Contents lists available at GrowingScience

International Journal of Data and Network Science

homepage: www.GrowingScience.com/ijds

Examining marketing cyber-security in the digital age: Evidence from marketing platforms

Tareq N. Hashem[a*]

[a]*Full Professor of Marketing, Marketing Department, Faculty of Business, Applied Science Private University, Amman, Jordan*

C H R O N I C L E

Article history:
Received: August 15, 2023
Received in revised format: September 25, 2023
Accepted: November 24, 2023
Available online: November 24, 2023

Keywords:
Marketing Cyber-Security
Digital Marketing
Cyber-Attacks
Scripting
Digital Platforms

A B S T R A C T

The current study aimed to examine marketing cyber-security (DDoS Attacks, Cross-Site Scripting, SQL Attacks, and passwords attacks) in the digital age by presenting evidence from digital marketing platforms. Depending on the quantitative approach and utilizing a questionnaire as a tool, (133) marketing managers in digital marketing companies in Jordan responded to an online questionnaire. SPSS was used to screen and analyze the gathered data. Results of the study accepted the main hypothesis, and it appeared that marketing cyber-security has a statistically positive influence on marketing platforms, in addition to that, it appeared that the highest influence of sub-variables was for the benefit of Structured Query Language (SQL) Attacks explaining 35.8% of the variation. This result meant that SQL attacks-security does have a statistically positive influence on marketing platforms. This hypothesis could be tested through various methodologies, for example, surveys, interviews, focus groups, and/or experiments. The study recommended that marketers should use role-based access to limit the data employees can access and regularly review their permissions. Further recommendations were presented in the study.

1. Introduction

Digital marketing security is an important element of protecting businesses from cyber threats. It encompasses both technical solutions and best practices that organizations must put in place to protect confidential customer data, prevent malicious external attacks, and secure a company's digital assets (Mukherjee et al., 2021). According to Konyeha (2020), digital marketing security protocols cover a range of areas, from authentication and authorization measures designed to protect customer accounts, to the identification and limitation of privileged user access rights. Additionally, digital marketing security measures include protection from data breaches, data loss, malware and other security threats, as well as ensuring regulatory compliance (Krishen et al., 2021). Implementing and maintaining adequate digital marketing security measures are essential in today's digital world to ensure customer safety and protect businesses from financial losses (Singh, 2021). In an overall estimation, digital marketing and cyber-security are two sides of the same coin. Digital marketing involves promoting, advertising, and optimizing products or services using a range of digital technologies (Suleiman et al., 2021). According to Halesha and Arundathi (2020), cyber-security, on the other hand, involves protecting digital customer data, intellectual property and business operations from cyber-attacks, data breaches and other malicious activities. As both digital marketing and cyber-security are interlinked, businesses need to ensure that their digital marketing strategies are secure and their cyber-security systems are up to date to protect both customer and business data (Magano & Cunha, 2020). Launching from the above argument, this current study aimed to assess the impact of digital tools and techniques on the security of marketing platforms. The goal is to determine the nature of cyber-security attacks (DDoS Attacks, Cross-Site Scripting, SQL Attacks and Passwords Attacks) on digital marketing platforms and how organizations' awareness can help in protecting their users and how they can improve their security measures to keep their users safe from malicious cyber-attacks. The evidence gathered from marketing platforms should be used to identify potential weaknesses and develop more secure marketing solutions.

* Corresponding author.
E-mail address: t_hashim@asu.edu.jo (T. N. Hashem)

ISSN 2561-8156 (Online) - ISSN 2561-8148 (Print)

doi: 10.5267/j.ijdns.2023.11.020

2. Literature Review and Related Studies

2.1 Cyber-Security in Marketing

According to Wibowo and Sulaksono (2021), cyber-security in marketing refers to the use of security measures to protect digital assets and customer information. This includes encrypting website data, setting up two-factor authentication, monitoring for suspicious activity, implementing data breach prevention strategies, and creating strong passwords (Khan et al., 2021). Additionally, marketing teams should develop a security and privacy policy that makes sure customers understand how their data will be used and kept secure (Pedley et al., 2020). Among the most common cyber-security attacks in digital marketing arena is what came along with Trim and Lee (2019) and Pham et al. (2019) when they argued that marketing through digital channels can result in many cyber-attacks that included:

2.2 Distributed Denial of Service (DDoS) Attacks

DDoS attacks are a type of cyber-attack in which a malicious actor aims to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target with a flood of internet traffic. A DDoS attack usually involves sending more requests to the target server than it can handle, resulting in that server crashing and becoming unavailable for a period of time (Asbaş & Tuzlukaya, 2022). According to Martins et al. (2022), this type of attack can have a significant negative impact on digital marketing efforts, as they can cause website unavailability, slow page loads, malformed pages, and data loss. When a website is under attack, digital marketers may not be able to reach their target audiences, which can lead to lost opportunities for sales and revenue. Additionally, DDoS attacks can cause reputational damage due to the perceived insecurity of the site. Threatened customers may choose to look elsewhere for services (Alanazi et al., 2023). Finally, DDoS attacks can incur costly outlays to remediate the issue, ultimately negatively impacting profits (Wazid et al., 2022).

2.3 Cross-Site Scripting (XSS)

XSS is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side scripts into web pages viewed by other users (Rodríguez et al., 2020). These scripts can have malicious consequences such as stealing user data, like session cookies, or redirecting the user to malicious sites (Wibowo & Sulaksono, 2021).
XSS attacks can have a serious impact on digital marketing. They can allow malicious third parties to inject malicious scripts into webpages, stealing user information and manipulating functionality (Mishra and Gupta, 2020). This could lead to customers feeling unsafe when dealing with the business, reducing trust in the brand, and ultimately causing customers to turn away from the business and its products (Gupta and Chaudhary, 2020). To prevent XSS attacks, digital marketing platforms should take steps to ensure their code is secure, and use techniques such as form validation to protect against malicious input (Kumar et al., 2022).

2.4 Structured Query Language (SQL) Attacks

SQL attacks, also known as SQL injection attacks, are malicious attacks that exploit security vulnerabilities in a website's software (Mishra, 2019). An attacker can inject malicious code into a vulnerable website, allowing the attacker to bypass security measures and gain access to sensitive data and other resources like usernames, passwords, or even credit card numbers stored in a database (Pattewar et al., 2019). SQL attacks can have a major and long-lasting effect on digital marketing by damaging the website, stealing clients' data, and damaging the reputation of the company (Latchoumi et al., 2020). SQL attacks can also result in significant financial losses due to loss of customers and revenue. In addition, the attacks can impact the effectiveness of digital marketing campaigns, as the website may become inaccessible or distorted for customers (Veerabudren & Bekaroo, 2022).

2.5 Passwords (PW) Attacks

Password attacks are attempts to gain unauthorized access to a system or its data by using various methods to guess, crack, or otherwise discover a password (Gazzari et al., 2021). Common methods of password attacks include dictionary attacks, brute-force attacks, rainbow table attacks, and social engineering (Lei et al., 2021). Passwords attacks can have a significant impact on digital marketing efforts, particularly for businesses that rely heavily on digital marketing campaigns (Kolomeets & Chechulin, 2021). Such attacks can cause a loss of customer confidence as customers may fear their data has been compromised, leading to a loss of sales or a drop in loyalty (Prasad et al., 2020). Ba et al. (2021) added that any funds subsequently spent on digital marketing campaigns may be wasted due to customers being reluctant to purchase or provide personal information. Furthermore, passwords attacks may cause an increase in spam and phishing campaigns, further damaging the company's reputation and reducing the chances of success for digital marketing efforts (Mirian et al., 2019).

3. Digital Marketing

According to Herhausen et al. (2020) and Junusi (2020), digital marketing is the use of digital channels and technologies to promote a product or service. This includes leveraging social media, search engine optimization, content marketing, email marketing, pay-per-click advertising, display advertising and mobile marketing campaigns (Pandey et al., 2020). Digital marketers work to create content that engages customers and encourages them to interact with the brand across various digital channels (Deb et al., 2022). Mogaji et al. (2020) noted that digital marketers also measure the success of their campaigns

using analytics, which allows them to make performance-based adjustments to their campaigns and strategies in order to maximize their returns.

4. Digital Marketing Platforms

According to Saura (2021) and Hashem (2021), digital marketing platform refers to a system of online tools and technologies used for managing and optimizing digital marketing campaigns. It typically includes analytics tools, automation tools, and content management tools that help businesses analyze data, build campaigns, and monitor performance. These platforms often integrate with various other marketing channels, like social media, email, and search marketing (Desai, 2019). Saura et al. (2021) and Olson et al. (2021) presented the most popular digital marketing platforms that included (Google Ads, Facebook Ads, Twitter Ads, LinkedIn Ads, Instagram Ads, YouTube Ads, Search Engine Optimization (SEO), Content Marketing, Email Marketing, Affiliate Marketing, Native Advertising, Online Display Advertising and Pay-Per-Click (PPC) Advertising).

4.1 Related Studies

A study by Kumar et al. (2022) discussed the current cyber security threats plaguing digital marketing and how they may impact consumers, marketers, and businesses. In particular, authors focused on how digital marketing can create issues with data privacy, data breaches, credential theft, and cyber-attacks. Additionally, they analyze various cyber security precautions that can be taken to ensure that digital marketing remains secure. Finally, they provide proposed recommendations for the future of digital marketing to help protect businesses, consumers, and marketers from cyber security threats. Overall, the authors conclude that digital marketing must be carefully monitored to remain secure and that a strategy of prevention, detection, and response should be employed to successfully defend against cyber-security threats. A study by Khakimova (2019) explored the importance of cyber security in digital marketing, citing numerous examples of data security breaches that have occurred in recent years. It examines how firms must take steps to ensure their digital data is safeguarded and secure, as well as highlighting potential security threats which firms must be aware of to be adequately prepared. The article also provides an overview of the types of security measures firms can put in place to protect their data, as well as advice for how firm's data should be monitored for any suspicious activity. Subramaniam (2020) examined the successful digital marketing strategy of Starbucks on Twitter. It looks at how the company has used social media as a tool to reach and engage with their customers, ultimately leading to an increase in sales. The article also explores how Twitter has enabled Starbucks to build relationships with customers and track the analytics of their campaigns. Finally, the article provides some useful tips for other marketers looking to implement a successful strategy on Twitter. Mathur (2018) discussed the need for businesses to develop social media marketing capability in order to protect themselves from the perceived risk of cyber security threats. It argues that businesses should assess their existing vulnerabilities and use the data to build robust marketing strategies for their social media platforms. It outlines the steps needed to gain a greater understanding of the threats, how to protect customer data and how to create resilient systems of defense. Finally, it highlights the importance of monitoring and evaluating the effectiveness of any protective measures implemented. Based on argument above, and launching from previous studies adopted, researcher built the following model in order to highlight the relationship between variables and extract hypotheses of study:

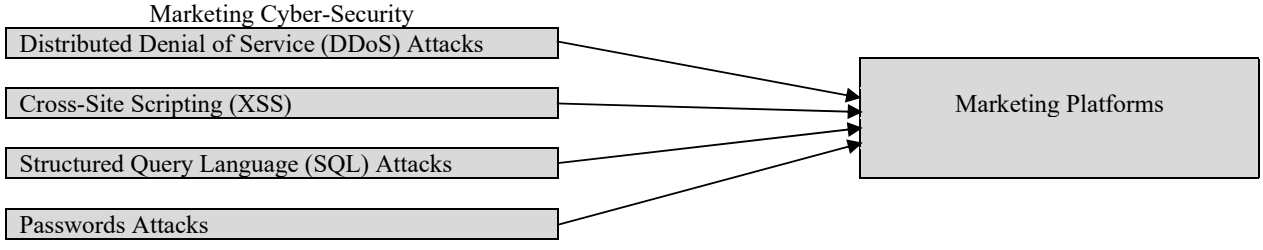

Fig. 1. Study Model (Kumar et al., 2022)

H: *Marketing cyber-security has a statistically positive influence on marketing platforms.*
H$_1$: *DDoS attacks-security has a statistically positive influence on marketing platforms.*
H$_2$: *Cross Site attacks-security has a statistically positive influence on marketing platforms.*
H$_3$: *SQL attacks-security has a statistically positive influence on marketing platforms.*
H$_4$: *Passwords attacks-security has a statistically positive influence on marketing platforms.*

4.2 Procedural Definitions of Study Constructs

Distributed Denial of Service (DDoS) Attacks

Malicious attempts to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of internet traffic.

Cross-Site Scripting (XSS)

A type of web application security vulnerability that allows attackers to inject malicious code into webpages viewed by other users; XSS can be used to cause a variety of malicious activities such as stealing user information, redirecting users to malicious sites, displaying ads or modifying the appearance of the page.

Structured Query Language (SQL) Attacks

Attacks that exploit security vulnerabilities in website databases, usually to gain access to information, alter information, or delete information. These attacks are possible because users often provide unrestricted access to databases.

Passwords (PW) Attacks

Type of cyber-attack used to gain access to a system, server, or website by guessing or cracking the password. Attackers use various automated methods such as brute force and dictionary attacks to guess or crack passwords.

5. Methodology

5.1 Methodological Approach

Quantitative methodology was adopted in current study in order to collect the needed primary data that would serve the main aim of study. According to Henson et al. (2020) quantitative methodology is a scientific approach to collecting, analyzing, and interpreting numerical data. Sheridan et al. (2020) noted that it is suitable for social research because it allows researchers to examine large amounts of data, identify patterns and correlations, and draw inferences. It also enables researchers to accurately compare data points over time and across different variables, allowing them to gain further insight into complex social phenomena. Additionally, quantitative research allows researchers to make well-informed decisions based on statistical evidence, which can lead to more successful strategies for social change (Limone et al., 2022).

5.2 Population and Sampling

Population of current study consisted of all managers of marketing managers in digital marketing companies in Jordan. Population of study is the entire set of items of interest in a statistical study (Thomson et al., 2020). A convenient sample of (150) marketing managers were chosen in order to represent population of the study. A sample in a research study is defined as a subset of the population that is used to represent the population in a statistical analysis (Asiamah et al., 2022).

5.3 Tool of Study

A questionnaire was chosen to be the main tool of study; a questionnaire is a series of questions that is used to collect information from a specific audience (Haraldsen, 2023). It is a research instrument used to gain insight into the views, opinions, and attitudes of people about a particular topic or issue. Questionnaires can be used for various types of research, such as market research, political polling, and technology trends (Sharma, 2022). In Current study, the questionnaire consisted of two main sections; the first took into perspective demographics of study sample; while the second section contained statements that are related to study sub-variables as according to the following Table 1.

Table 1
Distribution of Statements on Sub-Variables

Variables	Number of Statements
Marketing Cyber-Security	
DDoS Attacks	5
Cross-Site Scripting	5
SQL Attacks	6
Passwords Attacks	5
Marketing Platforms	7

The questionnaire was built by researcher with the help of previous studies, and it was built on liker 5 scale (1) Strongly disagree; (2) Disagree; (3) Neither agree nor disagree; (4) Agree; (5) Strongly agree. To preserve the highest level of social distancing, the questionnaire was uploaded online on Google forms platforms, it remained online for total of (8) weeks, and after application process it was found that (133) marketing managers responded to the questionnaire which indicated the response rate of 88.6% as statistically accepted.

5.4 Statistical Processing

Statistical package for social science (SPSS) was used in order to screen and analyze the gathered primary data. SPSS is a software package used for statistical analysis related to social science, health science, and market research. It is used to analyze and interpret data, draw conclusions, and inform policy decisions. It is available in both Windows and Mac OS versions (Okagbue et al., 2021). The reliability of a scale was evaluated using Cronbach's alpha and an alpha value of 0.89 or higher that was more than the threshold of 0.70 indicated a legitimate and trustworthy scale.

6. Results and Discussion

6.1 Demographic Results

Frequency and percentages were calculated for sample respondents, as in table 2 below, it was seen that majority of the sample were males forming 63.9% of total sample, who held an MA degree forming 52.6% of the sample with an experience of 6-9 years forming 33.1% of total sample.

Table 2
Demographics of Sample

	f	%
Gender		
Male	85	63.9
Female	48	36.1
Education		
BA	13	9.8
MA	70	52.6
PhD	50	37.6
Experience		
2-5	16	12.0
6-9	44	33.1
10-13	42	31.6
+14	31	23.3
Total	133	100.0

6.2 Questionnaire Analysis

Descriptive statistics of questionnaire statements were presented in mean and standard deviation, as it was seen in Table 3 below, all of variables and statements were well-received as they scored a mean higher than mean of scale 3.00. In terms of variables, it was seen that the highest mean was scored by Distributed Denial of Service (DDoS) Attacks with mean of 3.89/5.00 compared to the least variable which scored a mean of 3.50/5.00 as Cross-Site Scripting (XSS).

Table 3
Descriptive Statistics

Statement	Mean	Std. Deviation
Huge amount of traffic can be sent to the website and deny the service/product	4.27	.80
DDoS attacks can be done through malware, a 'botnet' of hijacked computers	3.77	1.04
DDoS attacks can be done through legitimate but extremely large requests	3.85	.87
DDoS can overwhelm the targeted service and cause it to crash or become unavailable.	3.85	.85
DDoS attacks can temporarily take down a server or website by flooding it with too many requests	3.73	.93
Distributed Denial of Service (DDoS) Attacks	**3.89**	**.64**
(XSS) injects malicious code into webpages viewed by users.	3.17	1.23
XSS are commonly carried out through malicious JavaScript code that is injected into the webpage content	3.50	1.13
Attackers use XSS to collect user information, hijack user sessions, and redirect webpages	3.69	.99
XSS attacks are usually executed by exploiting vulnerabilities in web applications	3.05	1.13
Preventing XSS attacks involves proper input validation and output encoding.	4.10	.92
Cross-Site Scripting (XSS)	**3.50**	**.74**
SQL attacks occur when malicious code is injected into a system by exploiting vulnerabilities in the underlying SQL code	4.06	.78
SQL attacks can result in the compromise of sensitive data, unauthorized changes to the data, or even disruption of the application or system	3.59	1.11
Attackers leverage web application programming flaws in the input and output validation, authentication and authorization processes, and database operations	3.59	1.05
SQL injection attack, a malicious user exploits the input validation flaws in order to execute unauthorized SQL statements that can modify and display data.	3.55	.89
SQL attacks can be prevented by using parameterized queries, validating user input, and using various security best practices	4.11	.86
Structured Query Language (SQL) Attacks	**3.78**	**.57**
Password attack is when a computer system is used to try out many different words or phrases to guess a password.	3.92	.74
It involves using complicated software algorithms to guess passwords in a very short time.	3.01	1.00
It is based on the usage of disinformation and other psychological tactics to try and guess passwords	3.74	.79
Phishing attacks use deceptive emails and websites to try and trick users into giving away passwords.	3.62	1.00
Rainbow tables offer an efficient way to store commonly used passwords, making them vulnerable to attack.	3.68	.96
Passwords (PW) Attacks	**3.60**	**.58**
Staff members are educated and equip them with the necessary knowledge to recognize suspicious emails and avoid phishing scams.	3.92	.77
Leverage cutting-edge antivirus software to protect against malware and ransom ware	3.93	.91
Firewalls and regularly update software to thwart cyber-attacks are installed.	3.82	.85
Multi-factor authentication to limit unauthorized access to accounts are implemented	3.95	.82
Regular scans to identify vulnerable areas such as outdated systems or applications are run	3.72	1.05
A username and password to access sensitive information are required	4.10	.83
Traffic to identify potential cyber threats is monitored	3.61	1.13
Digital Marketing Platforms	**3.86**	**.65**

Going deeper into analysis, it was seen that also all statements were well received as they all scored mean that was higher than scale 3.00, the highest mean was scored by the statement articulated " Huge amount of traffic can be sent to the website and deny the service/product" 4.27/5.00 compared to the least statement "(XSS) injects malicious code into webpages viewed by users" with mean of 3.17/5.00 but still positive as it was higher than mean of scale.

7. Hypotheses Testing

The main hypothesis was tested using multiple regression, (Marketing cyber-security has a statistically positive influence on marketing platforms) as in the following Table 4. The table revealed that F value of 19.134 was significant at the 0.05 level. This indicated that Marketing cyber-security has a statistically positive influence on marketing platforms. In addition, it was discovered that r=0.612 indicates a strong level of correlation, and the independent variables explain 37.4% of the variation in the variable that was being studied (the dependent variable).

Table 4
Main Hypothesis Testing

Coefficients									
		Unstandardized Coefficients		Standardized Coefficients					
	Model	B	Std. Error	Beta	t	Sig.	F Value	R	R Square
1	(Constant)	.907	.373		2.434	.016	19.134	.612	.374
	DDoS	.107	.081	.105	1.329	.186			
	XSS	.034	.092	.038	.369	.713			
	SQL	.551	.119	.480	4.637	.000			
	Passwords	.094	.103	.083	.912	.364			

Sub-Hypotheses were tested using linear regression and as it appeared in table 5 below, following results were reached:

- In the 1st sub-hypothesis, F value of 19.037 was significant at the 0.05 level. This indicated that DDoS attacks-security has a statistically positive influence on marketing platforms. In addition, it was discovered that r=0.356 indicated a medium level of correlation, and the independent variable explains **12.7%** of the variation in the variable that was being studied (the dependent variable).
- 2nd sub-hypothesis F value = 31.101 was significant at the 0.05 level, it indicated that Cross Site attacks-security has a statistically positive influence on marketing platforms, r=0.438 indicated a medium level of correlation, and the independent variable explains **19.2%** of the variation in the variable that was being studied (the dependent variable).
- 3rd sub-hypothesis was also tested using linear regression, it was seen that F value of 73.058 was significant at the 0.05 level and indicated that SQL attacks-security has a statistically positive influence on marketing platforms. In addition, it was discovered that r=0.598 indicated a medium level of correlation, and the independent variable explains **35.8%** of the variation in the variable that was being studied (the dependent variable).
- 4th sub-hypothesis F value of 23.863 was significant at the 0.05 level; this meant that Passwords attacks-security has a statistically positive influence on marketing platforms. In addition, it was discovered that r=0.393 indicated a medium level of correlation, and the independent variable explains **15.4%** of the variation in the variable that was being studied (the dependent variable).

Table 5
Testing Sub-Hypotheses

Coefficients								
	Unstandardized Coefficients		Standardized Coefficients					
Model	B	Std. Error	Beta		t	Sig.	R	R Square
1 (Constant)	2.440	.330			7.392	.000	.356[a]	.127
DDoS	.365	.084		.356	4.363	.000		
H1: DDoS attacks-security has a statistically positive influence on marketing platforms								
Coefficients								
	Unstandardized Coefficients		Standardized Coefficients					
Model	B	Std. Error	Beta		t	Sig.	R	R Square
1 (Constant)	2.506	.248			10.090	.000	.438[a]	.192
XSS	.387	.069		.438	5.577	.000		
H2: Cross Site attacks-security has a statistically positive influence on marketing platforms								
Coefficients								
	Unstandardized Coefficients		Standardized Coefficients					
Model	B	Std. Error	Beta		t	Sig.	R	R Square
1 (Constant)	1.270	.307			4.140	.000	.598[a]	.358
SQL	.686	.080		.598	8.547	.000		
H3: SQL attacks-security has a statistically positive influence on marketing platforms								
Coefficients								
	Unstandardized Coefficients		Standardized Coefficients					
Model	B	Std. Error	Beta		t	Sig.	R	R Square
1 (Constant)	2.275	.329			6.913	.000		
Passwords	.441	.090		.393	4.885	.000		
H4: Passwords attacks-security has a statistically positive influence on marketing platforms								

8. Discussion

The current research was carried out as an approach to assess the impact of cyber-security in digital marketing and define the nature of influence of cyber-security attacks (DDoS Attacks, Cross-Site Scripting, SQL Attacks and Passwords Attacks) on digital marketing platforms. For that sake, quantitative methodology was adopted and a questionnaire was distributed on a sample of (133) managers of marketing and marketing campaigns in e-marketing companies in Jordan. SPSS was employed in order to screen and analyze the gathered primary data, results of study accepted the main hypothesis arguing that "Marketing cyber-security has a statistically positive influence on marketing platforms" explaining 37.4% of the variation. Sub-hypotheses were also accepted, and it was indicated that (DDoS Attacks, Cross-Site Scripting, SQL Attacks and Passwords Attacks) as cyber-security attacks have the ability to influence digital marketing platforms if no suitable action were taken into consideration matching results of Subramaniam (2020).

Through analysis of study, it was revealed that the highest influence of sub-variables were for the benefit of Structured Query Language (SQL) Attacks explaining35.8% of the variation. This result meant that SQL attacks-security does have a statistically positive influence on marketing platforms. This hypothesis could be tested through various methodologies, for example, surveys, interviews, focus groups and/or experiments. To investigate this influence, marketing professionals would need to look into how different levels of security can influence the success of marketing initiatives. Additionally, it would be important to research the types of attack that can negatively impact a platform, as well as the technologies that can help to improve security. Through collecting and analyzing data, a correlation may be established between increased levels of security and a more successful marketing platform. This could help businesses make decisions about the right security level to invest in, in order to maximize the success of their platform which agreed with Khakimova (2019).

Explaining a variation of 19.2%, the 2nd hypothesis indicated that "Cross Site attacks-security has a statistically positive influence on marketing platforms" and came second in influence. Through results, it was suggested that implementing enhanced security functions to protect online sites and data from attacks, such as cross-site scripting, can positively impact marketing platforms. This could include a variety of marketing elements, such as increasing customer confidence, reducing the prevalence of fraudulent marketing activities, and providing a more reliable experience for customers interacting with marketing platforms. Moreover, improved security measures can create better trust between customers and marketers, and thus open doors to more opportunities for marketing campaigns. Ultimately, a secure and trustworthy environment is important on any platform, but especially on marketing platforms that often require a certain level of trust and security to succeed matching results of Kumar et al. (2022).

In the 3rd rank of influence, it appeared that the hypothesis "Passwords attacks-security has a statistically positive influence on marketing platforms" with a variation of 15.4%. Results indicated that strengthening password security can positively influence marketing platforms. Researchers could conduct experiments to test this hypothesis in order to determine its validity. For instance, researchers could investigate whether marketing platforms that use stronger password security protocols have higher user engagement or better outcomes than those that use weaker password security protocols. They could also analyze data from similar marketing platforms to see whether password security is linked to marketing success. If the analysis suggests a positive correlation between password securities and marketing platform performance, then the hypothesis could be considered confirmed. On the other hand, if weak or no correlation is observed, then the hypothesis could be considered invalid which came in agreement with Mathur (2018).

9. Conclusion and Recommendations

In conclusion, marketers must be increasingly vigilant in promoting digital security within their organizations and maintain a secure and compliant digital infrastructure in order to ensure a safe digital experience for their customers. In particular, this applies to data security, best practices for digital marketing, and implementation of processes that enable secure interactions between the organization, its customers and other stakeholders.

From above results, discussion and conclusion, researcher recommended the following:

- Marketers should educate themselves on the latest threats in digital marketing
- Customers should be encouraged to use strong passwords for their accounts in the website or application
- Marketers should regularly run system and network scans to detect any suspicious activity.
- Marketers should use role-based access to limit the data employees can access and regularly review their permissions.

References

Alanazi, M., Mahmood, A., & Chowdhury, M. J. (2023). SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues. *Computers & Security*, *125*, 103028. https://doi.org/10.1016/j.cose.2022.103028

Asbaş, C., & Tuzlukaya, Ş. (2022). Cyberattack and cyberwarfare strategies for businesses. *Conflict Management in Digital Business*, 303–328. https://doi.org/10.1108/978-1-80262-773-220221027

Asiamah, N., Mensah, H. K., & Oteng-Abayie, E. F. (2022). Non-probabilistic sampling in Quantitative Clinical Research. *International Journal of Applied Research on Public Health Management*, *7*(1), 1–18. https://doi.org/10.4018/ijarphm.290379

Ba, M. H. N., Bennett, J., Gallagher, M., & Bhunia, S. (2021). A Case Study of Credential Stuffing Attack: Canva Data Breach. In *2021 International Conference on Computational Science and Computational Intelligence (CSCI)* (pp. 735-740). IEEE.

Deb, S. K., Mohanty, P. P., & Valeri, M. (2022). Promoting family business in handicrafts through local tradition and culture: An innovative approach. *Journal of Family Business Management*. https://doi.org/10.1108/jfbm-10-2021-0131

Desai, D. M. (2019). Digital Marketing: A Review. *International Journal of Trend in Scientific Research and Development*, *Special Issue*(Special Issue-FIIIIPM2019), 196–200. https://doi.org/10.31142/ijtsrd23100

Junusi, R. E. (2020). Digital marketing during the pandemic period; a study of Islamic perspective. *Journal of Digital Marketing and Halal Industry*, *2*(1), 15. https://doi.org/10.21580/jdmhi.2020.2.1.5717

Gazzari, M., Mattmann, A., Maass, M., & Hollick, M. (2021). My(O) armband leaks passwords. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *5*(4), 1–24. https://doi.org/10.1145/3494986

Gupta, B. B., & Chaudhary, P. (2020). *Cross-site scripting attacks: classification, attack, and countermeasures*. CRC Press. https://doi.org/10.1201/9780429351327

Halesha, P. M., & Arundathi, K. L. (2020). A Study On Digital Marketing and its Impact on Customers of Pl India Securities Pvt Ltd Bangalore.

Haraldsen, G. (2023). What Computerized Business Questionnaires and questionnaire management tools can offer. *Advances in Business Statistics, Methods and Data Collection*, 335–355. https://doi.org/10.1002/9781119672333.ch15

Hashem, T. N. (2021). The reality of internet of things (Iot) in creating a data-driven marketing opportunity: mediating role of customer relationship management (Crm). *J. Theor. Appl. Inf. Technol*, *99*(2),329-342.

Henson, R., Stewart, G., & Bedford, L. (2020). Key challenges and some guidance on using strong quantitative methodology in Education Research. *Journal of Urban Mathematics Education*, *13*(2),42-59. https://doi.org/10.21423/jume-v13i2a382

Herhausen, D., Miočević, D., Morgan, R. E., & Kleijnen, M. H. P. (2020). The Digital Marketing Capabilities Gap. *Industrial Marketing Management*, *90*, 276–290. https://doi.org/10.1016/j.indmarman.2020.07.022

Khakimova, M. C. (2019). Cyber security in digital marketing. In *Развитие бизнеса и финансового рынка в условиях цифровизации экономики* (pp. 275-278).

Khan, O. G., El-Saadany, E. F., Youssef, A., & Shaaban, M. F. (2021). Cyber security of market-based congestion management methods in power distribution systems. *IEEE Transactions on Industrial Informatics*, *17*(12), 8142–8153. https://doi.org/10.1109/tii.2021.3065714

Kolomeets, M., & Chechulin, A. (2021, May). Analysis of the malicious bots market. In *2021 29th conference of open innovations association (FRUCT)* (pp. 199-205). IEEE. https://doi.org/10.23919/fruct52173.2021.9435421

Konyeha, S. (2020). Exploring cybersecurity threats in digital marketing. *NIPES Journal of Science and Technology Research*, *2*(3), 12. 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

Kumar, S., Pallathadka, H., & Pallathadka, L. K. (2022). An Analysis of Cyber Security Threats in Digital Marketing. *Journal of Critical Reviews*, *9*(03), 85-94.

Latchoumi, T. P., Reddy, M. S., & Balamurugan, K. (2020). Applied machine learning predictive analytics to SQL injection attack detection and prevention. *European Journal of Molecular & Clinical Medicine*, *7*(02), 3543-3553.

Lei, Z., Nan, Y., Fratantonio, Y., & Bianchi, A. (2021). On the insecurity of SMS one-time password messages against local attackers in modern mobile devices. *Proceedings 2021 Network and Distributed System Security Symposium*. https://doi.org/10.14722/ndss.2021.24212

Limone, P., Toto, G. A., Guarini, P., & di Furia, M. (2022). Online quantitative research methodology: Reflections on good practices and future perspectives. *Lecture Notes in Networks and Systems*, 656–669. https://doi.org/10.1007/978-3-031-10461-9_45

Magano, J., & Cunha, M. N. (2020). Digital marketing impact on tourism in Portugal: A quantitative study. *African Journal of Hospitality, Tourism and Leisure*, *9*(1), 1-19.

Martins, I., Resende, J. S., Sousa, P. R., Silva, S., Antunes, L., & Gama, J. (2022). Host-based ids: A review and open issues of an anomaly detection system in IOT. *Future Generation Computer Systems*, *133*, 95–113. https://doi.org/10.1016/j.future.2022.03.001

Mathur, M. (2018). Where is the security blanket? developing social media marketing capability as a shield from perceived cybersecurity risk. *Journal of Promotion Management*, *25*(2), 200–224. https://doi.org/10.1080/10496491.2018.1443310

Mirian, A., DeBlasio, J., Savage, S., Voelker, G. M., & Thomas, K. (2019). Hack for hire: Exploring the emerging market for account hijacking. *The World Wide Web Conference*. https://doi.org/10.1145/3308558.3313489

Mishra, P., & Gupta, C. (2020). Cookies in a cross-site scripting: Type, utilization, detection, protection and remediation. *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*. https://doi.org/10.1109/icrito48877.2020.9198003

Mishra, S. (2019). SQL injection detection using machine learning. https://doi.org/10.31979/etd.j5dj-ngvb

Mogaji, E., Soetan, T. O., & Kieu, T. A. (2020). 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

Mukherjee, S., Chittipaka, V., & Baral, M. M. (2021). Developing a model to highlight the relation of Digital Trust with privacy and security for the blockchain technology. *Advances in Marketing, Customer Relationship Management, and E-Services*, 110–125. https://doi.org/10.4018/978-1-7998-8081-3.ch007

Okagbue, H. I., Oguntunde, P. E., Obasi, E. C., & Akhmetshin, E. M. (2021). Trends and usage pattern of SPSS and Minitab Software in scientific research. *Journal of Physics: Conference Series*, *1734*(1), 012017. https://doi.org/10.1088/1742-6596/1734/1/012017

Olson, E. M., Olson, K. M., Czaplewski, A. J., & Key, T. M. (2021). Business strategy and the management of Digital Marketing. *Business Horizons*, *64*(2), 285–293. https://doi.org/10.1016/j.bushor.2020.12.004

Pandey, N., Nayal, P., & Rathore, A. S. (2020). Digital marketing for B2B organizations: Structured Literature Review and future research directions. *Journal of Business & Industrial Marketing*, *35*(7), 1191–1204. https://doi.org/10.1108/jbim-06-2019-0283

Pattewar, T., Patil, H., Patil, H., Patil, N., Taneja, M., & Wadile, T. (2019). Detection of SQL injection using machine learning: a survey. *Int. Res. J. Eng. Technol.(IRJET)*, *6*(11), 239-246.

Pedley, D., Borges, T., Bollen, A., Shah, J. N., Donaldson, S., Furnell, S., & Crozier, D. (2020). Cyber security skills in the UK labour market 2020. *Department for Digital, Culture, Media & Sport*.

Pham, H. C., Brennan, L., Parker, L., Phan-Le, N. T., Ulhaq, I., Nkhoma, M. Z., & Nhat Nguyen, M. (2019). Enhancing cyber security behavior: An internal social marketing approach. *Information & Computer Security*, *28*(2), 133–159. https://doi.org/10.1108/ics-01-2019-0023

Prasad, R., & Rohokale, V. (2019). Cyber threats and attack overview. *Springer Series in Wireless Technology*, 15–31. https://doi.org/10.1007/978-3-030-31703-4_2

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

Saura, J. R., Ribeiro-Soriano, D., & Palacios-Marqués, D. (2021). Setting B2B Digital Marketing in artificial intelligence-based CRMS: A review and directions for future research. *Industrial Marketing Management*, *98*, 161–178. https://doi.org/10.1016/j.indmarman.2021.08.006

Sharma, H. (2022). How short or long should be a questionnaire for any research? researchers dilemma in deciding the appropriate questionnaire length. *Saudi Journal of Anaesthesia*, *16*(1), 65. https://doi.org/10.4103/sja.sja_163_21

Sheridan, R. P., Karnachi, P., Tudor, M., Xu, Y., Liaw, A., Shah, F., Cheng, A. C., Joshi, E., Glick, M., & Alvarez, J. (2020). Experimental error, kurtosis, activity cliffs, and methodology: What limits the predictivity of quantitative structure–activity relationship models? *Journal of Chemical Information and Modeling*, *60*(4), 1969–1982. https://doi.org/10.1021/acs.jcim.9b01067

Singh, R. (2021). Digital Marketing in today's privacy-conscious world. *Digitization of Economy and Society*, 121–151. https://doi.org/10.1201/9781003187479-8

Subramaniam, T. V. (2020). Impact of social media on digital marketing: starbucks marketing strategy on Twitter. *Case study*, *2*, 1-7.

Suleiman, D. A., Awan, T. M., & Javed, M. (2021). Enhancing digital marketing performance through usage intention of AI-powered websites. *IAES International Journal of Artificial Intelligence (IJ-AI)*, *10*(4), 810. https://doi.org/10.11591/ijai.v10.i4.pp810-817

Thomson, D. R., Rhoda, D. A., Tatem, A. J., & Castro, M. C. (2020). Gridded Population Survey Sampling: A systematic scoping review of the field and strategic research agenda. *International Journal of Health Geographics*, *19*(1). https://doi.org/10.1186/s12942-020-00230-4

Trim, P. R. J., & Lee, Y.-I. (2019). The role of B2B marketers in increasing cyber security awareness and influencing behavioural change. *Industrial Marketing Management*, *83*, 224–238. https://doi.org/10.1016/j.indmarman.2019.04.003

Veerabudren, K. R., & Bekaroo, G. (2022). Security in web applications: A comparative analysis of key SQL Injection Detection Techniques. *2022 4th International Conference on Emerging Trends in Electrical, Electronic and Communications Engineering (ELECOM)*. https://doi.org/10.1109/elecom54934.2022.9965264

Wazid, M., Das, A. K., Chamola, V., & Park, Y. (2022). Uniting Cyber Security and machine learning: Advantages, challenges and future research. *ICT Express*, *8*(3), 313–321. https://doi.org/10.1016/j.icte.2022.04.007

Wibowo, R. M., & Sulaksono, A. (2021). Web vulnerability through Cross site scripting (XSS) detection with Owasp Security shepherd. *Indonesian Journal of Information Systems*, 149–159. https://doi.org/10.24002/ijis.v3i2.4192