International Journal of Computers and Informatics (IJCI)
Vol. (4), No. (11)

IJCI

المجلة الدولية للحاسبات والمعلوماتية
الإصدار (4)، العدد (11)

November 2025

The Impact of Social Media Advertising on Customer Deception in the Context of Cybersecurity

Abdullah Albalawi
Shaqra University, Department of Computer Science, College of Computing and Information Technology, Shaqra, Riyadh 11961, Saudi Arabia
aalbalawi@su.edu.sa

Abstract

Social media advertising has changed the way businesses trade on consumers as the personalized and engaging content is delivered faster and wider than ever before. On the other hand, the very dynamic environment of advertising also allows creating space for several forms of deceptions, including fake promotion, misleading claims, and phishing campaigns. These tactics take advantage of consumer trust towards brands and platforms and create a misconception between genuine and fake. Such deceptive practices have a very severe cyber security impact because customers end up sharing their private information or downloading malicious software, putting them in danger from cyber threats. The dependency of social media on the consumer and advancement of deceptive techniques has highlighted the need for the improvement of consumers' awareness along with regulatory oversight. Deceptive advertising, from a cybersecurity point of view, has been increasingly challenging for the individual as well as organizations. Fraudulent advertisements induce almost all social media techniques in order to manipulate consumers, making it quite hard to detect a breach or become a victim of identity theft. Furthermore, the rapid spread of such false adverts facilitated by algorithms creates a wider reach and risk to a larger audience. Therefore, collaborated action on part of policymakers, social media platforms, and experts in cybersecurity address this emerging issue by strengthening regulatory frameworks, enriching and verification processes, and improving digital literacy. This initiative can reduce the possibilities of misleading customers and instilling an

atmosphere of trust in using social media as an advertising platform.

Keywords: Deceptive Marketing, Social Media, Cybersecurity Risk, Consumer Awareness.

1. Introduction

Social media advertising can be defined as a generic term that incorporates all forms of advertising – whether explicit (e.g., commercial videos or banner advertisements) or implicit (firm-related tweets or fan pages) that are delivered through social networking sites (SNS) (Taylor, Lewin, and Sutton, 2011, Wright et al., 2010 as cited in Rahman and Rashid [1]). According to Oletewo (2016) in Ekwueme and Okoro [2], social media advertising uses social networking sites Instagram, Facebook, Twitter, LinkedIn, etc. for creating awareness and reinforcing consumer loyalty towards a person, product or idea by means of persuasive communication.

Another definition of the term was presented by Otugo et al. [3] where he referred to social media advertising as the process of gaining traffic or attention to one's website through SNS, with efforts based on creating content that attracts attention and encourages readers to share it with their social networks. Unlike traditional advertising strategies, social media advertising allows businesses to connect with their potential customers through real-time interaction and personalized experiences. With the advent of smartphones and internet connectivity, social media became an important factor for businesses and brands' due to their competitive edge over others in reaching audiences [4].

A major strength of social media advertising lies in its precise targeting and effectiveness of the outcomes. Platforms use huge volumes of user data, allowing businesses to define their audiences according to demographics, interests, behaviors, and geographical locations. Creating the base of advertisements on these data-driven parameters ensures that an advertisement budget is healthy and is focused towards

maximizing ROI. Examples of formats used in social media advertising are videos, images, stories, live streams, and interactive content like quizzes and polls that give brands an extensive range of approaches to engaging with their audience. In addition to this, the availability of real-time performance metrics helps the marketers to not only adjust but, refine marketing strategies for improved results [5].

The market size of social media advertisements has rapidly increased in the recent years. It has grown from $228 billion in 2024 to $256.5 billion in 2025 at a compound annual growth rate (CAGR) of 12.5% [6]. This growth can be associated increased internet penetration, increased social media platforms, data analytics and insights as well as targeted advertising capabilities. Social media advertising also has its fair share of challenges. Due to increased competition, advertising cost is on the rise. Moreover, concerns about data privacy and ethical aspects of advertising have increased the scrutiny over platforms itself as well as on the advertiser. According to Chi [7] another phenomenon of users suffering from ad fatigue, where too much advertisement becomes counterproductive in its effectiveness. To mitigate all of these challenges, brands must focus on creating something interesting, valuable, and real that will fit their ethical styles in their targeted audience. With developments in artificial intelligence, augmented reality, and influencer partnership, he future of social media advertisement is definitely well-defined.

Marketing deception is defined as a practice in which a business would purposely mislead its consumers, thereby influencing their choices regarding a product's purchase. Deceptive marketing strategies include: false advertisement, misleading product descriptions, hidden charges, as well as exaggerated benefits from a product. Such practices damage consumer trust and can have serious repercussions which might involve legal sanctions, reputational damage, loss in customer loyalty, and other implications for the business itself [8]. Many countries have strong disciplinary regulations; however, deceptive practices still persist in different forms particularly in

highly competitive industries where the pressure to increase sales can put ethical considerations in a corner.

False advertising is a very common form of customer deception, where businesses usually make false claims about a product's attributes or performance levels. Overstating the health benefits by using baiting -switching, or showing exaggerated testimonials which do not reflect consumer experiences can be some examples of false advertising. Another example of deception is omission, which is concealing crucial information, like not mentioning hidden fees, unfavorable provisions in contracts, or the actual cost of a product. The digitized era now experiences the emergence of yet another method of deception: fake reviews and influencer endorsements that mislead customers, making it even harder for them to make informed choices [9]. According to the data presented by Baltezarević [10], apart from other factors, deceptive or misleading advertisements (46%) is the emergent factor in contributing towards customer dissatisfaction and subsequent negative perception of the brand.

Cybersecurity has emerged as a critical issue in the context of social media because of the huge deposits of personal as well as financial and behavioral information of the users. Social media is, a matter of fact, an interactive hub where individuals, businesses, and organizations share concepts with one another, hence, presenting an ideal opportunity for a cyberattack. Cyber threats include data breaches, identity theft, phishing scams, or the transmission of malware. A major area of concern in this case is data privacy. Most of the time, social media applications collect vast amounts of user information, which if not properly secured, can be hacked by cybercriminals or unauthorized third parties. Indeed, almost every major data breach of the recent times was an expose of different sensitive information that consumers have been providing over the years and costing financial losses, reputational damages, and denting public trust. Moreover, attacks on the social media space can be of a more serious

consequence, such as manipulating elections and disinformation, which overall speak to the need for very secure and transparent means of doing data handling [11].

In such developmental cases, it is essential that a social media company also places cybersecurity at its very core. This means using not only encryption at advanced levels but also multi-factor authentication, and an active system of monitoring to detect and take down threats. Cooperation between cybersecurity professionals and government agencies and user communities is equally important in order to combat emerging risks effectively. As it continues to evolve, strong embedded cybersecurity eventually ensures the safety and integrity, of the users themselves and of the social platforms, providing an even more secure cyberspace [12].

The purpose of this research is to explore the effect of social media advertising on customer deception. Therefore, the aim is to understand the implications of modern digital marketing techniques with respect to consumer behavior, which usually tends to be achieved through manipulated or deceptive means, hence, this particular study aims to find out the effect of these misleading practices on consumer trust and cybersecurity. It underlines the necessity of strong measures for the safeguarding of the users in the increasingly digitized marketplace.

This report converges marketing ethics with cybersecurity. Social media advertisements often tend to use behavioral psychology and data analytics for influencing customer decisions. In association with deceptive practices, this would lead to phishing attacks, identity theft, and financial fraud. Understanding the issues would help organizations identify vulnerabilities existing within their advertising ecosystems and put safeguards in place to protect their customers. The research also brings forefront the importance of regulatory frameworks in terms of reducing deceptive advertising practices by offering a secure digital environment.

Finally, this study underscores the importance of consumer awareness and education on dealing with deceptive advertising. While regulation and technology solutions are

important considerations, so too are perceptions of consumer empowerment in revealing suspicious ads. This research fills in the interplay between social media advertising and cybersecurity which contributes to a more rational understanding of how to make a digitally advertised environment more readily transparent, ethical, and secure.

1.1 Research Objectives

1. To examine the influence of social media advertising on the prevalence of deceptive practices among customers.
2. To explore the role of cybersecurity awareness in mitigating the deceptive effects of social media advertising.
3. To investigate the relationship between social media advertising and customer deception, focusing on the cybersecurity implications of deceptive practices on social media platforms.
4. To assess the effectiveness of cybersecurity awareness programs in reducing the occurrence of deceptive practices related to social media advertising.

2. Literature Review

2.1 Theoretical Perspectives:

Traditional marketing messages alone are no longer enough to create the organization's brand because of which social media marketing has become the center of attention for most companies nowadays. There are various definitions related to social media marketing. According to Evans [13, p. 13], social media marketing is a form of social media in which natural conversation tone is strategically used to offer benefits to the organization. Additionally, Cosme [14] defined social media marketing as the establishing of relationships between businesses and their current and/or prospective customers and harnessing the power of peer-to-peer influence. The nature of social media serves to provide an

opportunity to balance the organization's conventional marketing practices along with new media opportunities [14]. This new approach to social media marketing mobilizes corporations to interact with their target on-the-field audience and encourages those customers to spread the message about the brand [15]. This also provides a much "richer" picture of customer needs by "tapping into customer intelligence," through their conversations [16]. As a matter of fact, social media marketing also has its fair share of challenges where negative viral marketing can cause damage to an organization's reputation, without the possibility of much remedial intervention. Additionally, the risk of no participation in activities associated with the organization's social network sites due to the lack of necessary incentives is another challenge related to social media marketing [13, p. 158].

2.1.1 Marketing Theory Related to Social Media:

Social media marketing is embedded in various foundational marketing theories, which illustrates how consumers relate to brands and how they purchase online. These theories offer the foundation for understanding how social media inspire consumer behavior, engagement, and brand perception.

2.1.1.1 AIDA Model (Attention, Interest, Desire, Action):

This model describes the stages that consumers go through before making a purchase. The process initiates with an eye-catching, visually aesthetic content which then leads to the cultivation of the desire through targeted advertisements. Social media platforms such as Instagram and TikTok utilizes algorithms so as to assure that the content is in alignment with user preferences thereby, increasing the probability of the customers to move throughout the stages of the AIDA model [17].

- *Attention*: The advertisement should have an aspect of grabbing the viewer's attention right from the beginning. If the customer's attention is lost, the entire effort is gone. This can be done by creating an advertisement with the utmost

appeal for the promotion of the brand. The advertisement should immediately catch attention and promise a benefit for continued viewing. Many brands also go on to feature celebrities for increased viewership.

- *Interest*: After grabbing the attention of the target audience, the next step is to develop interest in the product of service offering. This part must use emotions to talk the fact that this purchase is a good bargain, a solid decision.
- *Desire*: There is a huge difference between being attracted in something and desiring it. The purpose of this step is to develop a passion and desire for what has been put out there. An advertisement should create a very strong motivation to buy the product even if the need is not there.
- Action: Brands should convince their customers through ads to make a purchase or become inquisitive enough to know more about the product/brand. No matter how attractive or customer-focused an ad may be.

2.1.1.2 Social Exchange Theory:

Social Exchange Theory is based upon the notion that people consider their relationships in economic terms. People typically weigh this relationship against the accrued benefits: Worth = Rewards-Costs. This means, according to the theory, that there will be a value that will determine the result -from whether or not to maintain or end the relationship [18].

The theory states that social interaction is usually made through the expectation of reward. Take social media marketing as an example: brands nurture a relationship with the consumer through value-adding content, discounts, or exclusive offers in exchange for likes, shares, or an actual purchase. For instance, it is primarily this principle that describes how influencer partnerships are made: influencers get paid while their audience gets access to curated recommendations involving products.

Brand trust is the brand's strength to be trusted. Trust in a brand can be established

when marketers creatively create and keep consistent positive emotional attachments with its consumers. When consumers trust the brand, the next step is to implement loyalty to the brand. According to a study by Hokky and Bernarto [19] trust in a brand will have an effect over behavioral loyalty and consumers action on the brand. Loyalty is a promise to repurchase or to subscribe to the product or service, even though there exists situational influences and marketing efforts that holds the potential to push consumers into switching to competing products or services. Consumers often create a perception toward the product that have a positive perception associated with [20]. Customer satisfaction is the key for greater retention.

2.1.1.2.1 Behavioral Theories on Deception:

The behavioral theories contribute towards useful insights to the understanding of the course of deception in social media marketing, by evaluating psychological, social, and contextual factors influencing deceptive practices. Below mentioned are some of the important behavioral theories that illustrate the issue of deception in social media marketing:

2.1.1.3 Social Exchange Theory and Deception in Social Media Marketing:

Social Exchange Theory affirms that people and organizations engage in decision-making based on a cost-benefit analysis weighing the perceived rewards against probable risks. Within the context of social media marketing, the theory explains why deceptive practices incur despite legal or ethical considerations.

2.1.1.3.1 Perceived Benefits of Deception:

Marketers and influencers consider deception to be the easiest way to achieve high results like:

a. Increased sales: False claims about a product may serve as bait for a customer

to purchase items that they would usually avoid. For instance, a customer might be manipulated by ads that say "instant results" in terms of the effectiveness of skincare products.

b. Improved Brand Visibility: Making eye-catching but exaggerated or deceiving advertising such as, "Most Popular Product of the Year" gains a lot of focus and very quickly boosts reach and other engagement metrics.

c. Strengthening of Sponsorship Deal: Influencers tend to constantly operate under pressure to meet performance metrics such as sales conversions or engagement rate.

Hence, misrepresenting product of service in a way that is over exaggerated, however false, is crucial to maintaining ties with brands [21].

2.1.1.3.2 Marketing Strategy and Deceptive Messages:

Implication of social exchange theory in social media marketing can include designing of marketing campaigns that tends to exploit consumer behavior. These can include:

a. *Psychological Exploitation*: Marketers may make their claims dramatic to make an emotional connection e.g., ("This product changed my life!") to get a good response from consumers.

b. *Manipulative Tactics*: This can include a sensation of urgency with claims like 'Only 2 left in stock!' or '90% of people love this product'. Such marketing claims have been used and prove to be heavily manipulated so as to get people to make quick purchase decisions.

c. *Engagement at All Costs*: This marketing campaign can include deceptive practices like fake giveaways or pretending that there are more people or product reviews which improves engagement metrics and are often associated with algorithms and brand partnerships [22].

2.1.1.3.3 Influencer Behavior and Deception:

This theory is also applicable to influencers who serves to be intermediaries in social media marketing. Influencers have to weigh a fine balance between self-interest and ethical practices in which financial incentives weigh more thereby, outperforming moral implications of promoting a misleading or false product [23].

2.1.1.3.4 Rationalized Cost of Deceptive Marketing:

Marketers engaging in deceptive practices through social media always underestimate or rationalize the consequences of the act. One common gamble is that a deceptive marketing will damage consumer trust to a greater extent because trust is a foundation for brand loyalty and long-term outcomes [24]. Another aspect is that the regulatory penalties for false advertisement like fines or warnings which are often minimal costs under the much bigger profits earned from misleading campaigns. Similarly, influencers and brands sometimes think that they can alleviate reputation damage by rebranding or even apologize or target a completely new audience base. These practices have damaging effects in the long run, as damage to trust and reputation is not rebuilt easily, especially in the transparent and fast-paced environment of social media [24].

2.1.1.4 Cognitive Dissonance Theory:

Cognitive dissonance theory refers to the psychological discomfort that is experienced when there exists conflicting beliefs or attitudes. This theory has significant implications within social media marketing. Research claims that social media platforms can exacerbate cognitive dissonance by presenting to the users conflicting information and diverse viewpoints hence, creating feelings of discomfort and uncertainty [25]. Social media users experience cognitive dissonance when they come across content that poses challenges to their existing

beliefs and viewpoints, prompting them to either completely reject opposing viewpoints or reevaluate their attitudes altogether [26].

Marketers very often tend to exploit cognitive dissonance by exaggerating product claims or targeting existing discomforts so as to control and influence customer behavior. The higher the claims about a product's benefit, the greater there exists a gap between the current state of the consumer and the desired outcome. This perceived disparity creates dissonance hence, stimulating consumers to make a purchase decision which will be the only way to reconcile the gap [27].

Marketing tends to employ deceitful activities as a means of reducing consumers' cognitive dissonance and creating impulsive buying or misplaced confidence. Fake social proof, in the form of fake testimonials, reviews, and sponsored influencers, will persuade a consumer that a product or service has been approved by others, thereby lowering their doubt of the product's value or effectiveness. Moreover, scarcity and creating a sense of urgency tactics like "only 5 left!" or "limited stock available" and "hurry up-the discount is valid for 24 hours only", manipulates the consumers' fear of missing out, compelling them to make quick decisions without further assessments of their conclusions and judgments [26].

2.1.1.4.1Cybersecurity Theories and Models:

Cybersecurity theories and models provides a structured framework to understand, analyze, and mitigate cyber risks. It integrates technical, organizational, and human aspects towards individual and organizational improvement in within response strategies. Some of the most important theories and models are:

2.1.1.5 CIA Triad:

This is a very foundational model underlying cybersecurity based on confidentiality, integrity, and availability. Confidentiality is to ensure that sensitive data could be made accessible only to authorized individuals and prevents

unauthorized access or disclosure to such information. This principle can be achieved through the use of encryption, access control, and secure authentication mechanisms. Through the integrity principle, data is presumed to be accurate and consistent and unaltered except when expressly permitted. Unauthorized modification, corruption, or destruction of information must be prevented by measures like checksums, hashing, and version control system.

The last principle, availability, guarantees access for authorized users to Information and resources whenever needed, thus minimizing the downtime or the probability of such disruption. Mechanisms that facilitate achieving this goal include redundancy, failover systems, and robust disaster recovery plans. In combination, these three components form a comprehensive framework to design, implement, and evaluate security policies and technologies in various settings and applications with a proper balance in protecting data and systems.

2.1.1.6 NIST Cybersecurity Framework (CSF):

The NIST Cybersecurity Framework (CSF) is a structured framework developed by the National Institute of Standards and Technology to assist organizations in managing and mitigating their risks associated with cybersecurity threats. It serves to be a comprehensive approach through defining five core functions -Identify, Protect, Detect, Respond, and Recover [28].

- *Identify*: In order to stay protected from potential cyber-attacks, the cyber security team gains an in-depth understanding about the important assets and resources of the organization. This function includes different categories like business environment, asset management, risk assessment, governance, risk management strategy as well as supply chain risk management.
- *Protect*: This function includes most of the physical and technical security controls for developing and implementing suitable protections of the

infrastructure. These categories include identity management and access control, data security, awareness and training, maintenance and protective technology along with information protection procedures.

- *Detect*: This function implements particular measures that gives signals to the organization about cyberattacks. Detect categories involve events. Security, constant monitoring along with detection processes.
- *Respond*: This function category includes appropriate responses to cyberattacks and other cyber security events. Particular categories include analysis, communication, response planning, mitigation and improvements.
- *Recover*: The activities within this function implement plans for cyber resilience whilst assuring business continuity in case of a cyber-attack, any security breach or cybersecurity events. Recovery functions include recovery planning improvements and communications.

This framework is widely implemented by organizations mainly due to its flexibility within varying organizational contexts. This model allows enterprises to align their cybersecurity measures with particular objectives and risk profiles, assuring a customized approach towards cybersecurity risk management. Through the implementation of NIST CSF practices, organizations can improve resilience against cyber security threats, streamline their compliance efforts and stimulate a culture of continuous improvement within the aspect of cybersecurity.

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Cybersecurity Supply Chain Risk Management	GV.SC
	Roles, Responsibilities, and Authorities	GV.RR
	Policies, Processes, and Procedures	GV.PO
	Oversight	GV.OV
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

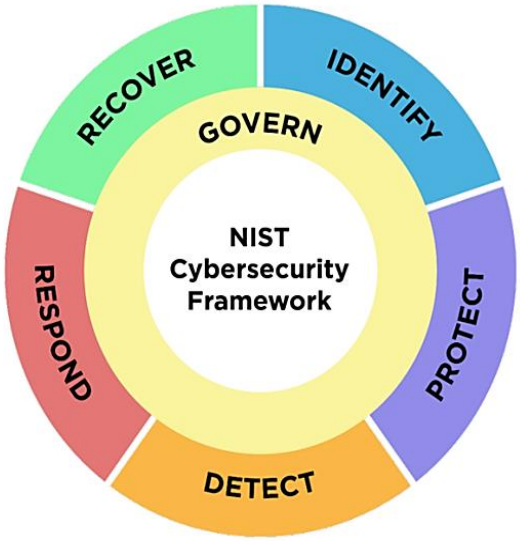

Figure (1): NIST Cybersecurity Framework.

3. Empirical Findings

Table (1): Studies on Social Media Advertising Effectiveness.

Key Themes	Findings	Source
Negative Appeals Effectiveness	Negative advertising appeals serves to be more effective as compared to positive appeals for driving engagement and actions on the social media platform. Several research indicated negative appeals within the context of charity and environmental concerns which resulted in superior outcomes in customer engagement along with having a positive impact over social behavior.	Yousef et al. [29]; Shahbaznezhad and Rashidirad [30]; Eckler and Bolls [31]
Ad Attributes and Consumer Perception	Attributes including liking, originality as well as credibility improve attitudes toward the advertisement, while irritation reduces engagement. Positive perceptions can lead to increased purchase intentions and brand recommendations whereas, negative perceptions deter customer engagement.	Pelet and Ettis [32]; Tran [33]
Platform Engagement Drives Ad Success	When consumers are actively participating on a social media platform, this increases interaction and response towards the advertisement.	Voorveld et al. [34]; David et al. [35]; De Vries and Jamie [36].

Sequential Advertising Strategies	Strategic sequencing of targeted ads can augment the returns on campaigns through information spillover.	Parshuram et al. [37]; Bimpikis et al. [38]
Product Type Influence	The effectiveness of advertising varies across product categories, where some product tends to benefit more significantly than others.	Huang et al. [39]; Muchnik et al. [40]
Short-Form Video Platform Ads	Large-scale experiments reveal the effectiveness of campaigns on short-form video social platforms.	Liang et al. [41]; Aral [42]; Gordon et al. [43]

Table (2): Research on Customer Deception in Advertising

Key Themes	Findings	Source
Consumer Trust	Deceptive advertising results in negative attitudes which results in reduced trust levels even on unrelated advertisements	Noorizzuddin bin Nooh [44]; Maicibi [45]
Long-term impact	Short term sales can increase through deceptive advertisements however, in the longer term, this can harm consumer demand, loyalty and brand reputation	Ukaegbu [47]; Xie and Boush [48]
Defensive processing	When consumers are exposed to deceptive advertising, they become highly skeptical and lose their trust in both the brand and its advertisement.	Darke and Ritchie [49]; Ritchie [50]
Regulatory guidelines	Federal Trade Commission emphasizes over the substantiation of advertising claims so as to prevent deception. The regulation imposes that advertiser should have a reasonable basis for their advertising claims.	Onuorah [51]; Boush et al. [52]
Consumer Expectations	Consumers expect advertisers that they avoid associating advertisements with any form of misleading content, which highlights the ethical responsibilities within advertisement.	Saydan and Dülek [53]; Plume et al. [54]; Domenico and Visentin [55]

Table (3): Previous Work on Cybersecurity Awareness among Consumers

Key Themes	Findings	Source
Consumer trust in the business	Research indicates the trust in businesses increases when they tend to employ certified cybersecurity professionalship is a demonstration towards the business's commitment in safeguarding sensitive data ensuring consumers about the reliability and credibility of the business. Approximately 76% of consumers consider cybersecurity to be crucial for national security.	Moffatt and Adedoyin [56]; Anderson et al. [57]; Bada and Nurse [58]; Blythe et al. [59]
Impact of cybersecurity breaches on behavior	The impact of breach is profound on consumer trust, where one in three consumers choose to stop doing business with such enterprises. The availability of alternates who tend to be secure poses threats to companies having cybersecurity issues.	Handoko and Putri [60]; Internet Security Threat Report [61]
Effectiveness of Awareness Campaigns	Awareness campaigns of cybersecurity most often struggle in achieving desired outcomes mainly due ineffective communication strategies that fails to resonate with the audience. Also overlooking of psychological motivators such as habit, fear or convenience tends to influence behavior significantly.	Bada et al. [62]; Kirlappos et al. [63]; Khan et al. [64]

3.1 Gaps in the Literature:

3.1.1 Limitations of Existing Studies:

Some of the limitations of existing research about cybersecurity awareness among consumers can be illustrated as follows:

- Lack of Diversity in Sample Populations: Most of the studies have been confined to a particular group of demographics or geographical locations. This means that it severely limits the generalizability of the findings across diverse populations.
- Reliance on Self-Reported Information/Data: Most studies rely heavily on self-reported behavior, which is often susceptible to a social desirability bias in one's tendency to either overestimate or underestimating of true practices.
- Limiting Longitudinal Analysis: Of the conducted studies, very few studies have followed up on changes in consumer awareness and behavior over time making it difficult to know the long-term value of such awareness campaigns.
- Emphasis on General Awareness: A majority of the research studies seem concerned with general awareness regarding cybersecurity; however, they lack in indicate specific threats or behaviors such as ransomware or phishing.
- Neglecting Psychological Factors: Most of the researches have disregarded psychological driving forces such as fear, trust, and so on, which constitute critical bases for establishing the right cyber security behaviors.

These limitations have underscored the need for more comprehensive, diverse longitudinal study methodologies in consumer cybersecurity awareness research.

3.1.2 Need for Integrating Cybersecurity with Advertising and Deception:

In the era of digital advertising, protection of sensitive data is a topmost concern. A lot of customer data is usually collected and processed in the course of digital advertising campaigns. These include, but are not limited to names and addresses, contact details, and, occasionally, payment-related and browsing behavioral data [65, 66]. Protecting this data does not only involve the primary ethical requirement of respecting customer privacy; it is also imperative to maintain customer trust and loyalty [67]. In the era where data breach has become very common, public scrutiny can tarnish a brand's image beyond redemption. Customers are generally less forgiving of such lapses, especially when their personal and financial information is involved. An event of data breach results in reduced customer engagement, a decline in sales, and an erosion of trust in the brand over time [68, 69]. Digital marketing data breaches carry significant legal and financial consequences. The enactment of data protection laws such as the GDPR within the European Union and CCPA in the United States has made more businesses realize and understand how difficult compliance is with strict demands for data protection. Investing in cybersecurity is, therefore, no longer only a defensive measure against a potential threat but a business strategy with effects at a far-reaching level. Adequate protection from customer-sensitive data assures compliance with legal standards, protects from financial loss, and preserves customers' trust and loyalty. Robust cybersecurity practices are no longer just an option for digital marketing; they are a necessity for sustainable and responsible business practice [70].

By far the most critical issue that advertisers have is the sheer quantity of consumer data, where it is at risk of being misused. Integration of cyber security practices, therefore safeguards this data and makes sure that all the regulations of privacy are followed, so as to protect individuals from exploitation [71]. It offers a platform where cyber security and advertisement can blend and educate an average person on

possible online threats, such as phishing and misuse of data, so that they may take appropriate action. In this manner, the two merge into a more secure and transparent digital space, dealing with ethical and practical problems in a connected world [72, 73].

4. Development of the Theoretical Framework

4.1 Conceptual Definitions:

4.1.1Social Media Advertising:

Social media advertising refers to using social media platforms to present paid advertisements that influences the way in which audience perceive, behave and decide. It uses special tools, algorithms, and info about users on each platform to send custom messages to specific groups of people. The goal is to meet marketing targets like getting people to know about a brand, interact with it, become potential customers, and generate leads. Unlike the conventional way of advertising, social media advertising is different because people can interact with them, focuses over precise audiences, real-time analytics along with the ability to foster two-way communication between the customers and the brand [74].

4.1.2 Customer Deception:

Customer deception indicates a situation when a business, advertiser, or entity uses misleading or false information to control how consumers think, decide, or act. This can involve overstating facts omitting out key details, making false claims, or using manipulative tactics to paint a distorted image of a product, service, or brand. Companies often do this to get ahead of competitors, boost sales, or reach other business goals at the cost of consumer trust, ethical standards or following regulations [75].

4.1.3 Cybersecurity Awareness:

Cybersecurity awareness refers to the understanding and knowledge organizations and communities have about possible cyber threats, vulnerabilities along with the necessary steps to protect digital, assets sensitive data and systems. This includes identifying risks like phishing, malware, social engineering, and data breaches as well as taking proactive actions to stay safe such as using strong passwords, encrypting data, and keeping software up to date. Cybersecurity awareness plays a key role in creating a secure digital environment and help stakeholders reduce risks [76].

4.2 Proposed Framework Components:

4.2.1 Relationships between Social Media Advertising Strategies and Customer Deception:

The growth of social media has transformed the way we communicate, connect and use information. However, this also comes with some cons mainly referring to deceptive advertising practices. Many companies are now using deceptive advertising practices to promote their products and services by benefitting from the extensive social media reach and how it can influence people.

Influencer deception has a significant impact on customer deception on social media. Brands tend to collaborate with influencers to showcase their products. While many influencers are honest and genuine and transparent whereas, some other may resort to deceptive practices. They might promote a product making it appear to be an unbiased recommendation. This lack of transparency can mislead the consumers into thinking that the product is of high quality and meet their requirements [77].

Fake testimonials and reviews are another form of deceptive advertising practices on social media platforms. Brands create fictitious accounts or pay individuals to give positive reviews about the product or service. These reviews are misleading and

creates a false sense of popularity. Consumers tend to rely over these reviews and make purchasing decisions which results in deception due to fake feedback [78].

Identifying deceptive advertising practices involves looking for user-generated reviews which are created by real customers. This can include images, videos or hand-written testimonials by customers who appreciate the brand. In this way, consumers can get an authentic perspective about the effectiveness and quality of the product or service. The case of Fyre Festival is exemplary in deceptive social media marketing. The festival organizers used social media celebrities and influencers to promote the event as a luxurious and glamorous festival however, when the attendees arrived, they were welcomed by a poorly organized and underwhelming event. The case highlights the power of deceptive marketing on social media and the consequences for both the brands and the customers [79].

In conclusion, social media platforms have become a breeding ground for deceptive advertising practices. From influencer deception to that of fake testimonials, brands are finding new ways to deceive consumers and manipulate their purchasing decision. By remaining informed and relying on genuine user-generated reviews, consumers can make informed decisions about brands and services.

Table (4): Frontier for Deceptive Marketing Practices

Steps	Key points	Description
1	Social media transformation	The rise of social media has undoubtedly transformed the way we communicate, connect, and consume information.
2	Influencer deception	Influencer deception is one of the most prevalent forms of deceptive marketing on social media.
3	Fake reviews	Fake reviews and testimonials are another deceptive marketing tactic that thrives on social media platforms.
4	Tip to identify deception	One tip to identify deceptive marketing practices on social media is to look for genuine user-generated content.
5	Fyre Festival case	The infamous case of the Fyre Festival serves as a cautionary tale of deceptive marketing on social media.
6	Consumer vigilance	It is crucial for consumers to be vigilant and skeptical when encountering marketing messages on social media.
7	Final Thought	In conclusion, social media has become a breeding ground for deceptive marketing practices.

4.2.2 Role of Cybersecurity Awareness in Moderating These Relationships:

Cybersecurity awareness has a very critical role in social media advertising as it can safeguard business practices, its audience as well as its campaigns from any potential threats. Awareness about cybersecurity can improve social media advertising in a way that it protects brand reptation, cybersecurity breaches such as phishing campaigns and hacked social media accounts can ruin the image of a brand. Awareness about cybersecurity along with proactive measures assures that the accounts are secure and the consumers' trust are preserved.

Brand advertisements can be misused by hackers so as to spread malicious links. When advertisers are aware about cybersecurity measures, they assure that advertisements are thoroughly vetted and the platforms are responsibly used. Additionally, cybercriminals may also make fake accounts or use bots for inflating metrics including clicks and views, resulting in wasted spending over the advertisement. Awareness is crucial for advertisers to recognize and deal with such fraudulent activities hence, optimizing the performance of marketing campaign [80].

Social media advertising involves collecting consumer data for targeted campaigns. Being aware of cybersecurity best practices helps in safeguarding this sensitive information, preventing of costly breaches along with remaining in compliance with privacy regulations. Moreover, being aware of cybersecurity laws like CCPA and GDPR also helps in avoiding penalties as well as boosting ethical business practices.

5. Implications of the Framework

5.1 Theoretical Implications:

5.1.1 Contribution to the Fields of Marketing and Cybersecurity:

This study indicates how social media advertising can be deceptive for consumers and offers valuable insights for both social media advertising and cybersecurity. With

respect to marketing, the study aims to deepen understanding about how deceptive advertising practices can impact consumers' trust. Gaining this understanding can help advertisers to prioritize ethical communication and transparency and take the responsibility for honest and open communication with the brand's audience. Moreover, the paper explains the role of cybersecurity concerns in the shaping of consumer attitudes hence, paving way for marketers to formulate advertisement campaigns that emphasizes over building trust and security.

With regards to cybersecurity, the paper aims in addressing how social media advertising are used as a method of spreading malware and conducting phishing attacks. Through identifying these vulnerabilities, the study contributes towards building formulating safety mechanisms to mitigate the issues. However, it is critical to determine aggressive and proactive media education strategy for protecting the end users, and not only the media consumers, but generally the general public, why deceptive advertisements exist and how to avoid cyber risks. Likewise, the research may be used to refine regulatory frameworks so as to assure that basic advertising policies are not violated and comply with a high standard of safety.

5.1.2 Insights for Further Research:

The paper open avenues for various aspect in future research. One avenue is to explore consumer psychology, particularly how they tend to perceive risk associated with any form of deceptive advertising along with the impact of cybersecurity awareness on their decision-making process. By understanding these psychological factors, brands can develop strategies that can mitigate these risks.

Another focus area can be the role of technology in combating deceptive advertising. Future researches can focus upon how artificial intelligence (AI) and machine learning (ML) tools can be helpful in detecting and preventing fraudulent activities along with how these tools can be better integrated within social media platforms.

Moreover, investigating the effectiveness of existing cybersecurity measures on social media networks can be useful in providing valuable insights for improving cybersecurity measures. These evaluations can help in creating a safer and a more transparent environment for both the advertisers and the consumers.

5.2 Practical Implications:

Recommendations for marketers on ethical advertising:

- Recommendation # 1: Prioritize Ethical Marketing Practices: Marketers needs to prioritize ethical marketing practices in order to build trust and promote long-term relationships with their customers. The key is being transparent. Advertisements should clearly communicate its purpose and intent and should avoid any type of deceptive visuals or misleading claims.
- Recommendation # 2: Consumer Privacy: Respect for consumer privacy is also crucial with adherence to data protection regulations like GDPR or CCPA. Advertisers should obtain explicit consent prior to collecting or using customer data.
- Recommendation # 3: Promote authenticity: Advertisers should promote authenticity by aligning brand values with advertising claims which is helpful in avoiding consumer deception.

The Key strategies for enhancing consumer cybersecurity awareness:

- Educational Campaigns: Initiating of focused and creative campaigns that would help educate consumers about how to identify phishing scams, fake ads, and other cyber threats. Make use of infographics, videos and other interactive material to make complicated concepts easier.
- Platform Integration: Partnering with social media companies in order to provide the users with integrated security tips, such as popup messages advising against certain suspicious links or encouraging strong password practices.

- Rewarding Consumer Interaction: Consumers should be provided with incentives, likes discounts or exclusive content after they participate in cyber security training seminars or answer quizzes about internet safety.
- Consistent Communication: Updating consumers regarding any rises in potential threats or inform them about the latest measures the brand undertakes regarding cybersecurity. The more transparent the message, the more trust the consumers will have and more alert they will be.

6. Conclusion

Summary and Reiteration of the proposed framework Cybersecurity awareness plays a very critical role in social media advertising as it protects business practices, its audience, and its campaigns from any possible threats. Cybersecurity awareness can help improve social media advertising in the way that it protects brand reputation, cybersecurity breaches such as phishing campaigns and hacked social media accounts which can destroy the image of a brand. Awareness regarding cyber security as well as preventive steps ensure that accounts are secure and the consumers' trust is maintained. Hackers can misuse brand advertisements as a way of spreading malicious links. When the advertisers are cyber-aware, they ensure that advertisements are well screened and that the platforms are appropriately used. Additionally, cybercriminals may create fake accounts or apply bots to inflate metrics such as clicks and views that wastes spending over the advertisement. Thus, awareness is imperative for the marketers to be on the lookout to detect and rectify such malpractice hence optimizing their marketing campaign's performance. Social media advertising requires collecting consumer data for targeted campaigns. Knowing the best practices of cybersecurity helps in safeguarding this sensitive information, prevents costly breaches along with remaining in compliance with privacy regulations. Also, knowing the cybersecurity laws such as CCPA and GDPR helps in avoiding penalties as well as boosting ethical business practices.

Conflict of Interest:

The author declares no conflicts of interest.

Funding:

This research received no external funding.

Acknowledgments:

We would like to extend our sincere gratitude to Shaqra University for their unwavering support throughout the research and preparation of this publication. The resources and academic environment provided by the university have played an integral role in shaping the outcome of this work. We are thankful for the opportunity to contribute to the scholarly community, and we recognize the invaluable contribution of Shaqra University in making this endeavor possible.

References

1. M. Rahman and M. Rashid, "Social media advertising and its effectiveness: A case study of South Asian teenage customers," *Global Journal of Management and Business Research*, vol. 8, no. 4, 2018.
2. C. Ekwueme and N. Okoro, "Analysis of the use of social media advertising among selected online businesses in Nigeria," *European-American Journals (EA Journals)*, 2018. [Online]. Available: https://www.eajournals.com.
3. E. Otugo, C. E. Uzuegbunam, and C. O. Obikeze, "Social media advertising/marketing: A study of awareness, attitude and responsiveness of Nigerian youths," *ResearchGate*, 2014. [Online]. Available: https://www.researchgate.net.
4. V. Bajpai, S. Pandey, and S. Shriwas, "Social media marketing: Strategies and its impact," *International Journal of Social Science and Interdisciplinary Research*, vol. 1, no. 7, 2012.
5. R. Kaushik, "Impact of social media on marketing," *IJCEM International Journal of Computational Engineering and Management*, vol. 15, no. 2, 2012.
6. The Business Research Company, *Social Media Advertisement Global Market Report 2024–2025*, The Business Research Company, 2025. [Online]. Available:

https://www.thebusinessresearchcompany.com/report/social-media-advertisement-global-market-report.

7. H. Chi, "Interactive digital advertising versus virtual brand community: Exploratory study of user motivation and social media marketing responses in Taiwan," *Journal of Interactive Advertising*, vol. 12, no. 1, 2011.
8. Y. B. Limbu, M. Wolf, and D. L. Lunsford, "Consumers' perceptions of online ethics and its effects on satisfaction and loyalty," *Journal of Research in Interactive Marketing*, vol. 5, no. 1, pp. 71–89, 2011.
9. P. Riquelme, S. Román, and D. Iacobucci, "Consumers' perceptions of online and offline retailer deception: A moderated mediation analysis," *Journal of Interactive Marketing*, vol. 35, pp. 16–26, 2016.
10. R. Baltezarević, "Deceptive advertising in the online environment," in *3rd International Black Sea Modern Scientific Research Congress, Proceedings: IKSAD – Congress Book*, M. Jikia, Ed., Samsun, Türkiye, Mar. 23–24, 2023, pp. 360–369. [Online]. Available: https://tr.blackseacountries.org/_files/ugd/614b1f_fc7ff5c034724b94959560eca665b2e3.pdf.
11. Salam, M. Panda, Y. Elbarawy, A. E. Hassanien, and A. Abraham, "Computational social networks: Security and privacy," in *Computational Social Networks: Security and Privacy*, Springer, 2012. [Online]. Available: https://link.springer.com/chapter/10.1007%2F978-1-4471-4051-1_1.
12. A. J. Y. Zaidieh, "Combatting cybersecurity threats on social media: Network protection and data integrity strategies," *Journal of Artificial Intelligence and Computational Technology*, vol. 1, no. 1, pp. 8-14, Oct. 2024.
13. D. Evans, *Social Media Marketing: An Hour a Day*. London: Wiley, 2008.
14. G. Cosme, "Social media: An introductory guide for your business, organisation or agency," 2008. [Online]. Available: http://www.ginocosme.com/downloads/Introductionto-Social-Media.pdf.
15. D. Charton, "Why social networking matters for SA marketers," *Marketing Web*, 2007. [Online]. Available: http://www.marketingweb.co.za.
16. Mullins, "Effective marketing for Web 2.0," 2008. [Online]. Available: http://www.bizcommunity.com.
17. P. Kotler, *Marketing Management*, Prentice Hall International, 2004.

18. G. Heggde and G. Shainesh, *Social Media Marketing: Emerging Concepts and Applications*, 1st ed. Singapore: Springer Nature, 2018.
19. L. A. Hokky and I. Bernarto, "The role of brand trust and brand image on brand loyalty on Apple iPhone smartphone users in DKI Jakarta," *Journal of Management*, vol. 12, no. 1, pp. 474–482, 2021.
20. Kotler and K. Keller, *Marketing Management*. London: Pearson, 2016.
21. M. S. Sohail, M. Hasan, and A. F. Sohail, "The impact of social media marketing on brand trust and brand loyalty: An Arab perspective," *International Journal of Online Marketing (IJOM)*, pp. 15–31, 2020.
22. H. Haudi, W. Handayani, M. Musnaini, and Y. T. Suyoto, "The effect of social media marketing on brand trust, brand equity and brand loyalty," *International Journal of Data and Network Science*, pp. 1–12, 2022.
23. A. C. Antunes, "The role of social media influencers on the consumer decision-making process," in *Research Anthology on Social Media Advertising and Building Consumer Relationships*, IGI Global, 2022, pp. 1420-1436.
24. C. Clune and E. McDaid, "Content moderation on social media: Constructing accountability in the digital space," *Accounting, Auditing & Accountability Journal*, vol. 37, no. 1, pp. 257–279, 2023. doi: 10.1108/AAAJ-11-2022-6119.
25. C. A. Bail, L. P. Argyle, T. W. Brown, and A. Volfovsky, "Exposure to opposing views on social media can increase political polarization," *Proceedings of the National Academy of Sciences (PNAS)*, vol. 115, no. 37, 2018. [Online]. Available: doi: 10.1073/pnas.1804840115.
26. E. C. Tandoc Jr., "Tell me who your sources are: perceptions of news credibility on social media," *Journalism Practice*, vol. 13, no. 2, pp. 178-190, 2019.
27. S. Lewandowsky, U. K. H. Ecker, C. M. Seifert, N. Schwarz, and J. Cook, "Misinformation and its correction: Continued influence and successful debiasing," *Psychological Science in the Public Interest*, 2012. doi: 10.1177/1529100612451018.
28. National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, Apr. 16, 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.
29. M. Yousef, T. Dietrich, and S. Rundle-Thiele, "Social advertising effectiveness in driving action: A study of positive, negative and coactive appeals on social media," *International Journal of Environmental Research and Public Health*, vol. 18, no. 11, p. 5954, Jun. 2021. doi: 10.3390/ijerph18115954.

30. H. Shahbaznezhad, R. Dolan, and M. Rashidirad, "The Role of Social Media Content Format and Platform in Users' Engagement Behavior," *Journal of Interactive Marketing*, vol. 53, pp. 47-65, 2021.
31. P. Eckler and P. Bolls, "Spreading the virus: Emotional tone of viral advertising and its effect on forwarding intentions and attitudes," *Journal of Interactive Advertising*, vol. 11, pp. 1–11, 2011. doi: 10.1080/15252019.2011.10722180.
32. J.-É. Pelet and S. Ettis, "Social media advertising effectiveness: The role of perceived originality, liking, credibility, irritation, intrusiveness, and ad destination," *International Journal of Technology and Human Interaction*, vol. 18, 2022. doi: 10.4018/IJTHI.2022010106.
33. P. Tran, "Personalized ads on Facebook: An effective marketing tool for online marketers," *Journal of Retailing and Consumer Services*, vol. 39, pp. 230–242, 2017.34. H. A. M. Voorveld, G. van Noort, D. G. Muntinga, and F. Bronner, "Engagement with social media and social media advertising: The differentiating role of platform type," *Journal of Advertising*, vol. 47, no. 1, pp. 38–54, 2018. doi: 10.1080/00913367.2017.1405754.
34. D. C. David, N. Ollikainen, J. C. Trinidad, M. P. Cary, A. L. Burlingame and C. Kenyon, "Widespread protein aggregation as an inherent part of aging in *C. elegans*," *PLoS Biology*, vol. 8, no. 8, e1000450, Aug. 2010.
35. N. J. De Vries and J. Carlson, "Examining the drivers and brand performance implications of customer engagement with brands in the social media environment," *Journal of Brand Management*, vol. 21, no. 6, pp. 495–515, 2014.
36. Hotkar, R. Garg, and K. L. Sussman, "Strategic social media marketing: An empirical analysis of sequential advertising," *Production and Operations Management*, vol. 32, no. 12, 2023. doi: 10.1111/poms.14075.
37. Bimpikis, A. Ozdaglar, and E. Yildiz, "Competitive targeted advertising over networks," *Operations Research*, vol. 64, no. 3, pp. 705–720, 2016.
38. S. Huang, J. Hu, and E. van den Hof, "Social Advertising Effectiveness Across Products: A Large-Scale Field Experiment," *Marketing Science*, vol. 39, no. 5, pp. 923-947, Oct. 2020.
39. Muchnik, S. Aral, and S. J. Taylor, "Social influence bias: A randomized experiment," *Science*, vol. 341, no. 6146, pp. 647–651, 2013.
40. Y. Liang, X. Chen, S. Han, J. Zhang, and Y. Chen, "Effectiveness of advertising campaigns on short-form video social platforms: An empirical analysis through a large-scale randomized field experiment on Byte Dance," SSRN, Nov. 23, 2023. doi: 10.2139/ssrn.4641827.
41. S. Aral, "What digital advertising gets wrong," *Harvard Business Review*, Feb. 19, 2021. [Online]. Available: https://hbr.org/2021/02/what-digital-advertising-gets-wrong.

42. B. R. Gordon, F. Zettelmeyer, N. Bhargava, and D. Chapsky, "A comparison of approaches to advertising measurement: Evidence from big field experiments at Facebook," *Marketing Science*, vol. 38, no. 2, pp. 193–226, 2019.
43. N. bin Nooh and K. F. Nooh, "The criteria and challenges of unethical advertising," *American Journal of Business, Economics and Management*, pp. 88–93, 2014.
44. N. A. Maicibi, "Criminal and unethical behaviours in organisations: Misuse of assets and false or misleading advertising," *Global Journal of Human Social Science: Political Science*, pp. 1–9, 2013.
45. R. Ukaegbu, "Deceptive Advertising and Consumer Reaction: A Study of Delta Soap Advertisement," *Open Access Library Journal*, vol. 7, pp. 1-7, 2020.
46. G. X. Xie and D. M. Boush, "How susceptible are consumers to deceptive advertising claims? A retrospective look at the experimental research literature," *The Marketing Review*, vol. 11, pp. 293–314, 2011. doi: 10.1362/146934711X589480.
47. P. Darke and R. Ritchie, "The defensive consumer: Advertising deception, defensive processing, and distrust," *Journal of Marketing Research*, vol. 44, pp. 114–127, 2007. doi: 10.1509/jmkr.44.1.114.
48. J. B. Ritchie, "Giving advertisers the benefit of the doubt: Trust, cooperative communication, and consumer acceptance of implication in advertising," Ph.D. dissertation, Sauder School of Business, Univ. of British Columbia, Vancouver, Canada, 2004.
49. E. Onuorah, "Imperatives of advertising regulation," *International Journal of Communication: An Interdisciplinary Journal of Communication Studies*, vol. 20, no. 1, 2017.
50. D. M. Boush, M. Friestad, and P. Wright, *Deception in the Marketplace: The Psychology of Deceptive Persuasion and Consumer Self-Protection*. London: Routledge, 2015. doi: 10.4324/9780203805527.
51. Saydan and B. Dülek, "The impact of social media advertisement awareness on brand awareness, brand image, brand attitude and brand loyalty: A research on university students," *International Journal of Contemporary Economics and Administrative Sciences*, vol. 9, no. 2, pp. 470–494, Dec. 2019.
52. C. J. Plume, Y. Dwivedi, and E. Slade, *Social Media in the Marketing Context*. Amsterdam: Chandos Publishing, 2017.
53. G. Di Domenico and M. Visentin, "Fake news or true lies? Reflections about problematic contents in marketing," *International Journal of Market Research*, vol. 62, pp. 409–417, 2020. doi: 10.1177/147078532093471.

54. Moffatt and F. Adedoyin, "The impact of a cyber-attack on consumer's online spending in the UK during the COVID-19 pandemic," *SSRN Electronic Journal*, May 1, 2021. [Online]. Available: https://ssrn.com/abstract=4374763 or doi: 10.2139/ssrn.4374763.
55. E. S. Anderson, J. D'Arcy, and K. Kelley, "When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches," *MIS Quarterly*, vol. 41, no. 3, pp. 893–916, 2017.
56. M. Bada and J. R. C. Nurse, "Developing Cybersecurity Education and Awareness Programmes for Small- and Medium-sized Enterprises (SMEs)," *Information and Computer Security*, vol. 27, no. 3, pp. 393–410, 2019.
57. J. M. Blythe, S. D. Johnson, and M. Manning, "What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices," *Crime Science*, vol. 9, no. 1, 2020.
58. H. Handoko and D. Putri, "Threat language: Cognitive exploitation in social engineering," in *Proc. Int. Conf. Social Sciences, Humanities, Economics and Law*, 2019.
59. Symantec Corporation, *Internet Security Threat Report*, vol. 28, Mountain View, CA, USA: Symantec, 2023.
60. M. Bada, A. M. Sasse, and J. R. C. Nurse, "Cyber security awareness campaigns: Why do they fail to change behaviour?" *International Conference on Cyber Security for Sustainable Society*, 2015. doi: 10.48550/arXiv.1901.02672.
61. Kirlappos, S. Parkin, and M. A. Sasse, "Learning from shadow security: Why understanding non-compliance provides the basis for effective security," *Workshop on Usable Security*, 2014.
62. B. Khan, S. K. Alghathbar, S. I. Nabi, and M. K. Khan, "Effectiveness of information security awareness methods based on psychological theories," *African Journal of Business Management*, vol. 5, no. 26, pp. 10862–10868, 2011. [Online]. Available: http://www.academicjournals.org/article/article1380536009_Khan%20et%20al.pdf.
63. Lies, "Marketing intelligence and big data: Digital marketing techniques on their way to becoming social engineering techniques in marketing," *International Journal of Interactive Multimedia and Artificial Intelligence*, vol. 5, no. 5, pp. 134–144, 2019. doi: 10.9781/ijimai.2019.05.002
64. R. Sachdev, "Towards security and privacy for edge AI in IoT/IoE-based digital marketing environments," in *Proc. 5th Int. Conf. Fog and Mobile Edge Computing (FMEC)*, 2020, pp. 341–346. doi: 10.1109/FMEC49853.2020.9144755.

65. E. Mogaji, T. O. Soetan, and T. A. Kieu, "The implications of artificial intelligence on the digital marketing of financial services to vulnerable customers," *Australasian Marketing Journal*, vol. 29, no. 3, pp. 235–242, 2021. doi: 10.1016/j.ausmj.2020.05.003.
66. Hammou, S. Aboudou, and Y. Makloul, "Social media and intangible cultural heritage for digital marketing communication: Case of Marrakech crafts," *Marketing and Management of Innovations*, vol. 2020, no. 1, pp. 99–109, 2020. doi: 10.21272/mmi.2020.1-09.
67. Y. J. Purnomo, "Digital marketing strategy to increase sales conversion on e-commerce platforms," *Journal of Contemporary Administration and Management (ADMAN)*, vol. 1, no. 2, pp. 54–62, 2023.
68. C. Raul, *the Privacy, Data Protection, and Cybersecurity Law Review*. London: Law Business Research Limited, 2021. [Online]. Available: https://datamatters.sidley.com/wp-content/uploads/sites/2/2019/11/The-Privacy-Data-Protection-and-CybersecurityLaw-Review-Edition-6.pdf.
69. H. Habibzadeh, B. H. Nussbaum, F. Anjomshoa, B. Kantarci, and T. Soyata, "A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities," *Sustainable Cities and Society*, vol. 50, p. 101660, 2019. doi: 10.1016/j.scs.2019.101660.
70. O. K. T. Kilag, N. V. Indino, A. M. Sabagala, C. F. K. Abendan, M. T. Arcillo, and G. A. Camangyan, "Managing cybersecurity risks in educational technology environments: Strategies and best practices," *American Journal of Language, Literacy and Learning in STEM Education*, vol. 1, no. 5, Article 5, 2023.
71. Mugarza, J. L. Flores, and J. L. Montero, "Security issues and software updates management in the industrial Internet of Things (IioT) era," *Sensors*, vol. 20, no. 24, p. 7160, 2020. doi: 10.3390/s20247160.
72. E. van der Walt, J. H. P. Eloff, and J. Grobler, "Cyber-security: Identity deception detection on social media platforms," *Computers & Security*, vol. 78, pp. 76–89, 2018. doi: 10.1016/j.cose.2018.05.015.
73. C. M. Harmeling, J. W. Moffett, M. J. Arnold, and B. D. Carlson, "Toward a theory of customer engagement marketing," *Journal of the Academy of Marketing Science*, vol. 45, no. 3, pp. 312–335, 2017.

74. E. F. Academy, "A Decade-by-Decade History of Cybersecurity," *Eleven Fifty Academy*, Jan. 25, 2021. [Online]. Available: https://elevenfifty.org/blog/a-decade-by-decade-historyof-cybersecurity/.
75. H. Kim and M. Park, "Virtual influencers' attractiveness effect on purchase intention: A moderated mediation model of the product–endorser fit with the brand," *Computers in Human Behavior*, vol. 143, p. 107703, 2023. doi: 10.1016/j.chb.2023.107703.
76. W. J. Johnston, S. Khalil, A. Nhat Hanh Le, and J. M. S. Cheng, "Behavioral implications of international social media advertising: An investigation of intervening and contingency factors," *Journal of International Marketing*, vol. 26, no. 2, pp. 43–61, 2018.
77. A. Stanwick and S. D. Stanwick, "Fyre Festival: The party that never got started," *American Journal of Humanities and Social Sciences*, vol. 3, no. 12, pp. 138–142, 2019.
78. B. Awojobi and J. Ding, "Data Security and Privacy," in *Cybersecurity for Information Professionals: Concepts and Applications*, Taylor & Francis Group CRC Press, 2020, pp. 291–304. doi: 10.1201/9781003042235-13.