that an interdisciplinary integration of technical, psychological, and policy-oriented frameworks provides a more comprehensive and effective strategy for malvertising defense than single-discipline approaches, reflecting the necessity of addressing system vulnerabilities and human factors in modern cyber threats (Bârgăoanu & Pană, 2024; Cavaliere et al., 2024). The study presumes the reliability and representativeness of the secondary data sources utilized, including industry reports and academic literature, in capturing current trends and tactics in malvertising and cognitive hacking (GeoEdge, 2024; Deepwatch Labs, 2025). Additionally, it is assumed that the tactics and techniques identified in recent literature are indicative of ongoing and emerging patterns, and that frameworks such as DISARM are sufficiently robust and adaptable for modeling malvertising incidents across diverse organizational contexts (Cavaliere et al., 2024; DISARM Foundation, 2024). The qualitative insights derived from thematic analysis are also presumed to be generalizable enough to inform best practices and policy recommendations for a variety of digital advertising environments (Bârgăoanu & Pană, 2024).

Limitations

Despite the comprehensive conceptual framework developed in this study, several significant limitations must be acknowledged. The analysis predominantly relies on secondary literature, including industry reports and academic studies, without incorporating longitudinal or controlled empirical investigations comparing the effectiveness of integrated malvertising defense strategies against traditional approaches. As a result, there is a lack of quantitative and qualitative evidence assessing the real-world impact, scalability, and operational challenges of such interdisciplinary frameworks across diverse organizational settings (Bârgăoanu & Pană, 2024; Cavaliere et al., 2024; DISARM Foundation, 2024). While the growing consensus advocates for multifaceted solutions that blend technical, psychological, and policy dimensions, these recommendations remain principally conceptual, pending further validation. This gap underscores an urgent research need for empirical studies, including longitudinal case analyses and experimental designs, to substantiate and refine integrated defense mechanisms and thereby enhance cybersecurity resilience in the face of evolving malvertising threats.

Delimitations

The delimitation of this research is defined by its focus on malvertising within digital advertising ecosystems, deliberately excluding other vectors such as email phishing or social media manipulation except where these intersect with advertising-based attacks (Sood & Enbody, 2011). While global data is referenced, the analysis primarily centers on North American and European digital advertising markets, acknowledging that regional variations may exist (GeoEdge, 2024; Maigre, 2022). This research centers its analysis on the DISARM framework and its integration with technical detection systems, rather than providing an exhaustive evaluation of alternative models (Cavaliere et al., 2024; DISARM Foundation, 2024). Methodologically, the research adopts a qualitative, thematic approach, intentionally excluding quantitative modeling or statistical hypothesis testing to focus on the nuanced interplay between technical and psychological dimensions (Bârgăoanu & Pană, 2024). Lastly, the findings and analysis are current as of mid-2025 and do not account for subsequent developments or incidents that may arise thereafter (GeoEdge, 2024; Deepwatch Labs, 2025). By clearly articulating these assumptions, limitations, and delimitations, the

study provides a transparent foundation for interpreting its findings and recommendations, while outlining the parameters within which its conclusions should be understood.

Statement of the Problem and the Research Gap

Despite growing recognition of malvertising's evolving impact, current research and industry practice remain largely fragmented. Recent research has shown that malicious ads are increasingly used to spread false narratives, disrupt information ecosystems, and erode trust in digital platforms (Bârgăoanu & Pană, 2024; Cybersecurity and Infrastructure Security Agency, 2024). Most studies and technical solutions focus on detecting and blocking malware delivery, but they overlook the psychological and behavioral dimensions exploited by sophisticated attackers. There is a critical gap in empirical evidence regarding the effectiveness, scalability, and operational challenges of integrated defense approaches that merge technical, psychological, and policy frameworks (GeoEdge, 2024). Existing defense strategies predominantly rely on secondary literature and qualitative analysis, and there is insufficient longitudinal or controlled research comparing these interdisciplinary methods to traditional approaches.

Policy frameworks addressing malvertising are frequently hindered by fragmented governance, checklist-based compliance, and siloed security responsibilities, which diminish accountability and coordination among stakeholders (Edwards, 2025; Benaroch, 2021). The lack of standardized protocols for threat intelligence sharing and collaborative incident response further exacerbates the vulnerability of digital advertising environments to persistent and adaptive threats (GeoEdge, 2024).

A significant gap exists in the limited integration of technical and psychological perspectives in academic research and practical defense mechanisms against malvertising, particularly in understanding its dual role as a vector for malware and cognitive manipulation (Cavaliere et al., 2024; Zhou & Yang, 2023). Bridging this gap is critical to developing effective, scalable, and resilient strategies that protect users and restore trust in digital advertising platforms (Bârgăoanu & Pană, 2024).

Further, the literature reveals a lack of empirical studies quantifying the impact of malvertising within influence operations and cognitive hacking campaigns (Cavaliere et al., 2024; Zhou & Yang, 2023). Most research has concentrated on isolated case studies or technical analyses, leaving a gap in understanding the broader societal implications and the effectiveness of interdisciplinary defense strategies (Cavaliere et al., 2024). This deficiency limits the development of holistic frameworks capable of anticipating and mitigating the multifaceted risks posed by malvertising (Bârgăoanu & Pană, 2024).

Addressing this gap is crucial for several reasons. First, the dynamic and adaptive nature of malvertising requires defense mechanisms that are equally versatile and interdisciplinary (Vishwakarma & Dhakad, 2024; Liua et al., 2022). Second, the psychological manipulation inherent in many malvertising campaigns demands that cybersecurity strategies move beyond technical solutions to include user education, policy development, and collaborative frameworks such as DISARM (Bârgăoanu & Pană, 2024; Cavaliere et al., 2024). Third, as digital advertising continues to expand, the potential for large-scale influence operations leveraging malvertising will inevitably increase, making it imperative to understand and counter these threats at multiple levels (Liua et al., 2022; Vishwakarma & Dhakad, 2024).

In summary, the significant gap lies in the insufficient integration of technical and psychological perspectives in malvertising research, especially concerning cognitive hacking and influence operations (Cybersecurity and Infrastructure Security Agency, 2024; GeoEdge, 2024; Bârgăoanu & Pană, 2024). Bridging this gap will enable the development of more effective, sustainable, and comprehensive defense strategies, ultimately enhancing

the resilience of digital advertising ecosystems and protecting users from technical and cognitive threats (Bârgăoanu & Pană, 2024).

Research Methodology and Design

This research utilizes a qualitative research methodology to investigate the complex dynamics of malvertising, cognitive hacking, and disinformation. Qualitative research is well-suited for exploring multifaceted phenomena that are context-dependent and not easily quantifiable. In cybersecurity research, qualitative methods such as case studies, interviews, and thematic analysis are effective for uncovering nuanced insights into attacker behavior, user vulnerabilities, and the efficacy of defense mechanisms. These methods enable a deeper understanding of the motivations, tactics, and impacts associated with malvertising campaigns, particularly where technical and psychological factors intersect (Bârgăoanu & Pană, 2024; Cavaliere et al., 2024).

The research design is structured around the analysis of documented incidents, industry reports, academic literature, and practical applications of the DISARM framework. By synthesizing findings from diverse sources, the study aims to identify patterns and themes that characterize malvertising within broader influence operations. The DISARM framework provides a systematic methodology for categorizing and analyzing disinformation tactics, enabling structured incident analysis and collaborative intelligence sharing. Its use supports the development of a common language and standardized definitions, which are essential for ensuring consistency and comparability across different research contexts (Cavaliere et al., 2024; Bârgăoanu & Pană, 2024).

Data collection involves reviewing empirical studies, cybersecurity reports, and case analyses that document malvertising incidents and their integration with cognitive hacking strategies. Thematic analysis is employed to identify recurring motifs and strategies, such as the use of misleading ads, brand impersonation, and psychological manipulation. This approach facilitates the examination of how technical vulnerabilities and cognitive biases are exploited in malvertising campaigns. The research also considers the role of automated detection systems, collaborative defense frameworks, and policy interventions in mitigating these threats (GeoEdge, 2024; Cybersecurity and Infrastructure Security Agency, 2024).

The methodology emphasizes the importance of triangulating data from multiple sources to enhance the validity and reliability of findings. By integrating technical, psychological, and governance perspectives, this research seeks to provide a holistic understanding of malvertising and its implications for cybersecurity. The qualitative design is flexible, accommodating the evolving nature of cyber threats and supporting the iterative refinement of research questions and analytical frameworks (Sood & Enbody, 2011; Vishwakarma & Dhakad, 2024).

In summary, this research employs a qualitative, interdisciplinary methodology grounded in thematic analysis and supported by the DISARM framework. This approach is well-suited to capturing the dynamic and multifaceted nature of malvertising, enabling the development of comprehensive recommendations for practitioners, researchers, and policymakers (Bârgăoanu & Pană, 2024; Cavaliere et al., 2024; GeoEdge, 2024).

Literature Review

This literature review critically examines the existing body of research related to malvertising, integrating insights from cybersecurity, cognitive hacking, and digital advertising fields. It aims to provide a comprehensive overview of how malvertising tactics have evolved, the technical and psychological vulnerabilities they exploit, and the current defense strategies employed. By evaluating scholarly articles, industry reports, and empirical studies, this review identifies gaps in knowledge and underscores the necessity of holistic

frameworks like DISARM. This foundation is essential to contextualize the discussion and support the development of practical, multidimensional approaches to counter malvertising threats. This literature review covers policy framework gaps in malvertising and cyber defense, evolution and mechanisms in malvertising, critique: evolution and mechanisms of malvertising, malvertising and cognitive hacking, critique: malvertising and cognitive hacking, defense frameworks and collaborative approaches, critique: defense frameworks and collaborative approaches, detection and mitigation techniques, critique: detection and mitigation techniques, and a summary of the literature review.

Policy Framework Gaps in Malvertising and Cyber Defense

Persistent gaps remain within current policy frameworks addressing malvertising and broader cybersecurity threats, often undermining the efficacy of technical and collaborative defenses (Benaroch, 2021). One major challenge involves fragmented governance and the prevalence of "checklist compliance" rather than substantive risk reduction. Many organizations adopt standards such as ISO 27001 or NIST, yet treat these frameworks as ends in themselves (Edwards, 2025). This approach can result in siloed security responsibilities, with governance often separated from technical operations, diminishing accountability and coordination in responding to malvertising incidents (Edwards, 2025).

Transitioning to broader regulatory concerns, legal and information sharing barriers significantly impede robust cyber defense (Congressional Research Service, 2015). Organizations frequently hesitate to share threat intelligence due to fears of liability, privacy breaches, and reputational harm (Brilingaitė et al., 2022). Even where laws, such as the U.S. Cybersecurity Information Sharing Act of 2015, provide some liability protection and incentives, varying global regulations and differing levels of data protection create uncertainty and hinder effective cross-border information exchange (Atlan, 2025). The result is a patchwork of compliance obligations and unclear pathways for collaboration, leaving critical gaps in response and prevention capabilities (Congressional Research Service, 2015).

Internationally, disparities in regulatory standards and enforcement further exacerbate these gaps. For example, the European Union enforces strict data protection through regulations like General Data Protection Regulation (GDPR) and the Directive on Security of Network and Information Systems (NIS Directive), while the United States and Middle Eastern countries use more voluntary or sector-specific approaches to cybersecurity (Bada & Nurse, 2021). These differences contribute to inconsistent practices in data handling, incident response, and certification, making it challenging to establish global best practices or harmonize efforts against malvertising and related threats (Bada & Nurse, 2021).

Differences in global regulatory regimes contribute significantly to gaps in malvertising defense. For instance, the European Union’s (GDPR) and NIS Directive enforce strict incident reporting and cybersecurity requirements, while the United States relies primarily on voluntary or sector-specific frameworks, resulting in inconsistent practices across regions (Bada & Nurse, 2021). This regulatory fragmentation impedes real-time threat intelligence sharing, coordination, and unified response to attacks, especially for multinational organizations and cross-border ad networks (Brilingaitė et al., 2022). Harmonizing international standards and deepening cross-sector collaboration would mitigate these vulnerabilities and improve the collective resilience of the digital advertising ecosystem (Bryson et al., 2021)

Beyond technical and regulatory fragmentation, policy frameworks also tend to lag behind the rapidly evolving tactics used by malvertisers, especially as attacks increasingly blend with cognitive hacking and disinformation techniques. The lack of explicit policy coverage for areas like social engineering, psychological manipulation, and AI-driven threats exposes blind spots and allows adversaries to exploit existing legal and structural

ambiguities (Falade, 2023). As technology advances, policy and regulatory development often fail to keep pace, leading to reactive rather than proactive defense strategies. Scholars and practitioners emphasize the necessity of coordinated, interdisciplinary action to address these persistent gaps. Closing these policy gaps will require harmonized standards, deeper cross-sector collaboration, more transparent legal frameworks for information sharing, and proactive regulation that anticipates technical and human-centered threats in the evolving landscape of malvertising and cyber defense (Brilingaitė et al., 2022; Bryson et al., 2021; Falade, 2023). An effective defense against malvertising requires simultaneous advancement of technical safeguards and the implementation of frameworks specifically designed to counteract the psychological manipulation central to these sophisticated attacks.

Evolution and Mechanisms of Malvertising

Malvertising has evolved from basic web redirects and pop-up schemes to highly sophisticated, multi-stage attacks that exploit the intricacies of the online advertising ecosystem (Sood & Enbody, 2011; SentinelOne, 2025). Early incidents typically relied on exploiting simple browser vulnerabilities or embedding malicious code within banner ads, resulting in drive-by downloads and phishing attempts (GeoEdge, 2024). As digital advertising technologies matured, attackers began leveraging content delivery networks, real-time bidding platforms, and legitimate ad exchanges to distribute malicious advertisements on reputable websites, expanding their reach and impact (Vishwakarma & Dhakad, 2024; Zhou & Yang, 2023).

Modern malvertising campaigns utilize advanced techniques such as hidden iframes, obfuscated JavaScript, and malicious browser extensions (Noever & McKee, 2025; Singh et al., 2025). These methods enable attackers to bypass traditional security measures and deliver payloads without requiring user interaction (Noever & McKee, 2025; Singh et al., 2025). Auto-redirects, for example, have become a persistent threat, evolving from simple JavaScript-based tactics to complex, multi-layered attacks that can evade detection (GeoEdge, 2024; Human Security, 2025). Attackers frequently impersonate trusted brands, leveraging social engineering to increase the likelihood of user engagement and compromise (SentinelOne, 2025).

The rise of programmatic advertising and automated ad placement has further complicated the malvertising landscape. Cybercriminals exploit the speed and scale of these systems, injecting malicious code into ads that are rapidly disseminated across multiple platforms (Liua et al., 2022). Additionally, evolutionary malware, capable of morphing its code and delivery mechanisms, has made detection and remediation increasingly challenging for defenders (Deepwatch Labs, 2025). This constant adaptation underscores the arms race between threat actors and cybersecurity professionals.

Critique: Evolution and Mechanisms of Malvertising

Technical analyses have provided valuable insights into the progression of malvertising tactics; however, they often fall short in addressing the human factors that contribute to the success of these campaigns (Bârgăoanu & Pană, 2024). Studies have concentrated on the mechanics of code injection, exploitation of chains, and ad network vulnerabilities, yet overlook the psychological triggers that entice users to interact with malicious ads (Sood & Enbody, 2011; GeoEdge, 2024). As given by Moras (2024), this narrow focus can lead to an overreliance on automated detection tools, which, although effective against known threats, may not anticipate novel attack vectors that exploit user trust and cognitive biases.

The rapid evolution of malware, particularly the emergence of evolutionary Trojans and polymorphic code, poses a formidable challenge to static signature-based defenses (Deepwatch Labs, 2025). The dynamic nature of malvertising campaigns means that

security solutions must continually adapt, yet resource constraints and the sheer volume of online ads make comprehensive coverage difficult to achieve. This dynamic creates gaps in protection, especially for smaller organizations with limited cybersecurity expertise.

The fragmented nature of the digital advertising ecosystem further complicates defense (West & Maurer, 2021). The involvement of multiple intermediaries, ad exchanges, networks, publishers, and third-party vendors complicates attribution and incident response. Attackers exploit these complexities to obfuscate their activities and distribute malicious ads at scale, often without immediate detection (Liua et al., 2022). Also, the lack of standardized protocols for threat intelligence sharing exacerbates this issue, hindering coordinated defense efforts. A more holistic approach that incorporates psychological, organizational, and policy dimensions is necessary to address the full scope of malvertising threats (Liua et al., 2022). .

Malvertising and Cognitive Hacking

While the technical aspects of malvertising are well-documented, its intersection with cognitive hacking and disinformation campaigns has emerged as a critical area of concern (Bârgăoanu & Pană, 2024). Malicious advertisements are now routinely used to manipulate public opinion, spread false narratives, and disrupt the integrity of information ecosystems (Cavaliere et al., 2024). Cognitive hacking leverages psychological manipulation, exploiting users' biases and emotions to achieve influence objectives (Portnox, 2024; Blackbird.AI, 2025).

Frameworks such as DISARM have been developed to analyze and counteract these multifaceted threats. DISARM provides a structured methodology for categorizing disinformation tactics, facilitating incident analysis, and enabling collaborative intelligence sharing among stakeholders (Cavaliere et al., 2024; DISARM Foundation, 2024). By integrating technical and psychological perspectives, DISARM supports the anticipation and mitigation of cyber-enabled influence operations.

Critique: Malvertising and Cognitive Hacking

The integration of malvertising within cognitive hacking and disinformation research is a relatively new development, and empirical studies quantifying its impact remain limited (Bârgăoanu & Pană, 2024; Cavaliere et al., 2024). Much of the existing literature relies on qualitative assessments or isolated case studies, which, while informative, do not provide a comprehensive understanding of the broader societal implications. This lack of robust, quantitative data hampers the development of evidence-based policies and targeted interventions.

Technical researchers often underestimate the psychological manipulation inherent in malvertising campaigns. While frameworks like DISARM offer valuable tools for analyzing influence operations, their effectiveness depends on widespread adoption and consistent application across diverse organizational contexts (DISARM Foundation, 2024). Variability in implementation can lead to gaps in coverage and reduce the overall efficacy of collaborative defense strategies.

The rapidly evolving nature of cognitive hacking tactics, including the use of deepfakes, AI-generated content, and automated bot networks, further complicates defense. Attackers are now able to deploy compelling synthetic media at scale, exploiting neurological trust mechanisms and bypassing traditional security protocols (Breacher.ai, 2025; Thales, 2025). The democratization of AI tools has lowered the barrier to entry, enabling a wider range of threat actors to orchestrate sophisticated influence campaigns and automated attacks (TRM Labs, 2025; F5 Labs, 2025). Frameworks must remain agile, incorporating ongoing threat intelligence and adapting to new attack vectors as they

emerge. This shift requires technical upgrades and continuous collaboration with behavioral scientists to anticipate and counteract manipulation strategies that target human cognition (Portnox, 2024; LinkedIn, 2025).

Interdisciplinary research that bridges technical, psychological, and policy perspectives is essential to develop holistic solutions capable of countering the multifaceted risks posed by malvertising-driven cognitive hacking. By integrating insights from neuropsychology, cybersecurity, and regulatory studies, researchers can design more resilient defense mechanisms that address system vulnerabilities and human factors (George Mason University, 2024; MDPI, 2024). Such collaboration enables the creation of adaptive frameworks that can evolve in response to emerging threats, ensuring that technological and social dimensions are considered in mitigation strategies (EthicAI, 2025). Ultimately, fostering interdisciplinary partnerships will strengthen the collective capacity to detect, analyze, and respond to the complex challenges presented by modern malvertising and cognitive hacking campaigns. An effective defense against malvertising requires simultaneous advancement of technical safeguards and the implementation of frameworks specifically designed to counteract the psychological manipulation central to these sophisticated attacks.

Defense Frameworks and Collaborative Approaches

The increasing complexity of malvertising has necessitated the development of collaborative defense frameworks. DISARM, inspired by the MITRE ATT&CK framework, offers a common language and standardized definitions for describing influence operations and coordinating responses (Bârgăoanu & Pană, 2024; Maigre, 2022). These frameworks enable organizations to share threat intelligence, automate detection and mitigation actions, and foster collective resilience against evolving threats (GeoEdge, 2024).

Frameworks like DISARM are designed for interoperability with established cybersecurity protocols, such as STIX and TAXII, allowing seamless integration with existing threat intelligence platforms and facilitating automated, real-time information exchange across sectors to enhance their effectiveness further (Maigre, 2022; Fenza et al., 2025). This interoperability supports rapid collective action, enabling stakeholders from government, industry, and civil society to coordinate responses to emerging malvertising campaigns more efficiently (DISARM Foundation, 2024). In practice, DISARM's structured approach helps organizations model incidents, track adversarial tactics, and implement countermeasures that are scalable and adaptable to new threats (GeoEdge, 2024).

Despite these advancements, challenges persist in data sharing, privacy, and interoperability. Organizational silos and varying levels of technical maturity can hinder the seamless adoption of collaborative defense measures (Cavaliere et al., 2024). Data sharing is further complicated by legal and regulatory requirements, which can restrict the flow of sensitive information and slow down response times (Atlan, 2023; Academic.oup.com, 2022). Interoperability issues, such as inconsistent data formats and fragmented toolsets, may also reduce the efficiency of joint operations and create gaps in threat coverage (Neumetric, 2024). Nevertheless, the integration of frameworks like DISARM remains essential for addressing the multi-dimensional risks posed by malvertising, as they provide a foundation for unified action and continuous improvement in defense strategies (Maigre, 2022; DISARM Foundation, 2024).

Critique: Defense Frameworks and Collaborative Approaches

Collaborative defense frameworks such as DISARM represent a significant advancement in the fight against malvertising and influence operations, yet their adoption is not without

obstacles (Bârgăoanu & Pană, 2024; Maigre, 2022). Organizational silos can impede the timely sharing of threat intelligence and hinder coordinated response efforts. Differences in technical capacity, resource allocation, and risk tolerance across organizations further complicate collaboration.

Privacy concerns and regulatory constraints also pose challenges to effective data sharing. Organizations may be reluctant to disclose sensitive information about incidents, fearing reputational damage or legal repercussions. This hesitancy can delay the dissemination of critical threat intelligence, allowing attackers to exploit vulnerabilities for more extended periods (Cavaliere et al., 2024). In some cases, the lack of clear legal frameworks or guidance further discourages timely cooperation, making it even more challenging to establish trust among industry participants. As a result, fragmented communication can undermine collective defense efforts and leave gaps that sophisticated threat actors are quick to exploit.

Additionally, the interoperability of defense frameworks remains a work in progress. Variations in terminology, data formats, and analytical methodologies can create confusion and reduce the efficiency of joint operations (GeoEdge, 2024). These inconsistencies often result in duplicated efforts or missed opportunities for collaboration, ultimately weakening the overall security posture. Achieving seamless interoperability will require not only technical solutions but also consensus on best practices and ongoing dialogue between stakeholders.

As given by the World Economic Forum (2021), the continued refinement and integration of collaborative defense frameworks are essential for enhancing resilience against malvertising. Further, addressing organizational, legal, and technical barriers will require sustained commitment from all stakeholders, as well as the development of clear guidelines and best practices for information sharing and incident response (World Economic Forum, 2021). Only through persistent collaboration and adaptive strategies can the industry keep pace with the evolving tactics of malvertisers and ensure robust protection for digital ecosystems. Building on the imperative for coordinated action, the following section explores the technological arsenal currently deployed to combat malvertising, offering insight into detection and mitigation techniques that reinforce defensive posture at the organizational and ecosystem levels.

Detection and Mitigation Techniques

A diverse array of technical solutions has been proposed to detect and mitigate malvertising. Machine learning algorithms, behavioral analysis, and network monitoring are commonly employed to identify anomalous ad behavior and block malicious content before it reaches end users (Vishwakarma & Dhakad, 2024; Perception Point, 2023). Real-time ad scanning, web application firewalls, and browser security settings further enhance organizational defenses (TechTarget, 2025). Real-time ad scanning, web application firewalls, and browser security settings further enhance organizational defenses (TechTarget, 2025).

However, cybercriminals continuously adapt their tactics, employing techniques such as polymorphic malware, modular payloads, and encrypted command-and-control channels to evade detection (Deepwatch Labs, 2025). As a result, technical defenses must be complemented by user education, policy interventions, and strategic partnerships with reputable ad networks to achieve sustainable protection (GeoEdge, 2024; TechTarget, 2025). A resilient defense posture also requires ongoing investment in threat intelligence and cross-sector collaboration to anticipate emerging attack vectors and ensure that mitigation strategies remain effective in the face of rapidly shifting adversarial techniques.

Threat intelligence platforms such as GeoEdge, Confiant, and Malwarebytes are significant in identifying, analyzing, and mitigating malvertising threats across digital advertising ecosystems (GeoEdge, 2024; Confiant Threat Intelligence Team, 2023;

Malwarebytes Threat Intelligence Team, 2023). These platforms provide automated threat detection, ad verification, and real-time intelligence feeds, empowering publishers, ad networks, and cybersecurity teams to block or remediate malicious ads before they reach end users (GeoEdge, 2024; Confiant, 2025). Academic research further affirms the importance of commercial and community-driven threat intelligence sources in aggregating data, enriching detection accuracy, and facilitating operational security across multiple attack categories (Guo et al., 2019).

Bridging these main findings to a critical perspective, the following section assesses the limitations and ongoing challenges that persist within each thematic area. As the threat landscape continues to evolve, it becomes increasingly important to scrutinize not only the effectiveness of current solutions but also the adaptability of organizations in responding to new forms of malvertising. A nuanced critique is essential for identifying gaps in existing strategies and for guiding future research toward more resilient and comprehensive defense mechanisms.

Critique: Detection and Mitigation Techniques

Despite the increasing sophistication of technical solutions for detecting and mitigating malvertising, several important limitations persist that undermine their overall effectiveness. One central issue is the heavy reliance on machine learning algorithms and behavioral analytics, which, while powerful, are fundamentally reactive and dependent on historical threat data (Vishwakarma & Dhakad, 2024). These systems may fail to identify new or evolving attack vectors that exploit zero-day vulnerabilities or employ previously unseen tactics, such as polymorphic malware and modular payloads, which can change their characteristics to evade detection (Deepwatch Labs, 2025). This lag in adaptation creates opportunities for attackers to bypass even advanced security measures.

The complexity of the digital advertising ecosystem further complicates defense efforts. The involvement of multiple intermediaries, including ad exchanges, supply-side platforms, and third-party vendors, results in a fragmented environment where accountability and visibility are often lacking (Liua et al., 2022). This fragmentation can delay the identification of malicious actors and hinder coordinated response efforts, as attackers exploit these structural weaknesses to distribute harmful ads across numerous platforms before detection mechanisms can respond (GeoEdge, 2024). The absence of standardized protocols for real-time threat intelligence sharing exacerbates this challenge, making it difficult for organizations to mount a unified and timely defense (Cybersecurity and Infrastructure Security Agency, 2024).

Technical defenses alone also fail to address the human element that malvertising frequently targets. Many campaigns rely on psychological manipulation, such as enticing offers or urgent calls to action, to prompt user engagement (GeoEdge, 2024). Without comprehensive user education and awareness programs, even the most advanced detection systems may be circumvented, as users remain vulnerable to social engineering tactics (Bârgăoanu & Pană, 2024). Policy interventions and industry-wide partnerships are essential to enforce higher standards for ad quality and network security; however, progress in these areas is often impeded by competing commercial interests and regulatory complexities (Cavaliere et al., 2024).

Finally, the sustainability of technical defenses is a growing concern. As cybercriminals continue to innovate, security teams face mounting pressure to keep pace with evolving threats. Resource constraints, alert fatigue, and the sheer volume of digital advertisements can overwhelm defenders, leading to gaps in coverage and delayed responses (GeoEdge, 2024). This environment highlights the need for a holistic approach that integrates technical, organizational, and educational strategies to achieve lasting protection against malvertising (Bârgăoanu & Pană, 2024; Vishwakarma & Dhakad, 2024).

Conceptual Framework

The conceptual framework underpinning this research is built upon the integration of cybersecurity, cognitive defense, and information governance to address the multifaceted threat of malvertising. At its core is the DISARM framework, which provides a structured methodology for analyzing disinformation incidents, facilitating collaborative intelligence sharing, and enabling a layered defense against technical and psychological attack vectors (Bârgăoanu & Pană, 2024; Cavaliere et al., 2024; Maigre, 2022).

This framework is distinguished by its multi-dimensional approach. It begins with automated detection systems that utilize machine learning and behavioral analytics to identify anomalous ad behaviors—such as rapid redirects, code obfuscation, and brand impersonation—across digital advertising platforms (Vishwakarma & Dhakad, 2024). Once a potential threat is flagged, the DISARM model is employed to conduct a deeper cognitive analysis. This employment involves examining the narrative content of suspicious ads, identifying manipulative messaging, and categorizing the psychological tactics in use, such as appeals to urgency or authority, which are common in influence operations (GeoEdge, 2024; DISARM Foundation, 2024).

The DISARM framework is modeled after the MITRE ATT&CK matrix and is designed to codify tactics, techniques, and procedures (TTPs) associated with disinformation and malvertising campaigns (Maigre, 2022; Fenza et al., 2025). It enables defenders to map incidents across phases, planning, preparation, execution, and evaluation, while documenting the technical artifacts and the psychological strategies present in each stage (Cavaliere et al., 2024; Bârgăoanu & Pană, 2024). This structure promotes a shared understanding among diverse stakeholders, including cybersecurity professionals, behavioral scientists, policymakers, and advertising networks, thereby facilitating rapid and coordinated responses to emerging threats (ACIG Journal, 2025).

A key strength of this conceptual framework is its emphasis on continuous adaptation. By incorporating feedback from real-world incidents and regularly updating its knowledge base of attack techniques and countermeasures, the framework ensures that defense strategies evolve in tandem with adversarial innovation (GeoEdge, 2024; Deepwatch, 2025). The approach also prioritizes cross-disciplinary collaboration, recognizing that sustainable resilience requires the collective expertise of technical, psychological, and governance domains (Bârgăoanu & Pană, 2024; Cavaliere et al., 2024).

In summary, this conceptual framework is optimal for malvertising defense because it unites advanced technical detection with cognitive analysis and collaborative policy development. Its layered structure, adaptability, and inclusivity of multiple disciplines make it well-suited to anticipate, identify, and counter the complex and evolving tactics employed in modern malvertising and cognitive hacking campaigns (Maigre, 2022; DISARM Foundation, 2024; Fenza et al., 2025). By fostering continuous feedback and knowledge exchange among technical experts, behavioral scientists, and policymakers, the framework ensures that defense strategies remain responsive to emerging threats and aligned with best practices across domains.

Conceptual Framework Critiques

The conceptual framework developed in this research is designed to provide a comprehensive and interdisciplinary defense against malvertising by integrating technical, psychological, and governance perspectives. While the framework is innovative in uniting these domains, it is essential to scrutinize its foundational assumptions and operational challenges. Such critique is critical for ensuring the framework's robustness and adaptability as cyber threats continue to evolve. This section addresses three principal critiques: the

complexity of stakeholder coordination, the risk of overreliance on automated detection systems, and the adaptability of the framework to evolving malvertising tactics.

Complexity of Stakeholder Coordination

A significant critique concerns the complexity of coordinating a diverse array of stakeholders within the integrated conceptual framework. The framework assumes effective collaboration among cybersecurity professionals, advertising networks, regulatory bodies, and end users, each with distinct mandates, resources, and risk tolerances (Bârgăoanu & Pană, 2024; Cavaliere et al., 2024). These differences can lead to misalignments in priorities, communication breakdowns, and delays in collective action. Establishing trust and overcoming organizational silos further complicates unified defense strategies (Cavaliere et al., 2024). The significance of this critique is substantial: without efficient stakeholder coordination, the framework's ability to facilitate rapid threat intelligence sharing and synchronized incident response is fundamentally limited. In fast-moving threat environments, any delays in communication or action can provide adversaries with opportunities to exploit vulnerabilities. Therefore, the challenge of stakeholder coordination represents not only an operational hurdle but also a foundational vulnerability that could undermine the overall effectiveness of the defense paradigm.

Overreliance on Automated Detection Systems

Another core critique involves the framework's reliance on automated detection systems as a primary defense mechanism against malvertising. While automation brings scalability and speed, it is inherently restricted by its dependence on historical data and algorithmic models, which may not fully capture the adaptive nature of emerging threats (Vishwakarma & Dhakad, 2024; Deepwatch Labs, 2025). Automated systems are prone to false positives and negatives, which can overwhelm security teams with alert fatigue or allow sophisticated attacks to evade detection (Sood & Enbody, 2011). Excessive automation also risks diminishing the essential role of human expertise, especially in interpreting ambiguous signals and contextualizing threats within broader operational and psychological contexts (Bârgăoanu & Pană, 2024). The importance of this critique lies in highlighting potential inefficiencies and vulnerabilities introduced by overautomation and in emphasizing the need for a balanced defense strategy that leverages technological and human analytical capacities. For this research, acknowledging this limitation is crucial for advocating a defense posture that is technologically advanced yet resilient to the limitations of automation.

Adaptability to Evolving Malvertising Tactics

A third critical critique addresses the framework's ability to adapt to the rapidly evolving tactics used by malvertisers. The cyber threat landscape is marked by constant innovation, with adversaries continuously developing new methods to circumvent detection and exploit emerging vulnerabilities (GeoEdge, 2024; Bârgăoanu & Pană, 2024). Frameworks lacking mechanisms for continuous learning, iterative improvement, and agile response risk becoming obsolete in the face of such dynamism. This challenge is heightened by the convergence of technical and psychological manipulation strategies, which require defenses to evolve in technical sophistication and understanding of human behavior and influence operations (Cavaliere et al., 2024). The significance of this critique is paramount: if the framework cannot anticipate and respond to new forms of attack, its long-term effectiveness and relevance are severely diminished. Addressing adaptability is essential to ensure that the proposed defense strategies remain future-proof and capable of safeguarding digital ecosystems against current and unforeseen malvertising threats.

The section on detection and mitigation techniques provides a focused overview of current strategies used to counter malvertising, highlighting technological and organizational approaches. It discusses the employment of machine learning algorithms, behavioral analysis, and network monitoring as primary tools for identifying and blocking malicious advertisements before they reach users (Vishwakarma & Dhakad, 2024; Perception Point, 2023). The summary also notes that cybercriminals continue to adapt by using advanced tactics such as polymorphic malware and encrypted command-and-control channels, which challenge the effectiveness of existing defenses (Deepwatch Labs, 2025). Furthermore, it emphasizes that technical solutions alone are insufficient, underscoring the necessity of user education, policy interventions, and strategic partnerships with reputable ad networks to achieve sustainable protection (GeoEdge, 2024; TechTarget, 2025). This section ultimately serves as a bridge to a critical analysis, setting the stage for a discussion of the limitations of technical controls on the limitations and ongoing challenges in malvertising defense.

Originality of the Text

This research distinguishes itself in four ways: (a) It offers a novel synthesis of malvertising within the broader context of cognitive hacking and disinformation, moving beyond conventional technical analyses to embrace an interdisciplinary perspective, (b) Unlike prior studies that predominantly focus on the detection and mitigation of malware delivery, this study deploys the DISARM framework to unite analysis of digital influence operations with actionable defense strategies, bridging cybersecurity and behavioral science (DISARM Foundation, 2024; Maigre, 2022). It integrates insights from cybersecurity, psychology, and information governance to address the multifaceted nature of malvertising threats (Bârgăoanu & Pană, 2024; Cavaliere et al., 2024). (c) The originality of this approach lies in its recognition that technical defenses alone are insufficient to counteract the evolving tactics of threat actors, who increasingly exploit technological vulnerabilities and human cognitive biases (GeoEdge, 2024; Sood & Enbody, 2011). (d) the study further emphasizes the convergence of malvertising with cognitive hacking and disinformation operations. By examining how malicious ads are used to manipulate public perception, spread false narratives, and erode trust in digital ecosystems, the study addresses a significant gap in the literature and offers actionable recommendations for practitioners and policymakers (Bârgăoanu & Pană, 2024; Blackbird.AI, 2025). The integration of technical, psychological, and policy dimensions allows for the development of holistic defense strategies that are adaptable to emerging threats and capable of anticipating the tactics of sophisticated adversaries (Vishwakarma & Dhakad, 2024; Zhou & Yang, 2023).

The rationale for this study emerges from the observed gap in scholarly and practical frameworks; existing models lack the flexibility to counteract rapidly evolving threats that manipulate user perception and leverage complex ad network vulnerabilities (Vishwakarma & Dhakad, 2024; Sood & Enbody, 2011). A central contribution of this study is the application and critical evaluation of the DISARM framework, which provides a structured methodology for analyzing disinformation tactics and facilitating collaborative intelligence sharing (Cavaliere et al., 2024; DISARM Foundation, 2024). By drawing parallels to established models such as MITRE ATT&CK, the research demonstrates how DISARM enables organizations to develop a common language and standardized definitions for describing influence operations, thus enhancing the coordination and effectiveness of multi-stakeholder defense strategies (Maigre, 2022; DISARM Foundation, 2024).

This interdisciplinary orientation is further reinforced by the inclusion of empirical case studies and thematic analysis, which illuminate the psychological manipulation strategies embedded within malvertising campaigns (GeoEdge, 2024; Portnox, 2024). In summary, this study's originality is grounded in its interdisciplinary methodology, the

innovative application of the DISARM framework, and its comprehensive treatment of malvertising as a technical and psychological threat. This foundation provides a seamless transition to the results section, where the practical implications and empirical findings of the research are explored in depth.

Furthermore, the research advances the field by advocating for continuous adaptation and interdisciplinary collaboration. It highlights the importance of user education, policy development, and international cooperation as essential components of a resilient defense posture (Cybersecurity and Infrastructure Security Agency, 2024; Sood & Enbody, 2011). The synthesis of these elements not only bridges existing gaps in malvertising research but also sets a precedent for future studies seeking to address the dynamic interplay between technical and cognitive aspects of cyber threats (GeoEdge, 2024; MDPI, 2024).

Solutions and Recommendations

The synthesis of recent research on malvertising reveals a threat landscape characterized by escalating technical sophistication and the growing use of psychological manipulation. Industry data from 2024 and early 2025 indicate a 10% year-over-year increase in malvertising incidents, highlighting the persistent and expanding threat to digital advertising ecosystems (GeoEdge, 2024; Vishwakarma & Dhakad, 2024; AdMonsters, 2025). Malvertising campaigns have evolved beyond simple redirects and pop-ups, now employing complex, multi-stage attacks that exploit programmatic advertising, real-time bidding platforms, and trusted ad networks to distribute malicious content at scale (Sood & Enbody, 2011; Liua et al., 2022).

Empirical studies and case analyses demonstrate that malvertising not only serves as a delivery mechanism for malware but also incorporates elements of cognitive hacking, using psychological manipulation to influence public opinion and disseminate disinformation (Bârgăoanu & Pană, 2024; Cavaliere et al., 2024; Blackbird.AI, 2025). The convergence of technical and psychological tactics complicates detection and mitigation efforts, as attackers exploit technological vulnerabilities and human cognitive biases (GeoEdge, 2024; Portnox, 2024). Misleading product offers and forced redirects remain dominant attack vectors, with campaigns increasingly leveraging social engineering and brand impersonation to deceive users (GeoEdge, 2024; SentinelOne, 2025). Forced redirects, in particular, have become the most prevalent method, automatically sending users to malicious landing pages without requiring user interaction, and are especially effective on mobile platforms where security protections are often weaker (AdMonsters, 2025).

The application of collaborative defense frameworks such as DISARM has shown promise in enhancing detection capabilities and enabling coordinated response efforts. DISARM's structured methodology allows for the categorization of disinformation tactics and supports intelligence sharing among stakeholders, thereby improving the speed and accuracy of threat identification (Cavaliere et al., 2024; DISARM Foundation, 2024). Real-world case studies illustrate how DISARM can be used to track and counter malvertising campaigns embedded within broader influence operations, demonstrating its value in hybrid threat environments (Bârgăoanu & Pană, 2024; ACIG Journal, 2025).

However, significant challenges persist. The increasing use of evasive malware, including polymorphic and encrypted payloads, complicates traditional signature-based detection methods and necessitates more adaptive and intelligent security solutions (Deepwatch Labs, 2025; WatchGuard Technologies, 2025). The rise of AI-enhanced cognitive hacking tactics, such as deepfakes and automated bot networks, further demands agile, interdisciplinary defense strategies that integrate technical, psychological, and policy perspectives (Breacher.ai, 2025; Portnox, 2024). Balancing automation with human oversight and ensuring privacy in intelligence sharing remain ongoing concerns.

These results underscore the necessity of continuous innovation and cross-sector collaboration to maintain effective defenses against malvertising. User education, policy development, and international cooperation are critical components of a resilient defense posture, complementing technical solutions and fostering a holistic approach to cybersecurity (Cybersecurity and Infrastructure Security Agency, 2024; Sood & Enbody, 2011). Ultimately, this research highlights the complex and evolving nature of malvertising threats and the imperative for adaptive, interdisciplinary strategies to safeguard digital ecosystems. The results of this research underscore the multifaceted nature of malvertising, revealing it as a threat that extends well beyond technical exploitation to encompass psychological manipulation and influence operations (Bârgăoanu & Pană, 2024; Cavaliere et al., 2024). The persistent growth in malvertising incidents, coupled with the increasing sophistication of attack vectors, highlights the urgent need for adaptive and interdisciplinary defense strategies (GeoEdge, 2024; Vishwakarma & Dhakad, 2024). Traditional security measures, such as machine learning-based detection and automated network monitoring, are essential but insufficient on their own, as cybercriminals continuously develop new techniques to evade these controls, including polymorphic malware and encrypted command-and-control channels (Deepwatch Labs, 2025).

One of the most significant implications of these findings is the necessity for a holistic approach that integrates technical, psychological, and governance perspectives. The convergence of malvertising with cognitive hacking demonstrates that attackers are not only exploiting system vulnerabilities but are also leveraging social engineering and psychological tactics to manipulate user behavior and erode trust in digital platforms (Bârgăoanu & Pană, 2024; Blackbird.AI, 2025). This dual-threat environment requires defense mechanisms that can anticipate and counter technical exploits and cognitive manipulation. The application of frameworks such as DISARM has shown promise in structuring incident analysis and facilitating collaborative intelligence sharing, thereby enhancing the speed and effectiveness of response efforts (Cavaliere et al., 2024; DISARM Foundation, 2024). However, the implementation of collaborative defense frameworks is not without challenges. Organizational silos, privacy concerns, and regulatory constraints can impede the timely sharing of threat intelligence, leading to delayed or fragmented responses (Cavaliere et al., 2024). These barriers must be addressed through the development of clear guidelines, best practices, and legal frameworks that encourage cooperation while safeguarding sensitive information. Additionally, variations in terminology, data formats, and analytical methodologies can hinder interoperability, emphasizing the need for ongoing dialogue and consensus-building among stakeholders (GeoEdge, 2024).

User education and awareness remain critical components of a resilient defense posture. Many malvertising campaigns rely on psychological manipulation, such as enticing offers or urgent calls to action, to prompt user engagement (GeoEdge, 2024; Bârgăoanu & Pană, 2024). Without comprehensive awareness programs, users are likely to remain vulnerable to social engineering tactics, regardless of the sophistication of technical controls. User education and behavioral interventions are indispensable components of a resilient malvertising defense strategy. While technical controls play a crucial role in detecting and blocking malicious advertisements, attackers frequently exploit human factors through psychological manipulation (Nobles & Burrell, 2024), making user awareness and behavioral change essential for comprehensive protection (Burton, 2022).

A robust user education initiative should be designed to empower individuals with the knowledge and critical thinking skills needed to recognize and resist malvertising tactics (Burrell & Nobles, 2022; Burton, 2022). This action includes training users to identify common red flags, such as unsolicited offers, urgent calls to action, and suspicious brand impersonations. Interactive modules can simulate real-world malvertising scenarios,

allowing users to practice safe browsing habits and decision-making in a controlled environment. Additionally, periodic awareness campaigns, delivered through email, intranet, or workplace seminars, can reinforce best practices and keep users informed about emerging threats (Burrell & Nobles, 2022; Burton, 2022).

Behavioral interventions should be grounded in insights from cognitive psychology, targeting specific vulnerabilities that malvertisers commonly exploit (Bargh & Ferguson, 2000). For example, educational materials can address cognitive biases like authority bias or scarcity effect, teaching users to pause and critically evaluate emotionally charged advertisements before engaging. Organizations may also implement just-in-time warnings within browsers or email clients, prompting users to reconsider risky actions when interacting with digital ads. User education programs should be regularly updated (Burton, 2022), to reflect the latest attack trends and tailored to the needs of different user groups, such as employees, executives, or high-risk departments to maximize effectiveness. As given by Lewis (2024), metrics such as click rates on simulated malvertising, completion rates of training modules, and post-training incident reports can be used to assess program impact and guide continuous improvement. Policymakers also play a vital role by establishing regulations that promote responsible Ad network management, data sharing practices, and minimum security standards for digital advertising platforms (Cybersecurity and Infrastructure Security Agency, 2024). Through the creation of clear legal frameworks and enforcement mechanisms, they can incentivize industry compliance and foster greater accountability among stakeholders. Effective policy measures not only help deter malicious actors but also encourage the adoption of best practices and technological innovations that enhance the overall security of the digital advertising ecosystem.

The findings further suggest that sustainable protection against malvertising will require continuous innovation and cross-sector collaboration. This includes not only technical advancements but also the integration of behavioral science insights and the fostering of international cooperation to address the global nature of digital advertising threats (Vishwakarma & Dhakad, 2024; Sood & Enbody, 2011). The dynamic and adaptive strategies employed by malvertisers demand that defense mechanisms remain flexible, incorporating real-time threat intelligence and iterative improvements to keep pace with evolving risks.

In conclusion, the discussion highlights the necessity of a comprehensive, adaptive, and interdisciplinary approach to defending against malvertising. By bridging gaps between technology, policy, and human behavior, stakeholders can develop more robust and sustainable strategies for mitigating the pervasive risks posed by malvertising and safeguarding the integrity of digital ecosystems (Bârgăoanu & Pană, 2024; Cavaliere et al., 2024; GeoEdge, 2024). Continued collaboration and innovation across these domains will be essential to keep pace with the rapidly evolving tactics employed by threat actors in the digital advertising landscape.

Future Research Directions

As malvertising continues to evolve, intersecting with cognitive hacking, disinformation, and advanced cyber threats, it is imperative for scholarship to explore uncharted areas that can enhance understanding and inform effective defense mechanisms (Caramancion et al., 2022). The insights from this research lay a foundation for multidisciplinary inquiry, highlighting the pressing need to adapt quickly to the shifting tactics of malicious actors and the vulnerabilities found in organizational, technological, and behavioral contexts. Future research should therefore extend beyond technical and procedural defenses, harnessing collaborative, empirical, and interdisciplinary approaches to keep pace with the ingenuity of threat actors and the complexity of modern attack surfaces. Five ideas for future research are noted.

Empirical Assessment of Integrated Frameworks

A critical trajectory for advancing this field involves empirically evaluating the effectiveness of integrated defense models, such as the DISARM framework, across diverse organizational environments. Future studies could deploy longitudinal case studies or quasi-experimental designs to measure outcomes in settings where technical, psychological, and policy responses are jointly implemented. Such research would provide robust evidence on the scalability, adaptability, and practical barriers of interdisciplinary approaches highlighted in recent analyses, addressing the recognized gap in empirical quantification of malvertising impacts and defense efficacy (Cavaliere et al., 2024; DISARM Foundation, 2024; Bârgăoanu & Pană, 2024).

Mobile Platform Vulnerabilities and Adaptive Threats

Given the increasing prevalence of malvertising in mobile environments, with adware accounting for 35% of mobile threat detections in 2024, future inquiry should focus on the unique vulnerabilities and mitigation strategies related to mobile platforms (GeoEdge, 2024). Studies might investigate the evolution of pre-click and post-click attack vectors, the comparative efficacy of detection tools for mobile versus desktop, and the specific psychological manipulations that influence mobile user behavior. This line of research would be salient for adapting frameworks like DISARM to the unique constraints and behaviors characterizing mobile technology adoption and risk exposure.

Human Factors and Cognitive Manipulation

Exploring the psychological dimension of malvertising remains an urgent avenue for research, particularly concerning how deceptive ads successfully manipulate user cognition, exploit decision-making biases, and degrade trust in digital ecosystems (Bârgăoanu & Pană, 2024; Kumar & Urwin, 2024). Future work should aim to identify the most potent psychological levers used in cognitive hacking, develop empirical models linking ad content features to user susceptibility, and test behavioral interventions that might inoculate users against malvertising-induced misinformation. These studies can inform the design of awareness campaigns, digital literacy programs, and adaptive defenses that go beyond technical barriers.

Automated Detection and Adaptive Adversary Strategies

Another pivotal research direction centers on the dynamic interplay between automated malvertising detection systems and the continually adaptive strategies of adversaries. As attackers refine their techniques to evade machine learning algorithms, with innovations like code obfuscation and rapid delivery pattern changes, future research should evaluate how detection technologies can evolve to pre-emptively recognize novel threat signatures (Kumar & Urwin, 2024; Deepwatch Labs, 2025). Examination of feedback loops between detection enhancements and attacker countermeasures will be crucial for sustaining protection in rapidly changing environments.

Societal and Policy Impacts of Malvertising-Driven Disinformation

Last, research must delve into the broader societal implications of malvertising, especially its convergence with disinformation campaigns and cognitive influence operations (Bârgăoanu & Pană, 2024; Cavaliere et al., 2024). Future studies could analyze how malvertising campaigns shape public perception, erode trust in digital information ecosystems, and contribute to the spread of false narratives during critical events. There is also a need for comparative policy analysis to identify regulatory best practices and their effectiveness in reducing the proliferation and impact of malicious ads.

By advancing these research directions, the academic and cybersecurity communities can more comprehensively address the complexity of malvertising as a technical and psychological threat, supporting the development of adaptive, collaborative, and resilient defense strategies. These efforts will foster a deeper understanding of how malicious actors exploit systemic vulnerabilities and user behaviors across evolving digital platforms. In turn, such scholarship will enable the design of proactive interventions and evidence-based policies that protect users, reinforce ecosystem trust, and ensure long-term resilience against emerging threats in the online advertising landscape.

Conclusions

The preceding analysis has illuminated the multifaceted and evolving nature of malvertising, revealing it as a threat that transcends traditional technical exploitation by incorporating psychological manipulation and disinformation into its operational arsenal (Bârgăoanu & Pană, 2024; Cavaliere et al., 2024). As digital advertising ecosystems continue to expand and diversify, the risks associated with malvertising are intensifying, necessitating the adoption of agile, interdisciplinary, and collaborative defense strategies. The persistent escalation in attack sophistication, manifested through polymorphic malware, brand impersonation, and AI-driven disinformation, has rendered conventional detection and mitigation approaches increasingly insufficient (GeoEdge, 2024; Deepwatch Labs, 2025). This dynamic landscape compels defenders to remain vigilant and proactive, continually refining their methodologies to keep pace with adversarial innovation.

The original contribution of this research is its holistic synthesis of malvertising as a technical and psychological phenomenon. By integrating cybersecurity, cognitive defense, and information governance perspectives, the research advances the field beyond traditional malware detection, offering a novel interdisciplinary framework that addresses the complex interplay between technology, human behavior, and policy (Bârgăoanu & Pană, 2024; Cavaliere et al., 2024). The application and critical evaluation of the DISARM framework exemplify how structured incident analysis and collaborative intelligence sharing can enhance detection and response capabilities across sectors (Cavaliere et al., 2024; DISARM Foundation, 2024). This approach fills a notable gap in the literature by examining malvertising's role within broader influence operations and cognitive hacking campaigns, providing actionable insights for practitioners and policymakers (Bârgăoanu & Pană, 2024; Blackbird.AI, 2025).

The findings of this research carry significant implications for policy and management. Stakeholders are encouraged to prioritize cross-sector partnerships, invest in adaptive technologies, and foster a pervasive culture of security awareness that extends from end users to industry leaders (Bârgăoanu & Pană, 2024; Cavaliere et al., 2024). Policymakers should focus on developing robust regulatory frameworks that promote responsible ad network management, secure data sharing practices, and enforce minimum security standards for digital advertising platforms (Cybersecurity and Infrastructure Security Agency, 2024; Sood & Enbody, 2011). For management teams, continuous user education and training are paramount to counteract the social engineering tactics that underpin many malvertising campaigns.

Despite these advancements, the study acknowledges persistent barriers to effective implementation. Organizational silos, privacy concerns, and the rapid evolution of adversarial tactics continue to hinder timely and coordinated responses to malvertising threats. These challenges significantly impede the resilience of digital advertising ecosystems and highlight the need for ongoing research, standardized assessment tools, and adaptive best practices (GeoEdge, 2024; Vishwakarma & Dhakad, 2024). Addressing such limitations will require not only technological innovation but also strong leadership and sustained cross-sector engagement.

Looking ahead, several fruitful avenues for further research emerge. These include the empirical evaluation of integrated defense frameworks, the development of metrics for assessing the societal impact of malvertising, and the exploration of international cooperation models to confront the global dimensions of digital advertising threats (Liua et al., 2022; Zhou & Yang, 2023). Investigating the real-world effectiveness of interdisciplinary and adaptive frameworks will be essential for refining best practices and ensuring sustainable protection. By fostering a dynamic, collaborative, and forward-looking approach, the digital ecosystem can be better safeguarded against the multifaceted and persistent risks posed by malvertising. Continued vigilance and adaptability will be indispensable as the threat landscape continues to evolve.

References

Atlan. (2025, June 24). Cross-border data transfers: Stay compliant globally in 2025. Author. https://atlan.com/know/data-governance/cross-border-data-transfers/

Bada, A., & Nurse, J. R. C. (2021). Developing cybersecurity education and awareness programs for small- and medium-sized enterprises (SMEs). Information & Computer Security, 29(1), 1–20. https://doi.org/10.1108/ICS-07-2020-0101

Bârgăoanu, A., & Pană, M. (2024). Cyber influence defense: Applying the DISARM framework to a cognitive hacking case from the Romanian digital space. Applied Cybersecurity & Internet Governance, 3, pp 91-121. DOI: https://doi.org/10.60097/ACIG/190196

Bargh, J. A., & Ferguson, M. J. (2000). Beyond behaviorism: On the automaticity of higher mental processes. Psychological Bulletin, 126(6), 925–945. https://doi.org/10.1037/0033-2909.126.6.925

Benaroch, M. (2021). Third-party induced cyber incidents—Much ado about nothing? Journal of Cybersecurity, 7(1), tyab020. https://doi.org/10.1093/cybsec/tyab020

Braun, V., & Clarke, V. (2025). Reporting guidelines for qualitative research: A values-based approach. Qualitative Research in Psychology, 22(2), 399–438. https://doi.org/10.1080/14780887.2024.2382244

Brilingaitė, A., Bukauskas, L., Juozapavičius, A., & Kutka, E. (2022). Overcoming information-sharing challenges in cyber defence exercises. Journal of Cybersecurity, 8(1), tyac001. https://doi.org/10.1093/cybsec/tyac001

Bryson, J. M., Crosby, B. C., & Stone, M. M. (2021). Designing and implementing cross-sector collaborations: Needed and challenging. Public Administration Review, 75(5), 647–663. https://doi.org/10.1111/puar.12432

Burrell, D. N., & Nobles, C. (2022). Assessing the Value of Executive Leadership Coaches for Cybersecurity Project Managers. In Research Anthology on Business Aspects of Cybersecurity (pp. 349–362). IGI Global. DOI: 10.4018/978-1-6684-3694-3.ch020

Burton, S. L. (2022). Cybersecurity Leadership from a Telemedicine/Telehealth Knowledge and Organizational Development Examination (Doctoral dissertation, Capitol Technology University). ProQuest Dissertations Publishing. Document ID: 29066056.

Caramancion, K. M., Li, Y., Dubois, E., & Jung, E. S. (2022). The missing case of disinformation from the cybersecurity risk continuum: A comparative assessment of disinformation with other cyber threats. Data, 7(4), 49. https://doi.org/10.3390/data7040049

Cavaliere, D., Fenza, G., Furno, D., & Loia, V. (2024, May). A semantic model bridging DISARM framework and Situation Awareness for disinformation Attacks Attribution. In 2024 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA) (pp. 55-62). IEEE. doi: 10.1109/CogSIMA61085.2024.10553682.

Confiant. (2025). Malvertising attack matrix: SamClub. Author. https://matrix.confiant.com/profile/scamclub.html

Confiant Threat Intelligence Team. (2023, September 27). ScamClub Threat Intelligence Report Overview. Author. https://www.confiant.com/news/scamclub-threat-intelligence-report-q1-q2-2023

Congressional Research Service. (2015, February 11). Cybersecurity and information sharing: Legal challenges and solutions (CRS Report R43941). Author. https://sgp.fas.org/crs/intel/R43941.pdf

Cybersecurity and Infrastructure Security Agency. (2024, May). Capacity Enhancement Guide Securing Web Browsers and Defending Against Malvertising for Federal Agencies. Author. https://www.cisa.gov/sites/default/files/publications/Capacity_Enhancement_Guide-Securing_Web_Browsers_and_Defending_Against_Malvertising_for_Federal_Agencies.pdf

Deepwatch Labs. (2025, April 24). Cyber Intel Brief: April 17–23, 2025. Author. https://www.deepwatch.com/labs/cyber-intel-brief-april-17-23-2025/

DISARM Foundation. (2024). DISARM Framework: Defending against influence operations through coordinated action. Author. https://www.disarm.foundation/

Edwards, M. (2025, May 21). Mapping SOC 2 controls to ISO 27001, NIST, and other frameworks. Information Security Management Systems. https://www.isms.online/soc-2/controls/

Falade, P. V. (2023). Decoding the threat landscape: ChatGPT, FraudGPT, and WormGPT in social engineering attacks. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 9(5), 185–198. https://doi.org/10.48550/arXiv.2310.05595

Fenza, G., Cavaliere, D., Furno, D., & Loia, V. (2025, February 28). Toward interoperable representation and sharing of disinformation incidents: A comparative analysis of frameworks and standards. arXiv:2502.20997v1. https://doi.org/10.48550/arXiv.2502.20997

GeoEdge. (2024). How AdTech fared against malvertising in early 2024. Author. https://www.geoedge.com/q1-malvertising-adtech/

Jones, L. A. (2020). Reputation Risk and Potential Profitability: Best Practices to Predict and Mitigate Risk Through Amalgamated Factors (Doctoral dissertation, Capitol Technology University). ProQuest Dissertations Publishing. ProQuest Document ID: 28152966

Kumar, A., & Urwin, M. (2024). Development beyond 2030: More collaboration, less competition? International Development Planning Review, 46(4), 421–437. https://doi.org/10.3828/idpr.2024.4

Liua, M., Hua, Z., Laia, Z., Zhenga, D., & Nie, X. (2022, November 30). Real-time bidding strategy in display advertising: an empirical analysis. University of Electronic Science and Technology of China. https://arxiv.org/pdf/2212.02222

Maigre, M. (2022, February). Hybric CoE Paper 11: Cyber threat actors: How to build resilience to counter them. European Centre of Excellence for Countering Hybrid Threats. HybridCoE. https://www.hybridcoe.fi/publications/hybrid-coe-paper-11-cyber-threat-actors-how-to-build-resilience-to-counter-them/

Moras, K. (2024, September 24). Evolving malvertising threats: How cybercriminals are exploiting online ads. SecureWorld. https://www.secureworld.io/industry-news/evolving-malvertising-threats-online-ads

Mukherjee, C., Mohamed, R., Arunasalam, A., Farrukh, H., & Celik, Z. B. (2025). Shadowed realities: An Investigation of UI attacks in WebXR. In USENIX Security Symposium. https://www.usenix.org/system/files/conference/usenixsecurity25/sec25cycle1-prepub-1236-mukherjee.pdf

Nobles, C. & Burrell, D. N. (2024). Exploring the Variability of Human Factors Definitions in Cybersecurity Literature. MWAIS 2024 Proceedings. 28. https://aisel.aisnet.org/mwais2024/28/

Noever, D., & McKee, F. (2025). Favicon trojans: Executable steganography via ico alpha channel exploitation. arXiv preprint arXiv. https://arxiv.org/abs/2507.09074

Pedael, M. (2025). Decoding ScamClub's malicious VAST attack. GeoEdge. https://www.geoedge.com/decoding-scamclubs-malicious-vast-attack/

SentinelOne. (2025, May). What is malvertising?: Examples, risks, and prevention. Author. https://www.sentinelone.com/cybersecurity-101/cybersecurity/malvertising/

Singh, V. K., Rivas, L., Khandelwal, V., & Kelly, B. K. (2025). Leveraging QR codes to bypass data loss prevention solutions. 2025 IEEE 15th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2025, pp. 00848-00853, doi: 10.1109/CCWC62904.2025.10903730.

Sood, A. K., & Enbody, R. J. (2011). Malvertising – exploiting web advertising. Computer Fraud & Security, 2011(4), 11-16. https://doi.org/10.1016/S1361-3723(11)70041-0

Spadafora, A. (2024, December 30). Over 600,000 Chrome users at risk after 16 browser extensions compromised by hackers: What you need to know. Tom's Guide.
https://www.tomsguide.com/computing/online-security/over-600-000-chrome-users-at-risk-after-16-browser-extensions-compromised-by-hackers-what-you-need-to-know

Vishwakarma, R., & Dhakad, R. (2024). Online Advertising and Fraud Click in Online Advertisement: A Survey. International Journal of Computer Applications, 186(1), 1–8. https://www.researchgate.net/profile/Ranjeet-Vishwakarma-2/publication/381368755_Online_Advertising_and_Fraud_Click_in_Online_Advertisement_A_Survey/links/66bc9d44311cbb094937bf98/Online-Advertising-and-Fraud-Click-in-Online-Advertisement-A-Survey.pdf

West, J., & Maurer, T. (2021). Cybersecurity and human rights in the digital age. Carnegie Endowment for International Peace. https://carnegieendowment.org/2021/03/11/cybersecurity-and-human-rights-in-digital-age-pub-84036

World Economic Forum. (2021, March). Principles for board governance of cyber risk. Author. https://www.weforum.org/publications/principles-for-board-governance-of-cyber-risk/

Zeng, J., Han, D.,Zhu, Y., Wang,Y., & Weng, F. (2024, April 27). A survey of third-party library security research in application software. arXiv:2404.17955. https://doi.org/10.48550/arXiv.2404.17955

Zhou, Y. & Yang, X. (2023). The evolution and innovation of marketing strategies in the digital era. Academic Journal of Business & Management, 6(6). DOI: 10.25236/AJBM.2024.060637