Research Article

DOI: 10.30520/tjsosci.1412062

Digital Marketing in the Age of Cyber Threats: A Comprehensive Guide to Cybersecurity Practices

Hafize Nurgül DURMUŞ ŞENYAPAR[1]

[1] Ph.D., Gazi University, Ankara, Türkiye, nurguld@gazi.edu.tr

Abstract: As digital marketing strategies become increasingly integrated into business models, unique vulnerabilities to cyber threats make cybersecurity essential. This descriptive study provides a detailed analysis of cybersecurity for digital marketing, which is rapidly evolving with technological advancements and consumer behavior transitions. The integration of tools like Search Engine Optimization, social media, and online advertising and their susceptibility to cyber risks are investigated. Critical cybersecurity threats in digital marketing, including phishing attacks, malware and ransomware, data breaches, and Distributed Denial of Service attacks, are explored, emphasizing their potential impact on business operations, customer trust, and brand reputation. The study further explores best practices in cybersecurity tailored to the digital marketing area, advocating for regular software updates, comprehensive employee training, stringent data encryption protocols, strong password policies, multi-factor authentication, and periodic security audits, highlighting the importance of data backups and adherence to data protection laws in maintaining legal and ethical standards. The role of Artificial Intelligence and Machine Learning is investigated, emphasizing how these technologies enhance cybersecurity measures through proactive threat detection and efficient incident management. Additionally, the study examines the rising consumer concerns and awareness regarding data privacy and security in digital marketing, reflecting how these concerns influence business practices and the increasing demand for transparency and data control among consumers. Necessitating continuous vigilance and adaptation to protect against ever-evolving cyber threats, effective cybersecurity is indispensable in digital marketing for protection against cyber threats and as a vital element in building and maintaining consumer trust and loyalty.

Keywords: Digital Marketing, Cybersecurity, Data Protection, Consumer Privacy, Cyber Threats.

JEL Classification: M31, D18, L86

ORCID[1]**:** 0000-0003-0927-1643

Received Date: 29.12.2023

Accepted Date: 21.02.2024

INTRODUCTION

Digital marketing is an expansive and dynamic field encompassing various marketing efforts utilizing the internet and electronic devices. At its core, digital marketing seeks to harness the power of digital channels such as search engines, social media platforms, email, and various websites to connect businesses with their current and potential customers (Saura, 2021). This modern marketing approach promotes products, services, and brands while building substantial online presence and engagement. Key strategies integral to digital marketing include Search Engine Optimization (SEO), which enhances the visibility of a website in search engine results; content marketing, which involves creating and distributing valuable, relevant content to attract and retain a target audience; social media marketing, which uses platforms like Facebook, X and Instagram to engage with audiences, email marketing, a direct marketing approach using email to promote products or services, and online advertising, which includes various forms of paid advertising like pay-per-click (PPC), display ads and sponsored content. In digital marketing, cybersecurity plays a pivotal role (Agarwal, 2021; Das, 2021; Sisodia and Sisodia, 2023). Cybersecurity in digital marketing refers to the comprehensive set of practices, strategies, and technologies employed to protect digital marketing assets from a wide range of cyber threats and attacks (Huzaizi et al., 2021). Since digital marketing frequently involves collecting, storing, and processing sensitive customer data, including personal information and payment details, it becomes a prime target for cybercriminals (Dubovyk et al., 2022; Konyeha, 2020). These cyber threats can take numerous forms, including hacking attempts, phishing scams, malware attacks, and data breaches

(Garg et al., 2022; Konyeha, 2020; Rosário, 2023). In this case, cybersecurity measures are critical to safeguard data privacy and ensure marketing campaigns' integrity and continuity. These measures include the implementation of robust encryption protocols, regular security audits, the use of secure and updated software, and the adoption of stringent data protection policies (Alawida et al., 2022; Omorogbe, 2023). Moreover, effective cybersecurity in digital marketing is not only about protecting against financial and data losses. It plays a crucial role in maintaining customer trust and loyalty, which are integral to the success of any business (Ilyas et al., 2021). In an era where consumers are increasingly aware of data privacy concerns, demonstrating a commitment to cybersecurity can significantly enhance a brand's reputation and customer relationships (Krishen et al., 2021). Furthermore, compliance with various data protection regulations, such as the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States, is mandatory for businesses operating in those regions (Bukaty, 2019; Hoofnagle et al., 2019). These regulations impose strict guidelines on how customer data should be handled and protected, making cybersecurity an essential legal requirement in digital marketing. As the digital marketing area continues to grow and evolve, so does the importance of cybersecurity within it. Businesses must recognize that effective digital marketing is about reaching and engaging customers and protecting them and their data in the digital area. By integrating robust cybersecurity practices into their digital marketing strategies, businesses can safeguard their assets, comply with legal standards, and build stronger, trust-based customer relationships.

2. THE IMPORTANCE OF CYBERSECURITY IN DIGITAL MARKETING

In the area of digital marketing, the protection of sensitive data stands as a paramount concern. Digital marketing campaigns frequently collect and process many customers' data. This data typically includes but is not limited to names, addresses, contact details, and often, more sensitive information such as payment details and browsing behaviors (Lies, 2019, Sachdev, 2020). Protecting this data extends beyond the fundamental ethical responsibility of respecting customer privacy; it is critical to maintaining customer trust and loyalty (Mogaji et al., 2021). In an era where data breaches are increasingly common, customers are becoming more conscious of how their data is handled and protected. Failing to secure this sensitive information can lead to a loss of customer confidence, as individuals become reluctant to engage with brands that they perceive as careless with their data (Mukherjee et al., 2021). Furthermore, the issue of brand reputation is intimately tied to how a company manages and safeguards customer data. A data breach can devastate a brand's image and credibility. In today's digital age, data breach news spreads rapidly, and public scrutiny can irreparably harm a brand's reputation. Customers tend to be less forgiving of such lapses in security, especially when their personal and financial information is at stake. The impact of a data breach can manifest in reduced customer engagement, a decline in sales, and a long-term erosion of trust in the brand (Hammou et al., 2020; Purnomo, 2023). The legal and financial ramifications of data breaches in digital marketing are also significant. With the enactment of data protection laws such as the GDPR in the European Union and the CCPA in the United States, businesses are under increased pressure to comply with stringent data protection standards. These regulations mandate specific measures for data handling and require companies to implement robust cybersecurity protocols. Non-compliance can result in severe legal consequences, including hefty fines that can reach millions of dollars and, in some cases, lawsuits from affected parties. Moreover, the costs associated with a data breach are not limited to legal fines alone. Businesses often incur substantial expenses in managing the breach, such

as costs related to forensic investigations, strengthening security post-breach, public relations efforts to mitigate damage to brand reputation, and compensation to affected customers (Bukaty, 2019; Hoofnagle et al., 2019; Singh, 2019). Investing in cybersecurity is not merely a defensive measure against potential threats but a strategic business decision with far-reaching implications. Adequate protection of sensitive customer data ensures compliance with legal standards, safeguards against financial losses, and preserves the trust and loyalty of customers. For digital marketing endeavors, robust cybersecurity practices are no longer optional but fundamental for sustainable and responsible business operations.

3. KEY CYBERSECURITY THREATS IN DIGITAL MARKETING

In the case of digital marketing, the threat area is diverse and constantly evolving, with several critical types of cyber-attacks posing significant risks. Phishing attacks are among the most prevalent threats in the digital space. These attacks typically involve disseminating fraudulent emails or messages that meticulously mimic communications from reputable sources, such as financial institutions or well-known companies. These deceptive communications trick recipients into revealing sensitive information such as login credentials, credit card numbers, or other personal data. Phishing can be particularly damaging in digital marketing, where customers and employees frequently interact through electronic communications. The sophistication of these attacks has grown, with cybercriminals using advanced tactics like social engineering to make their attempts more convincing, thereby increasing the risk of compromised sensitive information (Konyeha, 2020; Srivastav and Gupta, 2021). Malware and ransomware represent another significant threat to digital marketing systems. Malware, short for malicious software, encompasses harmful software designed to infiltrate, damage, or turn off computers and computer systems. In the case of digital marketing, malware can be used to steal data, monitor user activities, or even take control of marketing systems. Ransomware, a specific type of malware, encrypts a victim’s data and demands payment for its decryption. This can be particularly crippling for digital marketing efforts, as access to critical data and systems is essential for daily operations. The impact of such attacks can range from temporary disruption of services to severe, long-term damage to a company’s infrastructure and reputation (Butt et al., 2020; Jenkinson, 2022; Maglaras and Kantzavelou, 2021). Data breaches are a critical concern involving unauthorized access to customer databases, leading to the exposure and potential misuse of personal information. In digital marketing, vast amounts of customer data are collected and stored, making these systems attractive targets for cybercriminals. Data breaches can result from various factors, including inadequate security measures, employee negligence, or sophisticated cyber-attacks. The consequences of a data breach are far-reaching, leading to the loss of sensitive customer data and potentially causing severe financial and reputational damage to the business (Makridis, 2021; Srinivas and Liang, 2022). DDoS attacks are a significant threat to online marketing platforms and services. These attacks involve overwhelming a system’s resources by flooding it with massive traffic from multiple sources, rendering it inoperable. For digital marketing, a DDoS attack can mean the crippling of critical platforms such as websites, e-commerce portals, and online advertising services. This disrupts the customer experience and can lead to substantial revenue losses, mainly if the attack occurs during peak business hours or important marketing campaigns (Gupta, 2020; Kaur Chahal et al., 2019). The cybersecurity area in digital marketing is fraught with diverse threats, including phishing, malware, ransomware, data breaches, and DDoS attacks. Each poses a unique set of challenges and potential damages, emphasizing the need for robust and proactive cybersecurity measures to protect sensitive data, maintain customer trust, and ensure the uninterrupted operation of

digital marketing services.

4. BEST PRACTICES FOR ENHANCING CYBERSECURITY

Enhancing cybersecurity in digital marketing is a multifaceted endeavor, requiring a combination of technology, policy, and education. Best practices in this area are crucial for safeguarding against various cyber threats. Regular software updates are a foundational aspect of cybersecurity. This involves ensuring that all digital marketing tools and platforms are up-to-date with the latest patches and software versions. Regular updates are vital because they often include fixes for known vulnerabilities that cyber attackers could exploit. This practice extends to all software used in digital marketing campaigns, including content management systems, analytics tools, customer relationship management systems, and email marketing platforms. Keeping these systems updated mitigates the risk of security breaches arising from outdated software (Kilag et al., 2023; Mugarza et al., 2020). Employee training is another critical component of a robust cybersecurity strategy. Since human error is one of the most common causes of security breaches, staff must be well-trained in recognizing and avoiding potential cybersecurity threats. This includes identifying phishing attempts, which are fraud efforts to obtain sensitive information such as usernames, passwords, and credit card details by disguising themselves as a trustworthy entity in an electronic communication. Regular training sessions can help employees learn the latest phishing tactics and cybersecurity threats (He and Zhang, 2019; Reeves et al., 2021). Data encryption plays a crucial role in protecting sensitive information. Encrypting data at rest (data stored) and in transit (data transmitted over a network) ensures that even if data is intercepted or accessed by unauthorized individuals, it remains unreadable and secure. This practice is critical in digital marketing, where sensitive customer information is frequently handled (Habibzadeh et al., 2019). Implementing strong password policies is a simple yet effective measure for enhancing cybersecurity. This involves using strong, unique passwords for each platform and account. Passwords should be complex, combining letters, numbers, and symbols, and should be changed regularly. Using a password manager can help manage these passwords, as it allows for the generation and storage of complex passwords without the need to remember each one (Algharibeh et al., 2021). Multi-factor authentication (MFA) adds a layer of security. MFA requires more than one method of authentication to verify the user's identity for a login or other transaction, which typically includes something the user knows (like a password), something the user has (like a smartphone), or something the user is (like a fingerprint) (Sain et al., 2021). Regular security audits are essential in identifying and addressing vulnerabilities in digital marketing systems. These audits should assess all aspects of cybersecurity, from the physical security of servers to the protection of applications and data (Sabillon, 2022). Data backup is critical in ensuring that essential data can be recovered during a cyberattack or other data loss event. Regular backups should be made of all crucial data and tested frequently to ensure they can be restored effectively (Murn, 2021). Finally, compliance with data protection laws is a legal requirement and crucial to building customer trust. Understanding and adhering to regulations such as the GDPR and the CCPA is vital. These regulations mandate strict data privacy and security guidelines, and non-compliance can lead to significant penalties (Raul, 2021). Enhancing cybersecurity in digital marketing requires a comprehensive approach that includes regular software updates, employee training, data encryption, strong password policies, multi-factor authentication, periodic security audits, data backup, and compliance with data protection laws. By implementing these best practices, businesses can significantly reduce their cyber threat risk and protect their and customers' data.

5. THE ROLE OF AI AND ML IN CYBERSECURITY

Integrating AI and ML in cybersecurity, particularly in digital marketing, represents a significant advancement. These technologies are increasingly leveraged to bolster defense mechanisms against various cyber threats. AI and ML algorithms analyze vast amounts of data rapidly and efficiently, surpassing human capabilities in speed and accuracy. This feature is particularly beneficial in digital marketing, where large volumes of data are generated and must be constantly monitored for security threats (Ansari, Dash, et al., 2022; Dasgupta et al., 2022). AI and ML contribute to cybersecurity in several vital ways. Firstly, they are instrumental in detecting patterns and anomalies within data that could indicate potential security threats. Unlike traditional security software that relies on known threat databases, AI and ML systems can learn and evolve, adapting to detect new and emerging threats. They can analyze the behavior patterns of users, systems, and network traffic and identify deviations from the norm that might signify a cyber-attack, such as unusual login attempts, spikes in data traffic, or uncharacteristic data access patterns (Wiafe et al., 2020). Furthermore, AI and ML enable proactive threat detection and response. Instead of reacting to breaches after they occur, these technologies can predict and identify potential vulnerabilities before they are exploited. For instance, in digital marketing, an AI system might detect a suspicious pattern of user behavior on a website, such as rapid-fire attempts to access customer accounts and trigger an alert or an automatic response to block these attempts (Kanimozhi and Jacob, 2019). These technologies also enhance the efficiency of cybersecurity operations. AI-driven security tools can automate routine tasks such as scanning for vulnerabilities, monitoring network traffic, and responding to low-level security alerts. This automation allows cybersecurity personnel to focus on more complex tasks that require human oversight (Alhayani et al., 2021). Another critical aspect of AI and ML in cybersecurity is their role in incident response and recovery. In the aftermath of a security breach, AI can assist in quickly identifying the extent of the breach, isolating affected systems, and initiating recovery processes. This rapid response can significantly reduce the impact of a violation (Dunsin et al., 2022; Naseer et al., 2021). Moreover, AI and ML are becoming invaluable in combating sophisticated cyber threats such as phishing and advanced persistent threats (APTs). A.I. systems can be trained to recognize the characteristics of phishing emails and websites, significantly reducing the likelihood of successful phishing attacks. In the case of APTs, which involve prolonged and targeted cyber-attacks, AI can help continuously monitor and analyze network behavior to detect signs of infiltration (Ansari Sharma et al., 2022). The role of AI and ML in enhancing cybersecurity in digital marketing is becoming increasingly crucial. By enabling the detection of patterns and anomalies, facilitating proactive threat detection, automating routine tasks, assisting in incident response, and combating sophisticated threats, AI and ML are reshaping the area of cybersecurity. Their ability to adapt and learn makes them indispensable tools in the ongoing battle against cyber threats in the dynamic world of digital marketing.

6. CONSUMER CONCERNS AND AWARENESS ABOUT CYBERSECURITY IN DIGITAL MARKETING

Consumer concerns and awareness about cybersecurity in digital marketing have become increasingly prominent in recent years. As digital marketing strategies become more sophisticated and pervasive, encompassing a wide range of activities from targeted advertising to personalized customer experiences, consumers are becoming more conscious of the security and privacy of their personal information.

6.1. Consumer Concerns

- Privacy of Personal Data: With digital marketing strategies often involving the collection and analysis of personal data such as browsing habits, purchase history, and social media activity, consumers are increasingly worried about how their information is being used, stored, and protected. There is a growing concern over unauthorized data sharing or selling to third parties without explicit consent (Beauvisage and Mellet, 2020).
- Risk of Data Breaches: News of data breaches and cybersecurity incidents has heightened consumer awareness and concern about the security of their personal and financial information. Consumers are wary of the potential risks of online transactions and sharing sensitive information with online businesses (Juma'h and Alnsour, 2020).
- Identity Theft: The risk of identity theft is a significant concern. Cybersecurity lapses in digital marketing systems can lead to personal information falling into the wrong hands, which can then be used to commit dishonesty or identity theft (Akdemir, 2021).
- Misuse of Information: Consumers are increasingly skeptical about how their data is used in targeted advertising and personalized marketing. There is a concern that their data might be used in ways they have not agreed to, leading to intrusive or unwanted marketing practices (Mukherjee et al., 2021).

6.2. Consumer Awareness

- Educated on Rights and Options: Consumers are becoming more educated about their rights regarding data privacy, such as the right to access, correct, and delete their data. Awareness of privacy-enhancing tools and options like ad blockers, cookie management, and opting out of data collection is also growing (Furnell and Vasileiou, 2022).
- Expectations for Transparency and Security: There is a rising expectation for transparency from companies in collecting, using, and protecting consumer data. Consumers increasingly favor businesses committed to cybersecurity and data privacy (Tezel et al., 2022).
- Demand for Compliance with Data Protection Laws: With the introduction of regulations like GDPR and CCPA, consumers are more aware of legal standards and expect businesses to comply with these regulations. They are likelier to trust and engage with companies that adhere to these standards (Hoofnagle et al., 2019; Kollnig et al., 2022).
- Engagement with Secure Platforms: Consumers prefer engaging with digital platforms they perceive as secure. They are more likely to conduct transactions with websites and apps that offer secure connections and show clear indicators of data protection practices (Peter and Dalla Vecchia, 2021).
- Increased Vigilance and Reporting: Consumers are more vigilant about monitoring their accounts for unusual activity and are more likely to report suspected breaches or dishonesty (Scott, 2023).

As digital marketing continues to evolve, consumer concerns and awareness about cybersecurity are becoming more pronounced. Consumers are not only more informed about the risks associated with digital marketing practices but are also demanding higher standards of data privacy and security from businesses. This transition necessitates companies prioritizing cybersecurity and transparent data practices to maintain consumer trust and loyalty.

CONCLUSION AND DISCUSSION

The comprehensive exploration of cybersecurity in digital marketing underscores its critical importance in today's increasingly digital business area. As we have searched into the nuances of digital marketing strategies, ranging from SEO to social media marketing, it becomes evident that digital marketing is not just a platform for business growth and customer engagement but also a fertile ground for various cyber threats. The importance of cybersecurity in this case cannot be overstated, as it directly impacts the protection of sensitive customer data, maintains brand reputation, and ensures legal and financial compliance. Critical cybersecurity threats present formidable challenges, including phishing, malware, ransomware, data breaches, and DDoS attacks. These threats, if not adequately mitigated, can lead to significant financial loss and erosion of customer trust. Adopting best practices such as regular software updates, employee training, data encryption, strong password policies, multi-factor authentication, periodic security audits, and data backups is essential in creating a secure digital marketing environment. Compliance with data protection laws like GDPR and CCPA further reinforces a company's commitment to data security. The role of advanced technologies such as AI and ML in enhancing cybersecurity measures offers a proactive approach to threat detection and response, showcasing the potential for continuous evolution in cybersecurity strategies. These technologies not only automate the detection of threats but also provide invaluable support in incident response and recovery, making them indispensable in the modern cybersecurity toolkit. Consumer concerns and awareness about cybersecurity have significantly shaped how businesses approach digital marketing. The growing consumer demand for transparency, security, and control over personal data compels companies to prioritize robust cybersecurity measures as a compliance necessity and cornerstone of customer trust and loyalty. As digital marketing continues to evolve, it becomes increasingly essential for businesses to stay ahead of cyber threats and ensure the security and integrity of their digital marketing efforts. In conclusion, the cybersecurity and digital marketing intersection is dynamic and critical, demanding constant vigilance and adaptation. Businesses must recognize the integral role of cybersecurity in protecting their data and systems, their brand reputation, and customer relationships. By embracing comprehensive cybersecurity strategies and acknowledging the evolving nature of cyber threats, businesses can safeguard themselves against potential risks and strengthen their position in the competitive digital marketing area.

CONFLICT OF INTEREST DECLARATION

The author declares no conflict of interest with any institution or person within the scope of the study.

REFERENCES

Agarwal, M. (2021). A study on Pay-Per-Click advertising. Asian Journal of Multidimensional Research, 10(11), 618–624. https://doi.org/10.5958/2278-4853.2021.01042.9

Akdemir, N. (2021). Coping with Identity Theft and Fear of Identity Theft in the Digital Age. In Legal Challenges in the New Digital Age (pp. 176–197). Brill Nijhoff. https://doi.org/10.1163/9789004447417_011

Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. Journal of King Saud University - Computer and Information Sciences, 34(10, Part A), 8176–8206. https://doi.org/10.1016/j.jksuci.2022.08.003

Algharibeh, M. M., Husari, G., & Jaf, S. (2021). A Data-Driven Password Strength Meter for Cybersecurity Assessment and Enhancement. 2021 IEEE 23rd Int Conf on High Performance Computing & Communications; 7th Int Conf on Data Science & Systems; 19th Int Conf on Smart City; 7th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys), 1980–1987. https://doi.org/10.1109/HPCC-DSS-SmartCity-DependSys53884.2021.00296

Alhayani, B., Mohammed, H. J., Chaloob, I. Z., & Ahmed, J. S. (2021). Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry. Materials Today: Proceedings, 531.

Ansari, M. F., Dash, B., Sharma, P., & Yathiraju, N. (2022). The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review (SSRN Scholarly Paper 4323317). https://papers.ssrn.com/abstract=4323317

Ansari, M. F., Sharma, P. K., & Dash, B. (2022). Prevention of phishing attacks using AI-based Cybersecurity Awareness Training. Prevention, 3(3), Article 6, Available at: https://www.interscience.in/ijssan/vol3/iss3/6

Beauvisage, T., & Mellet, K. (2020). Datassets: Assetizing and marketizing personal data. Assetization: Turning Things into Assets in Technoscientific Capitalism, 75–96.

Bukaty, P. (2019). The California Consumer Privacy Act (CCPA): An implementation guide. IT Governance Ltd.

Butt, U. J., Abbod, M. F., & Kumar, A. (2020). Cyber Threat Ransomware and Marketing to Networked Consumers. In Handbook of Research on Innovations in Technology and Marketing for the Connected Consumer (pp. 155–185). IGI Global. https://doi.org/10.4018/978-1-7998-0131-3.ch008

Das, S. (2021). Search Engine Optimization and Marketing: A Recipe for Success in Digital Marketing. CRC Press, A Chapman and Hall Book.

Dasgupta, D., Akhtar, Z., & Sen, S. (2022). Machine learning in cybersecurity: A comprehensive survey. The Journal of Defense Modeling and Simulation, 19(1), 57–106. https://doi.org/10.1177/1548512920951275

Dubovyk, T., Buchatska, I., Zerkal, A., & Lebedchenko, V. (2022). Digital Marketing in the Condition of Wartime Posture in Ukraine, 22(7), 206. https://doi.org/10.22937/IJCSNS.2022.22.7.25

Dunsin, D., Ghanem, M. C., & Quazzane, K. (2022). The use of artificial intelligence in digital forensics and incident response in a constrained environment. International Journal of Information and Communication Engineering, 16(8), 280–285.

Furnell, S. M., & Vasileiou, I. (2022). A holistic view of cybersecurity education requirements. In Research Anthology on Advancements in Cybersecurity Education (pp. 289–307). IGI Global.

Garg, S., Gupta, S., & Gupta, B. (2022). Impacts of Blockchain on Digital Marketing. In A. K. Nagar, D. S. Jat, G. Marín-Raventós, & D. K. Mishra (Eds.), Intelligent Sustainable Systems (pp. 209–217). Springer Nature. https://doi.org/10.1007/978-981-16-6309-3_21

Gupta, N. (2020). Digital marketing: Trends, opportunities, and challenges. ASIAN JOURNAL OF MANAGEMENT, 11(4), 434–440. https://doi.org/10.5958/2321-5763.2020.00066.9

Habibzadeh, H., Nussbaum, B. H., Anjomshoa, F., Kantarci, B., & Soyata, T. (2019). A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. Sustainable Cities and Society, 50, 101660. https://doi.org/10.1016/j.scs.2019.101660

Hammou, I., Aboudou, S., & Makloul, Y. (2020). Social Media and Intangible Cultural Heritage for Digital Marketing Communication: Case of Marrakech Crafts, 2227-6718, https://doi.org/10.21272/mmi.2020.1-09

He, W., & Zhang, Z. (Justin). (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. Journal of Organizational Computing and Electronic Commerce, 29(4), 249–257. https://doi.org/10.1080/10919392.2019.1611528

Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: What it is and means*. Information & Communications Technology Law, 28(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501

Huzaizi, A. H. A., Tajuddin, S., Bahari, K. A., Manan, K. A., & Abd Mubin, N. N. (2021). Cyber-security culture towards digital marketing communications among small and medium-sized (SME) entrepreneurs. Asian Culture and History, 13(2), 1–20.

Ilyas, G. B., Munir, A. R., Tamsah, H., Mustafa, H., & Yusriadi, Y. (2021). The Influence of Digital Marketing and Customer Perceived Value through Customer Satisfaction on Customer Loyalty. Journal of Legal, Ethical and Regulatory Issues, 24 Pt. 2, 1.

Jenkinson, A. (2022). Ransomware and Cybercrime. CRC Press, Web Site: https://books.google.com.tr/books?hl=tr&lr=&id=DLprEAAAQBAJ&oi=fnd&pg=PT6&dq=Ransomware+and+Cybercrime.+CRC+Press&ots=Zu97Lehq3i&sig=sBKWktegxBmXO-dsQrsAvyDgdRY&redir_esc=y#v=onepage&q=Ransomware%20and%20Cybercrime.%20CRC%20Press&f=false

Juma'h, A. H., & Alnsour, Y. (2020). The effect of data breaches on company performance. International Journal of Accounting & Information Management, 28(2), 275–301. https://doi.org/10.1108/IJAIM-01-2019-0006

Kanimozhi, V., & Jacob, T. P. (2019). Artificial Intelligence-based Network Intrusion Detection with Hyper-Parameter Optimization Tuning on the Realistic Cyber Dataset CSE-CIC-IDS2018 using Cloud Computing. 2019 International Conference on Communication and Signal Processing (ICCSP), 0033–0036. https://doi.org/10.1109/ICCSP.2019.8698029

Kaur Chahal, J., Bhandari, A., & Behal, S. (2019). Distributed Denial of Service Attacks: A Threat or Challenge. New Review of Information Networking, 24(1), 31–103. https://doi.org/10.1080/13614576.2019.1611468

Kilag, O. K. T., Indino, N. V., Sabagala, A. M., Abendan, C. F. K., Arcillo, M. T., & Camangyan, G. A. (2023). Managing Cybersecurity Risks in Educational Technology Environments: Strategies and Best Practices. American Journal of Language, Literacy and Learning in STEM Education (2993-2769), 1(5), Article 5.

Kollnig, K., Shuba, A., Binns, R., Van Kleek, M., & Shadbolt, N. (2022). Are iPhones Really Better for Privacy? Comparative Study of iOS and Android Apps. Proceedings on Privacy Enhancing Technologies, 2022(2), 6–24. https://doi.org/10.2478/popets-2022-0033

Konyeha, S. (2020). Exploring cybersecurity threats in digital marketing. Journal of Science and Technology Research, 2(3), 12-20, https://doi.org/10.37933/nipes/2.3.2020.2

Krishen, A. S., Dwivedi, Y. K., Bindu, N., & Kumar, K. S. (2021). A broad overview of interactive digital marketing: A bibliometric network analysis. Journal of Business Research, 131, 183–195. https://doi.org/10.1016/j.jbusres.2021.03.061

Lies, J. (2019). Marketing Intelligence and Big Data: Digital Marketing Techniques on their Way to Becoming Social Engineering Techniques in Marketing, 5(5), 134-144, https://doi.org/10.9781/ijimai.2019.05.002

Maglaras, L., & Kantzavelou, I. (2021). Cybersecurity Issues in Emerging Technologies. CRC Press.

Makridis, C. A. (2021). Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018. Journal of Cybersecurity, 7(1), tyab021. https://doi.org/10.1093/cybsec/tyab021

Mogaji, E., Soetan, T. O., & Kieu, T. A. (2021). The implications of artificial intelligence on the digital marketing of financial services to vulnerable customers. Australasian Marketing Journal, 29(3), 235–242. https://doi.org/10.1016/j.ausmj.2020.05.003

Mugarza, I., Flores, J. L., & Montero, J. L. (2020). Security Issues and Software Updates Management in the Industrial Internet of Things (IIoT) Era. Sensors, 20(24), 7160. https://doi.org/10.3390/s20247160

Mukherjee, S. B., Ghatak, S. G. N., & Ray, N. (2021). Digitization of Economy and Society: Emerging Paradigms. CRC Press, Web Site: https://books.google.com.tr/books?hl=tr&lr=&id=BiA-EAAAQBAJ&oi=fnd&pg=PP1&dq=Digitization+of+Economy+and+Society:+Emerging+Paradigms.+CRC+Press.&ots=j1S58OZeKK&sig=gYc9QjnG7HrT0N8IoYCwNfQhEdY&redir_esc=y#v=onepage&q=Digitization%20of%20Economy%20and%20Society%3A%20Emerging%20Paradigms.%20CRC%20Press.&f=false, Apple Academic Press.

Murn, L. (2021). Data Safety and Cybersecurity. In Digital Transformation of the Laboratory (pp. 85–100). John Wiley & Sons, Ltd. https://doi.org/10.1002/9783527825042.ch4

Naseer, H., Maynard, S. B., & Desouza, K. C. (2021). Demystifying analytical information processing capability: The case of cybersecurity incident response. Decision Support Systems, 143, 113476. https://doi.org/10.1016/j.dss.2020.113476

Omorogbe, P. E. (2023). Improving Digital Marketing Strategy: The Impact of Digital Analytics, Bachelor's Degree in International Business Web Site: https://www.theseus.fi/handle/10024/803981

Peter, M. K., & Dalla Vecchia, M. (2021). The Digital Marketing Toolkit: A Literature Review for the Identification of Digital Marketing Channels and Platforms. In R. Dornberger (Ed.), New Trends in Business Information Systems and Technology: Digital Innovation and Digital Business Transformation (pp. 251–265). Springer International Publishing. https://doi.org/10.1007/978-3-030-48332-6_17

Purnomo, Y. J. (2023). Digital marketing strategy to increase sales conversion on e-commerce platforms. Journal of Contemporary Administration and Management (ADMAN), 1(2), 54–62.

Raul, A. C. (2021). The privacy, data protection, and cybersecurity law review. Law Business Research Limited, Web Site: https://datamatters.sidley.com/wp-content/uploads/sites/2/2019/11/The-Privacy-Data-Protection-and-Cybersecurity-Law-Review-Edition-6.pdf

Reeves, A., Calic, D., & Delfabbro, P. (2021). "Get a red-hot poker and open up my eyes; it's so boring."1: Employee perceptions of cybersecurity training. Computers & Security, 106, 102281. https://doi.org/10.1016/j.cose.2021.102281

Rosário, A. T. (2023). Security in Digital Marketing: Challenges and Opportunities. In Confronting Security and Privacy Challenges in Digital Marketing (pp. 206–233). IGI Global. https://doi.org/10.4018/978-1-6684-8958-1.ch010

Sabillon, R. (2022). Audits in Cybersecurity. In Research Anthology on Business Aspects of Cybersecurity (pp. 1–18). IGI Global. https://doi.org/10.4018/978-1-6684-3698-1.ch001

Sachdev, R. (2020). Towards Security and Privacy for Edge AI in IoT/IoE based Digital Marketing Environments. 2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC), 341–346. https://doi.org/10.1109/FMEC49853.2020.9144755

Sain, M., Normurodov, O., Hong, C., & Hui, K. L. (2021). A Survey on the Security in Cyber-Physical System with Multi-Factor Authentication. 2021 23rd International Conference on Advanced Communication Technology (ICACT), 1–8. https://doi.org/10.23919/ICACT51234.2021.9370515

Saura, J. R. (2021). Using Data Sciences in Digital Marketing: Framework, methods, and performance metrics. Journal of Innovation & Knowledge, 6(2), 92–102. https://doi.org/10.1016/j.jik.2020.08.001

Scott, H. (2023). 'Reject All': Data, Drift and Digital Vigilance. In S. Hayes, M. Jopling, S. Connor, & M. Johnson (Eds.), Human Data Interaction, Disadvantage and Skills in the Community: Enabling Cross-Sector Environments for Postdigital Inclusion (pp. 285–298). Springer International Publishing. https://doi.org/10.1007/978-3-031-31875-7_15

Singh, D., Sumesh. (2019). Handbook of Research on Innovations in Technology and Marketing for the Connected Consumer. IGI Global.

Sisodia, D., & Sisodia, D. S. (2023). A transfer learning framework towards identifying fraudulent publishers' behavioral changes in pay-per-click online advertising model for click fraud detection. Expert Systems with Applications, 232, 120922. https://doi.org/10.1016/j.eswa.2023.120922

Srinivas, S., & Liang, H. (2022). Being digital to being vulnerable: Does digital transformation allure a data breach? Journal of Electronic Business & Digital Economics, 1(1/2), 111–137. https://doi.org/10.1108/JEBDE-08-2022-0026

Srivastav, P., & Gupta, H. (2021). Role and Applications of Digital Marketing in Digital Era: A Review. 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 1–5. https://doi.org/10.1109/ICRITO51393.2021.9596087

Tezel, A., Papadonikolaki, E., Yitmen, I., & Bolpagni, M. (2022). Blockchain Opportunities and Issues in the Built Environment: Perspectives on Trust, Transparency and Cybersecurity. In M. Bolpagni, R. Gavina, & D. Ribeiro (Eds.), Industry 4.0 for the Built Environment: Methodologies, Technologies and Skills (pp. 569–588). Springer International Publishing. https://doi.org/10.1007/978-3-030-82430-3_24

Wiafe, I., Koranteng, F. N., Obeng, E. N., Assyne, N., Wiafe, A., & Gulliver, S. R. (2020). Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature. IEEE Access, 8, 146598–146612. https://doi.org/10.1109/ACCESS.2020.3013145