ZIBELINE INTERNATIONAL™ PUBLISHING

ISSN: 2616-5155
CODEN: MECJBU

Malaysian E Commerce Journal (MECJ)

DOI: http://doi.org/10.26480/mecj.01.2023.46.49

REVIEW ARTICLE

FACING SECURITY CHALLENGES IN DIGITAL MARKETING AND HOW TO OVERCOME THEM

Hilda, Girang Permata Gusti

Universitas Tanjungpura, Pontianak, Indonesia
**Corresponding Author Email: hilda.judiarto@ee.untan.ac.id*

ARTICLE DETAILS

Article History:

Received 23 September 2023
Revised 26 October 2023
Accepted 13 November 2023
Available online 16 November 2023

ABSTRACT

Digital marketing has become a critical component of modern business strategy, but it has also raised new challenges regarding cybersecurity. This research aims to investigate security challenges in digital marketing and the efforts made to overcome them. The research method used is a quantitative descriptive approach with secondary data collection. Data collected includes industry reports, articles, and previous studies related to cybersecurity in digital marketing. This data is analyzed to identify patterns and trends related to security threats and the strategies used by companies to deal with them. The research results show that digital marketing is faced with various security risks, such as data leaks, cyber-attacks, and fraud. Efforts to overcome these challenges include the use of advanced security technology, employee training on security awareness, and collaboration with third parties who are experts in the field of cybersecurity. This research provides an in-depth understanding of security in digital marketing and provides recommendations for companies to improve their security systems.

KEYWORDS

Digital Marketing, Cybersecurity, Security Challenges, Secondary Data Collection, Quantitative Descriptive.

1. INTRODUCTION

Digital marketing has become one of the dominant marketing strategies in the era of information technology and the Internet. Technological advances have allowed companies to reach broader audiences, measure campaign performance more accurately, and interact directly with consumers across digital platforms. However, along with the advantages and convenience offered by digital marketing, new challenges also arise, especially in terms of security.

Security is a major concern as more and more sensitive consumer data is collected and used in digital marketing. Data security breaches and misuse of personal information are serious threats to companies and consumers. Apart from that, the existence of spam, phishing, and online fraud practices also threaten the integrity of digital marketing and can damage a company's reputation. Security challenges in digital marketing are also related to increasingly stringent regulations and privacy policies in various countries. Countries and regulatory authorities have passed laws and regulations that require companies to properly protect consumer data and provide transparency in the use of data.

To overcome security challenges in digital marketing, companies need to take proactive steps and invest in a strong cybersecurity strategy. Implementing advanced security technologies, such as data encryption, firewalls, and threat detection, is an important first step. Apart from that, companies must also provide security training to employees and promote awareness of security risks.

Additionally, clear privacy policies and terms of use should be implemented to provide transparency in the collection and use of consumer data. Companies must comply with applicable data protection regulations and laws in their areas of operation and guarantee that consumer data is only used by the consent provided. It is also important for companies to always keep up with the latest technological developments and security threats. Implementing an effective monitoring and analysis system can help detect potential security threats quickly and take appropriate countermeasures.

Digital marketing offers companies a great opportunity to achieve success in an increasingly competitive market. However, security challenges related to the collection and use of consumer data must be taken seriously. By adopting a strong cybersecurity strategy, complying with privacy regulations, and providing transparency to consumers, companies can create a safe and trustworthy digital marketing environment, thereby building good relationships with consumers and increasing the success of their digital marketing campaigns.

2. THEORETICAL BASIS

In facing security challenges in digital marketing, several theories can be used as a reference for overcoming these problems. One suitable theory is the Technology Acceptance Model (TAM) (Mathieson, 1991; Szajna, 1996). This theory proposes that the adoption of technology by individuals depends on their perception of the ease of use and benefits they will obtain from the technology.

In the context of digital marketing, TAM can be used to understand how consumers respond to and adopt security initiatives implemented by companies. If consumers believe that the security measures taken by a company will protect their data well and benefit them in the long term, then they are more likely to accept and participate in those security programs.

Digital Marketing is a marketing strategy that uses digital technology and online platforms to promote products, services, or brands to a target audience. In digital marketing, various digital methods and channels are

Quick Response Code	Access this article online	
	Website: www.myecommerecejournal.com	**DOI:** 10.26480/mecj.01.2023.46.49

Cite The Article: Hilda, Girang Permata Gusti (2023). Facing Security Challenges in Digital Marketing and How to Overcome Them. *Malaysian E Commerce Journal, 7(1): 46-49.*

used to achieve marketing goals, including social media, search engines, paid advertising, email, digital content, and others. One of the main advantages of digital marketing is its ability to reach a wider and more targeted audience. With various digital platforms, companies can reach potential consumers throughout the world, as well as direct specific advertising and content to target segments that are relevant to the products or services offered.

Digital marketing also offers the ability to measure and analyze campaign performance more accurately. Through web analytics tools and digital advertising platforms, companies can track the number of ad impressions, user interactions, conversions, and more. This data helps companies identify effective strategies and make adjustments to make campaigns more successful. Digital marketing enables two-way interaction between companies and consumers. Through social media and other digital communication platforms, consumers can provide feedback, ask questions, or communicate directly with companies. This interaction allows companies to get closer to consumers, understand their needs, and increase customer satisfaction.

However, digital marketing faces various challenges, especially when it comes to security and data privacy. With more and more consumer data being collected and used in digital marketing, data protection and privacy have become crucial. Data security breaches or misuse of consumer information can damage a company's reputation and reduce consumer trust. To face these challenges, companies need to adopt a strong cybersecurity strategy and comply with applicable data protection regulations. In addition, prioritizing transparency in the use of consumer data and providing options for consumers to control the use of their data can increase customer trust and loyalty.

In the ever-growing digital era, digital marketing is the key for companies to remain relevant and compete in the global market. By understanding the potential and challenges of digital marketing, companies can design effective and sustainable strategies to achieve their marketing goals and build strong relationships with consumers.

Cybersecurity is an effort to protect computer systems, networks, software, and data from threats that come from cyberspace. In the context of digital marketing, cybersecurity is essential to protect consumers' personal information and data from threats such as hacking, data theft, malware, and other cyber attacks. Cybersecurity involves a set of actions, policies, and technologies aimed at preventing, detecting, and responding to security threats that may arise in the digital environment. One important aspect of cybersecurity in digital marketing is the protection of personal data. Today, companies often collect personal information from consumers, such as names, addresses, telephone numbers, and financial information. This data must be properly safeguarded and only used for lawful purposes.

Cybersecurity also plays an important role in protecting websites and marketing applications from cyberattacks. DDoS (Distributed Denial of Service) attacks, hacking, and the spread of malware are examples of threats that can damage a company's reputation and disrupt its operations. By having a strong cyber security system, companies can prevent these threats and maintain the smooth running of their digital marketing operations. Apart from that, cyber security is also related to protecting consumer transaction data and financial information. In a digital marketing environment, financial transactions are often carried out online, such as payments via credit card or bank transfer.

Cybersecurity challenges in digital marketing continue to grow as technology advances and hacking tactics become more sophisticated. Therefore, companies must always improve their cybersecurity capabilities by adopting the latest technologies and practices in protecting their data and systems. Apart from that, involving cybersecurity experts and conducting training for internal teams is also an important step in dealing with ever-changing security threats. By understanding the importance of cybersecurity in digital marketing, companies can protect consumer data, maintain business reputation, and provide a safe and enjoyable transaction experience for consumers.

3. Literature Review

In this literature review, three studies related to digital security will be discussed. The first research begins with a study of big data technology which is starting to enter the world of old computer systems that operate critical infrastructure (Michalec et al., 2022). These innovations promise fast Internet connectivity, remote operations, or predictive maintenance. Because traditional critical infrastructures are typically disconnected from the Internet, the prospect of their modernization requires an investigation into cybersecurity and how it relates to traditional engineering requirements such as safety, reliability, or resilience. Looking at how the adoption of big data technologies in critical infrastructure shapes the understanding of risk management, we focus on a specific case study of cybersecurity governance: the European Union Network and Information Systems Security Directive. We argue that the implementation of the Network and Information Systems Security Directive is the first step in the integration of safety and security through new risk management practices. Therefore, this is a step towards legitimizing the modernization of critical infrastructure. However, we also show that security risk management practices cannot be directly removed from the realm of safety, as cybersecurity is based on anticipating future attack behavior rather than historical equipment failure rates. Our analysis offers several postulates for the emerging research agenda on big data in complex engineering systems. Based on a conceptualization of safety and security based on materialist literature in the fields of Science and Technology Studies and Organizational Sociology,

A subsequent study (Spencer, 2022) presents an analysis of recent transformations in the field of cybersecurity assurance, which aims to determine the safety of technical products. This research is based on a series of narratives concerning issues in cybersecurity assurance, obtained through interviews with practitioners based in the United Kingdom. The research focuses on characterization: the stories told by these practitioners, the roles of characters in these narratives, and how these narratives give rise to problems within the cybersecurity domain. Mistrust, as revealed by this study, can be understood in terms of the skeptical narratives' capacity to undermine the value of security certifications, rendering them not directly acceptable. Consequently, this research develops a perspective on mistrust based on text and distinguishes it from disposition-centered views. Through an examination of mistrust, critical questions emerge regarding the diverse characters present in the field of cybersecurity, not just about changing dispositions to be "more trusting," as in conventional views. This research highlights the importance of characterization in shaping expert anticipations in policy formulation and the potential for developing "counter-characterization," for instance, around "concerned characters."

Finally, a research study (Whyte, 2022) attempts to delve into the racial politics underlying shifts in cybersecurity related to online disinformation issues and 'foreign influence' in U.S. politics. Using the case study of the Black Lives Matter (BLM) movement, the first part of this article discusses how contemporary cybersecurity creates 'racialized securitization' by viewing the BLM movement as a geopolitical vulnerability open to foreign manipulation through social media. By emphasizing political protests as sites of insecurity, the author argues that contemporary cybersecurity has expanded its traditional spatiality 'beyond the computer.' In the second part of the article, the author contends that racialization in cybersecurity has become the foundation for a politics of truth that is ultimately more concerned with defining the boundaries of safe political knowledge and communication than distinguishing between right and wrong. The author argues that contemporary cybersecurity has created an idealized subject with an obligation to possess contingent knowledge as a condition of safe political subjectivity. The article concludes with criticism of the tendency of contemporary cybersecurity to depict politically diverse movements like BLM as uninformed or misinformed.

4. Research Methods

This research uses a quantitative descriptive approach with secondary data collection. A quantitative descriptive approach was used to get a clear picture of security challenges in digital marketing and the efforts that have been made to overcome them. With this approach, researchers can collect data that can be measured and calculated statistically to provide a deep understanding of the security issues faced by companies in digital marketing.

Secondary data is used in this research because information about security in digital marketing has been widely published and is available in the form of reports, articles, and previous studies. The data includes a variety of sources such as academic journals, industry reports, and publications from government agencies related to cybersecurity. The use of secondary data allows researchers to access extensive and up-to-date information about security challenges in digital marketing from a variety of trusted sources.

5. Discussion

In Indonesia, the issue of personal data breaches has become a serious concern due to repeated occurrences. According to data from the Ministry of Communication and Information Technology, there have been 79 cases of data theft within the country since 2019. This number has been steadily

increasing, with 35 cases occurring in just the first six months of 2023, surpassing the total number of cases from the previous three years (2019-2021). Several prominent cases include the 2022 data breach of Indonesian citizens' SIM card information, involving the hacker Bjorka, which resulted in the exposure of data from 1.3 billion SIM card registrants, with a value of up to Rp743.5 million. Additionally, in 2023, there was a data breach involving the customers of Bank Syariah Indonesia, where the ransomware group Lockbit managed to steal 1.5 terabytes of personal data and demanded a ransom of Rp296 billion. In the same year, Bjorka was also involved in the data breach of 34 million passports, which were uploaded for sale at a price of Rp150 million. Most recently, in July 2023, there was a data breach of 337 million Dukcapil (Population and Civil Registration) records, uploaded by the group RRR on the Breach Forums website. This breach included personal information such as names, Family Card numbers, dates of birth, addresses, parents' National ID numbers, birth certificate numbers, marriage information, and religious affiliations. The issue of data breaches serves as a warning for the government and companies to enhance the security of personal data and protect critical information for the public (Febriari, 2023).

Personal data leaks that often occur in Indonesia are one of the security challenges in digital marketing. Cases such as leaks of SIM card data, bank customer data, and other personal data show that there needs to be stronger steps in protecting consumer data. This challenge is increasingly complex with increasing internet penetration in Indonesia and people's dependence on digital services.

One solution to overcome security challenges in digital marketing is to increase awareness and education about the importance of data security among the public and business people. Consumers need to be educated about the risks of data leaks and the steps they can take to protect their personal information. On the other hand, companies also need to be educated about best practices in managing and protecting customer data.

There is a need to adopt advanced technology and security infrastructure to protect personal data from attacks by hackers and hackers. Implementing robust cybersecurity is key to preventing data leaks and protecting consumer privacy. The use of advanced encryption technologies, firewalls, and threat detection systems can help prevent unauthorized access to personal data.

Companies also need to conduct regular security audits to identify potential vulnerabilities and security gaps in their systems. By conducting a security audit, companies can take the necessary precautions to address security issues before data leaks occur. In addition, companies need to comply with applicable regulations and security standards. For example, in Indonesia, there is a Personal Data Protection Law that regulates the management and protection of personal data. By complying with these regulations, companies can ensure that their customer data is processed correctly and securely.

Furthermore, to face digital marketing security challenges, companies need to improve the capabilities of their cybersecurity teams. Training and certification for cybersecurity professionals will help improve their skills and knowledge in dealing with ever-evolving security threats. Collaboration between related parties is also very important in overcoming security problems. Companies, governments, and other relevant institutions need to work together to identify and address security threats effectively.

No less important is consumers' awareness and active role in protecting their data. Consumers need to be more careful about providing their personal information and use security measures such as using strong passwords and enabling two-factor authentication.

Overall, security challenges in digital marketing in Indonesia require a comprehensive approach involving education, technology, regulatory compliance, collaboration, and consumer awareness. With these steps, it is hoped that we can reduce the risk of personal data leakage and protect consumer privacy so that people can feel more secure and confident in digital transactions.

6. Author's Opinion

Digital marketing has become a key pillar in modern business strategy, but with its growth also comes serious security challenges. Security in digital marketing includes various threats such as data theft, personal information leakage, cyber attacks, and phishing attempts that can result in huge losses to customers and damage a company's reputation. To face this challenge, companies must take proactive steps in securing their data and digital marketing activities. First, companies must prioritize data security by implementing a strong security system, including data encryption and two-factor authentication. Apart from that, protecting financial transactions must also be prioritized by ensuring the use of safe payment methods and a strict verification process.

Security awareness is also key in overcoming this challenge. Customers need to be empowered with knowledge about the importance of digital security and ways to identify potential attacks or fraud attempts. Companies can increase customer awareness through educational campaigns and providing information about proper security practices. Additionally, the use of web analytics tools can help companies monitor activity on their digital marketing platforms and detect potential security threats.

Complying with industry security standards is also critical to maintaining data integrity and customer trust. Companies must follow and comply with security standards set by relevant authorities, especially if they collect sensitive data such as credit card data. In addition, companies must also have emergency plans ready to use in the event of a security breach, so they can respond quickly and effectively.

By taking security challenges in digital marketing seriously and taking appropriate steps, companies can protect their customers, build trust, and maintain their reputation in an increasingly complex and risky digital era. Security is a crucial aspect of digital marketing, and a company's success in overcoming this challenge will be a determining factor in achieving success in its digital marketing strategy.

7. Conclusion

In conclusion, digital marketing has become an effective and important approach in the modern business world. However, amidst technological advances and dependence on the internet, security challenges have become a serious threat that must be overcome. Data theft, personal information leaks, cyberattacks, and phishing attempts can harm customers and damage a company's reputation. Therefore, companies must take proactive steps in securing their data and digital marketing activities.

The first step is to prioritize data security by implementing a strong security system and strict financial transaction protection. Additionally, increasing security awareness among customers is important, by educating them about proper security practices. The use of web analytics can also help detect potential security threats.

Furthermore, companies must comply with applicable industry security standards and have contingency plans ready to use in the event of a security breach. By taking these steps, companies can protect customers, build trust, and maintain their reputation in an increasingly complex digital world.

In the increasingly advanced era of digital marketing, security must be the main focus for every company. Taking security challenges seriously and proactively will be the key to success in achieving digital marketing goals and ensuring sustainable business growth. This way, companies can reap the full benefits of their digital marketing strategies without compromising the security of customers and personal data.

Suggestion

For further research regarding security in digital marketing, some several suggestions and recommendations can be considered. First, more in-depth research can be conducted to identify and analyze potential newer and more complex security threats that emerge as technology develops. The use of artificial intelligence technology and more sophisticated analytics can help in detecting and dealing with more detailed security threats that cannot be detected manually.

Future research could focus on understanding user behavior in the face of fraud attempts and cyberattacks. Understanding the factors that influence users' level of awareness and compliance with security practices will help design more effective education and training strategies.

References

Febriari, S., 2023. Series of Personal Data Leak Cases in Indonesia Throughout 2022-2023. Retrieved fromhttps://www.metrotvnews.com/play/NA0CXWqa-deretan-kas-kebocoran-data-personal-di-indonesia-sepanjang-2022-2023

Mathieson, K., 1991. Predicting User Intentions: Comparing the Technology Acceptance Model with the Theory of Planned Behavior.

Information Systems Research, 2(3), Pp. 173-191. doi:10.1287/isre.2.3.173

Michalec, O., Milyaeva, S., Rashid, A., 2022. When the future meets the past: Can safety and cyber security coexist in modern critical infrastructures? Big Data and Society, 9(1). doi:10.1177/20539517221108369

Spencer, M., 2022. Characterizing assurance: skepticism and mistrust in cyber security. Journal of Cultural Economy, Pp. 1-16. doi:10.1080/17530350.2022.2098515

Szajna, B., 1996. Empirical Evaluation of the Revised Technology Acceptance Model. Management Science, 42(1), Pp. 85-92. doi:10.1287/mnsc.42.1.85

Whyte, J., 2022. Cybersecurity, race, and the politics of truth. Security Dialogue, 53(4), Pp. 342-362. doi:10.1177/09670106221101725