AN ANALYSIS OF CYBER SECURITY THREATS IN DIGITAL MARKETING

Sanjeev Kumar[1], Dr. Harikumar Pallathadka[2*], Dr. Laxmi Kirana Pallathadka[3]

[1]Career Point University, Hamirpur, Himachal Pradesh, India

[2, 3]Manipur International University, Imphal, Manipur, India

[2*]harikumar@miu.edu.in

ABSTRACT: Addressing cyberspace security problems is essential to success in digital marketing, which is an online business. As the Digital Age evolves, more people choose to work online and start digital and technological businesses. Marketing is a well-known example. Digital marketing is a new marketing genre that has emerged in recent years. Digital marketing is a profitable and crucial industry since it can benefit almost any organization. As more people enter or develop in digital marketing, they need to know how to safeguard their businesses against cybercrime. In cybercrime, personal information and accounts may be stolen, exploited, and tampered with.

Moreover, for a company that runs purely online, it is vital to protect the company's security. This article explains how to secure a digital marketing company's success in the face of ongoing cyber threats. Online websites were used to collect data from persons interested in digital marketing. Research also tries to understand the challenges faced by digital marketers and the measures taken to prevent, fight, and reduce the effects of cyberattacks.

Keywords: Cyber Crime, Cyber Security, Digital Marketing, Digital fraud

Introduction

Cyberattacks are not uncommon. According to leading experts, cybercrime is expected to cause $6 trillion in losses by 2021. Small enterprises and large organizations alike face the same dangers. A cyber assault may happen to anybody at any time. According to research, some small firms have been unable to recover following an assault. That is the extent of the harm that cybercrime can do. It is just going to get worse from here on out. Cybersecurity may seem like a burden that falls solely on the shoulders of your IT department. Digital marketers, on the other hand, bear a disproportionate share of the burden of safeguarding your company's privacy and data. You are a prime target for hackers since you seek to reach a broad audience via marketing strategies. This is the scenario when you post a seemingly innocuous link to your social media profile, only for people to click through. This means that every person who clicks on the link will be affected if the link is harboring malware. The consequences will be even more severe when the assault is carried out via a trustworthy web source.

Many firms nowadays utilize content advertising in digital marketing since it is pretty helpful in attracting and maintaining clients. These sites also provide helpful information to customers. There is a risk of cyber-attacks on content management systems (CMS). WordPress, Drupal, and Joomla are all popular content management systems (CMS) for distributing malware. Using email means of digital marketing severely risks being hacked by internet thieves. Hackers might exploit businesses' email accounts to disseminate spam messages that include viruses, forcing other websites hosted on the same server to be blacklisted as a result. If this danger appears repeatedly, these sites may be put on a blacklist or prohibited, and email advertising and promotion may be discontinued. Social media advertising presents a significant risk of identity theft. Free or illegal downloads, password compromises, or payment transactions are primary causes.

Research problem

Cybercrime is not a word you will hear very often at work, even though it is becoming a more significant and more potent threat to businesses worldwide. People who know how to hack are getting smarter as more and more businesses move their work online. They are also using cloud-sharing technologies to make work more accessible and more productive, but they are also a target for hackers. When you are trying to develop a marketing plan, you do not want your data to be stolen by cybercriminals. This is where this article comes in.

This research paper will help you deal with this issue. The researcher will give you some of the information you need to ensure that digital marketing is safe.

Objectives

The main objective of the research is to analyze the cyber security threat to digital marketing, different types of threats in the current scenario, and the need for introducing a cyber security strategy for the safety of digital marketing.

Research methodology

For the present research paper, the doctrinal methodology has been applied. Researchers have taken the help of secondary sources. Secondary sources include articles, books, journals, newspapers, and websites.

Cyber Transformation?

A cyber transformation uses knowledge gathered from a cyberattack to make internal improvements to your company's security. In addition to improving your cyber strategy, a transformation may help you manage risk. Employees will feel more secure in their roles if their organizations undergo a cyber makeover. If you want your company's transition to be cost-effective and successful, you need a strategy.

Digital Transformation Security Challenges

There are many positive aspects to today's fast-paced digital world, but many negative ones are also. If your firm suffers a data breach, you have a significant security issue to deal with. Data breaches occur when others on the internet obtain access to the information you did not grant them access to, such as when a hacker breaks into your system. This is a dire and frightening situation, and marketers should do all they can to prevent it from happening to anybody.

Cybersecurity in Digital Marketing

Having a solid digital marketing strategy in place is critical to your company's success. Your entire marketing campaign must also be considered secure, from website to emails to social media. You and your client's personal information may be jeopardized if you ignore this detail.
Here are some typical forms of cyberattacks that involves digital marketing:

- *"Malware infection from files downloaded or links clicked"*
- *"Browser hijacking and redirection"*
- *"Stealing of data and other sensitive information."*
- *"Identity theft"*
- *"Proliferation of fake news "*
- *"DDoS attacks on website"*
- *"WordPress malware"*

In addition to these dangers, there are several more types of cyberattacks unknown to most digital marketers.

Investing in a cybersecurity plan is a smart move for your company's image. Aside from the apparent benefit of having a powerful anti-malware system, there are many more benefits. Protecting your clients' personal information is also a benefit. Cross-site scripting, SQL injection attacks, Denial-of-Service assaults, and password cracking are also protected by this software.

It is clear now that cybersecurity is not only the responsibility of your IT department. Claiming ignorance if your company's sensitive data has been breached or your systems have been hacked will not help. Everyone has a role to play in maintaining a safe online environment.

Cybercrime protection is not an insurmountable challenge, but it can be done. If you are concerned about cybersecurity in your digital marketing strategy, here are a few things to keep in mind.

Cyber Security Threats for Digital Marketers

In the digital marketing world, you may assume that cybersecurity is a problem that just your company's IT department has to deal with.

Here is some good news if that is the case: Everyone has a role in maintaining a safe online environment. If your company's sensitive data has been breached, professing ignorance will not help.

However, everything is not lost. Your team and organization may easily be protected from the bulk of cyber thieves.

a. Domain

There are problems with other site hosts as well, not only WordPress. Attacks like XSS, SQL injection, and DDoS, which all take advantage of domain-level security flaws, have grown in popularity in recent years. It is much more dangerous if independent contractors or consultants share your website.

b. Social media

Today's marketers are aware of the power of social media and how it can be used to their advantage. Nevertheless, there is a price to pay for such enormous power. Hackers target social media accounts because they can inflict even more damage than just stealing personal information - hijacking accounts to broadcast offensive things unless you pay them to cease.

There may be numerous people on your team that are utilizing the same social media account, which makes this an issue for your marketing department in particular. Everyone should use a password manager to keep all their passwords safe.

In addition, make sure your employees are aware of the dangers of receiving unwanted social media communications. Hackers may also use Facebook and Instagram to infiltrate your computer systems, as with email scams.

c. The bottom line

Digital marketers cannot afford to overlook cybersecurity because the phrase does not appear in their job descriptions. When a hack or data breach occurs, your personal information is dangerous, but so are the companies you deal with. There is just too much danger for them.

d. Damaged reputation

When a company's reputation is tarnished permanently due to a hack, it is challenging to restore goodwill among the general public. You may lose customers if it seems that your company is not taking the necessary steps to protect the personal information it collects from them. If they hack your accounts, the malicious messages they may send to your business's followers on social media could further harm your reputation.

e. Losing out to competitors

Suppose a hacker can access the company's business plans, including expansion strategies, new goods, and/or new services. In that case, there is a possibility that they may seek to sell this knowledge to rivals, allowing them to benefit from hard work and innovative ideas. In this situation, you can, of course, take someone to court, but it will be a time-consuming and inconvenient procedure. The most effective strategy to combat these issues is to confront them head-on by taking preventative measures and downloading anti-viral software.

f. Ransomware

Ransomware, which may prohibit employees from accessing IT systems until the organization pays a hacker, can also significantly strain a company's finances. According to Hiscox, 6 percent of businesses will pay a ransom in 2021, resulting in a loss of US$381 million.

Additionally, organizations may be required to retain attorneys and other professionals to stay in compliance with cybersecurity rules. They may also be forced to pay even more in attorney fees and damages if they are the target of a cyberattack that results in legal action against the company.

When Equifax, one of the major three credit agencies, had a data breach in 2021 that exposed the personal information of 147 million users, the company learned the hard way. The company agreed to pay up to $425 million in compensation for affected individuals due to the subsequent legal proceedings.

g. Operational Disruption

In addition to direct financial losses, businesses are often subjected to indirect expenses due to cyberattacks, such as the likelihood of a significant stoppage in operations, which may result in revenue losses.

Cybercriminals may stifle a company's usual operations in various ways, including infecting computer systems with malware that deletes high-value information or placing malicious code on a server that prevents customers from accessing your website.

Hacktivists, who have been known to infiltrate the computer systems of government agencies or multinational organizations in the name of exposing a perceived injustice or promoting transparency, are a popular weapon for disrupting normal corporate operations.

During the WikiLeaks controversy in 2010, for example, hackers sympathetic to the organization reacted against payment card companies Mastercard and Visa by launching assaults that caused their websites to go down briefly.

h. Altered Business Practices

Cybercrime has the potential to influence organizations in ways other than financial. Companies must reconsider how they gather and retain information if they want to avoid exposing sensitive information to unauthorized access. In recent years, customers' financial and personal information, such as credit card numbers, Social Security numbers, and birth dates, has been removed from many organizations' databases.

Some businesses have shut down their online storefronts because they are concerned that they will not be able to secure themselves from hackers fully. Customers are also more interested in learning how the organizations with whom they do business deal with security challenges. They are more willing to favor upfront and outspoken businesses about the security measures they have put in place to protect themselves.

i. Intellectual Property

Product designs, technology, and go-to-market strategies are frequently among a company's most significant assets, as are the relationships with customers and partners. Intellectual property adviser Ocean Tomo estimates that intangible assets accounted for 87 percent of the total market capitalization of S&P 500 businesses in 2015.

A large amount of this intellectual property is housed on the cloud, where it is subject to cyberattacks and theft. About 30 percent of U.S. corporations have reported that a Chinese competitor has stolen their intellectual property in the last ten years.

j. *Lost Revenue*

A rapid loss in income as clients flee to safer havens is one of the worst results of a cyberattack. Companies might potentially suffer financial losses due to extortion attempts by hackers. When Sony Pictures was about to release "The Interview," a comedy depicting an assassination attempt on North Korean leader Kim Jong Un, it was targeted by terrorists. Hackers made off with personal data from the company, including humiliating emails and appraisals of employees' work performance. North Korea has denied responsibility for the incident, although it is generally suspected that the country orchestrated it. As a consequence of this, Sony Pictures decided to distribute the picture online rather than in cinemas, which cost the company $30 million.

Methods for the protection of Digital Marketing from Cyber Attacks

When it comes to conducting campaigns, marketers must exercise extreme caution since digital marketing works with your company's data and the data of your consumers. Here are some of the most prevalent places that need extra care regarding internet security.

1. *Email*

Email marketing may seem to be a relic of the past, yet it remains one of the most successful methods of promoting a company today. When it comes to digital marketing, it has one of the best returns on investment (ROI), and it may assist in enhancing website traffic and conversion rates.

Unfortunately, emails are also well-known for being the preferred means of malware distribution. Emails are responsible for more than 90 percent of all assaults. Hackers often use phishing strategies to locate their next potential victim via the use of emails.

These criminals often send out emails that seem to be legitimate but, in reality, include links to fake websites or harmful files. Hackers send emails that seem like they are from genuine organizations, such as banks, PayPal, Amazon, Netflix, government agencies, or non-profits, all in an attempt to get personal information from you. Furthermore, the sort of assault that follows is determined by the information you have provided to the adversary. Because they are the ones that connect with consumers regularly, your digital marketing staff is particularly exposed to these types of attacks (or hackers disguised as customers). To keep your emails safe, ensure that everyone on your team knows how to recognize a phishing email. In addition to using a secure password and your email service provider's spam filter, you may help keep these risks at bay by following the recommendations above.

2. *WordPress*

WordPress' inclusion on this list may appear unexpected. WordPress is one of the most heavily-targeted CMS systems, as you will learn if you keep up with cybersecurity headlines. Hackers begin their attacks by exploiting the platform's security holes in many cases. Other hackers take advantage of the flaws in widely used WordPress plug-ins.

Beyond obsolete software, hackers may access a site or cause it to be unavailable in other ways, such as by using one of the following methods:

- *"DDoS Attack — This attack floods your website with an insane amount of traffic to break your server and website"*
- *"Cross-site Scripting — This happens when a hacker inserts a malicious code into your website to steal the data that enters your server"*
- *"SQL attacks — The hacker tries to gain access to your website's database"*
- *"Password Attack — Using weak passwords, such as your personal information, recycled passwords, or simple characters, makes it easier for hackers to access your data"*

Keeping your WordPress account up-to-date is the greatest method to defend it from internet attacks. Enabling automatic updates ensures that you get critical security fixes promptly. Remember to keep an eye on the plugins and extensions you are using to ensure they are up to current.

Enable two-factor authentication when it is available and use secure passwords. Protect your website by setting up a Web Application Firewall in the background of your website. In order to secure your website using SSL, you will need a digital certificate.

3. *Social Media*

Social media is one of the most efficient digital marketing channels at the moment, with billions of people using it every day. All ages utilize social media platforms, including Facebook, Instagram, YouTube, Twitter, and WhatsApp. Considerable potential, on the other hand, brings with it significant risk. Social media accounts are a favorite target for cybercriminals, and it is not only the accounts of celebrities that are often targeted. The more harm they can do by taking over other people's accounts, the better. If they obtain your login details, attackers may also hijack accounts and publish objectionable stuff on your profile. Those being harassed may be compensated for their services, or they may be hired by the businesses they are harassing to perform the dirty work. Marketing teams are particularly vulnerable because of the common practice of having numerous people log into the same social media account simultaneously. You may use a password manager or a social media management tool to restrict the dissemination of your login data. This includes training employees about the perils of unsolicited social media communications that include links. Hackers may infiltrate your system through social media sites like Facebook and other social media platforms, just as they can do with emails to fool you into disclosing personal information.

4. CRM Software

CRM (customer relationship management) software is a critical component of any digital marketing strategy since it houses all of your client's personal information. You may save and analyze your customer information in a CRM system and utilize it to create an effective marketing plan for your firm.

Assume that intruders breach your CRM system. They will be able to get their hands on that information, which they may then use to commit crimes. This breach will cost you money, but it also has the potential to harm your company's image.

It is not enough to keep your CRM software safe by using a complex password. Because it will not be as successful as you imagine, it is necessary to adopt a new method. Why? Because the majority of breaches originate from the inside. Ensure that only trustworthy personnel have access to the data in your CRM program. Those with access should be vetted to ensure that they can be trusted. Before entrusting your clients' data to your employees, do background checks. Please consider using account-monitoring software. It would be perfect. Finally, there should be no regulation allowing employees to bring their own devices to work. There should only be one device per employee, and that device should only be used for official business purposes.

Result and Discussion

Endpoint security, also known as endpoint protection, is one of the most influential and effective solutions available for preventing cybercrime. Endpoint security, also known as endpoint protection, is a strategy to protect computer networks that are remotely bridged to client devices. The linking of computers, tablets, mobile phones, and other wireless devices to business networks opens the door for cybercriminals to infiltrate corporate networks. The capacity of endpoint software to prevent issues from occurring is one of the most important reasons for its widespread use. Rather than merely addressing problems as they arise and take hold, the software can prevent them from occurring in the first place.

Malware put into a network via an external device linked to the network will not be prevented from accessing the network by a firewall. Typical antivirus software will respond to viruses. However, it will not necessarily prevent access to the network. This implies that even if you have these two barriers in place against hackers, your marketing plan will not be secure unless you decide to invest in endpoint security for all of your business's computers.

Implementing a successful cybersecurity strategy should be an intrinsic component of your overall B2B marketing strategy and plan. By demonstrating to your business partners that you take your cybersecurity duties seriously, you maintain your brand values while also protecting the company's interests.

In order to be successful in your digital marketing firm or to be successful in your job, you must take cybercrime seriously. Several experts from companies specializing in digital forensics have said that cybercrime is becoming a widespread concern for those who use computers and the Internet. As a result of people's increasing reliance on technology, he believes that hackers are getting more proficient. In light of the above, here are some tips for safeguarding your digital marketing firm or your digital marketing employment from cybercrime.

a. Software Up to Date

Keeping your digital marketing firm secure from cybercriminals may be as simple as following these simple steps. Software code flaws are among the most prevalent methods by that hackers get access to accounts and information. When a bug in the program is discovered and reported to the developers, an update is released to correct the problem. As a result, hackers may discover this flaw in the code and exploit it to get access to an individual's account, document, etc. Keeping your software up to date is important because hackers can see what software has been updated and what software has not.

b. Email Marketing Security

We must ensure that the email marketing system is safe to protect your marketing material and the personal information of your customers. A hacker would attempt to acquire access to an email account since it is one of the essential tools in digital marketing.

In order to protect your customers' private information, you should use email marketing solutions that have security mechanisms that encrypt and restrict access to the information they contain. Employees should be trained on maintaining these systems secure and preventing data breaches from guaranteeing that your marketing email is safe and sound.

c. Encrypt and Back-Up Sensitive Data

The most straightforward strategy to avoid a security breach and prevent hackers from taking all of your data in the case of cybercrime is to encrypt and back up data. This implies that only persons who know the decryption key/password can decipher the encrypted material. As with making copies and storing them on another device or in the cloud, backing up data is as simple as doing just that.

d. Set Up Strict Limitations

To protect themselves, digital marketing businesses should impose tight rules prohibiting their staff from installing or opening files that contain malware. It is possible to preserve yourself from a disastrous occurrence by enforcing solid digital restrictions. Preventing malware from entering your company's computer and network is as simple as being proactive and putting in place rigorous controls.

e. Keep Digital Marketing Content Secure

Because cyber criminals often prey on digital marketing firms, you must take every precaution to keep your systems safe. Keep these four digital marketing security recommendations in mind to keep yourself, your staff, your customers, and your whole organization safe and secure. Incorporating the advice in this guide can help you avoid being a victim of cybercrime.

Conclusion

In this case, the most crucial factor to remember is that digital marketers cannot afford to overlook cybersecurity just because it is not part of their job description. From the top down to the bottom up, everyone must take responsibility for the situation. A cyber-attack puts your data in danger and puts the data of all of your customers and other organizations that do business with you at risk.

Every marketing plan should incorporate the development of a sound cybersecurity strategy. The sections above should be given extra attention since they are the gateways via which most attackers enter the network. By resolving these problems, you will be able to advertise your company without being concerned about your online security anymore.

References

Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders, and attacks. *Journal of Cyber Security and Mobility*, 65-88.

Behera, R. K., Bala, P. K., Rana, N. P., & Kizgin, H. (2021). Cognitive computing-based ethical principles for improving organisational reputation: A B2B digital marketing perspective. *Journal of Business Research*.

Bowen, G., & Sethi, A. (2022). Internal Marketing Cybersecurity-Conscious Culture. In *Research Anthology on Business Aspects of Cybersecurity* (pp. 376-395). IGI Global.

Bauer, J. M., & Dutton, W. H. (2015). The new cybersecurity agenda: Economic and social challenges to a secure internet. *This is a joint working paper for the Oxford Global Cybersecurity Project at the Oxford Martin Institute, University of Oxford, and the Quello Center at MSU. It is based on a briefing document prepared by the authors to support the World Bank's World Development Report (2015).*

Chowdhury, M., & Bakar, A. (2016). Opportunities and challenges of digital marketing in Bangladesh.

Chaffey, D., & Ellis-Chadwick, F. (2019). *Digital marketing*. Pearson UK.

Das, R., & Patel, M. (2017). Cyber Security for Social Networking Sites: Issues, Challenges, and Solutions. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, *5*(4,833-838).

Das, R., & Patel, M. (2017). Cyber Security for Social Networking Sites: Issues, Challenges, and Solutions. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, *5*(4,833-838).

Gordiyevskaya, A. (2020). Ethics in digital marketing.

Gani, M. O., & Faroque, A. R. (2021). Digital marketing. In *Cross-Border E-Commerce Marketing and Management* (pp. 172-202). IGI Global.

Hamid, A., Alam, M., Sheherin, H., & Pathan, A. S. K. (2020). Cyber security concerns in social networking service. *International Journal of Communication Networks and Information Security*, *12*(2), 198-212.

Konyeha, S. (2020). Exploring Cybersecurity Threats in Digital Marketing. *Marketing*, *2*(3), 12-20.

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

Krasyuk, I., Kirillova, T., & Amakhina, S. (2019, October). Marketing concepts development In the digital economic environment. In *Proceedings of the 2019 International SPBPU Scientific Conference on Innovations in Digital Economy* (pp. 1-6).

Le, D., Nguyen, T. M., Quach, S., Thaichon, P., & Ratten, V. (2021). The Development and Current Trends of Digital Marketing and Relationship Marketing Research. In *Developing Digital Marketing*. Emerald Publishing Limited.

Madan, P. (2021). Digital marketing: a review. *V Paradigm shifts in management practices in the era of industry*, *4*, 64-71.

McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of awareness and training on cyber security. *Journal of Internet Commerce*, *9*(1), 23-41.

Mathur, M. (2019). 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.

Mishra, C. K. (2020). Digital Marketing: Scope Opportunities and Challenges. In *Promotion and Marketing Communications*. IntechOpen.

Moniruzzaman, M. (2018). *Analyze the customer effectiveness of digital marketing* (Doctoral dissertation, Daffodil International University).

Moşteanu, N. R. (2020). Challenges for Organizational Structure and design as a result of digitalization and cybersecurity. *The Business & Management Review*, *11*(1), 278- 286.

Mustafa, H. Digital Social Engineering Threatens Cybersecurity. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, *9*(1), 4016-4025.

O'Raghallaigh, E. (2017). Security issues in e-commerce. *Available from: Crossref. Date accessed*, *15*(02).

O'Raghallaigh, E. Latest Trends in the Field of Digital Marketing.

Pham, H. C., Brennan, L., Parker, L., Phan-Le, N. T., Ulhaq, I., Nkhoma, M. Z., & Nguyen, M. N. (2019). Enhancing cyber security behavior: an internal social marketing approach. *Information & Computer Security*.

Paul, A. K., Bhoi, S. K., & Srivasthva, V. (2019). Ideal Host for Digital Marketing: A Multi- Criterion Decision Model Approach.

Pashkov, V., Soloviov, O., & Harkusha, A. (2021). Digital Marketing: Problems of Internet Pharmacies Legal Regulation.

Rahman, K. T. (2021). Applications of Blockchain Technology for Digital Marketing: A Systematic Review. *Blockchain Technology and Applications for Digital Marketing*, 16-31.

Raghallaigh, E. O. Latest Trends in the Field of Digital Marketing.

Ryan, D. (2016). *Understanding digital marketing: marketing strategies for engaging the digital generation*. Kogan Page Publishers.

Rao, N. J. (2015). Cybersecurity: Issues and Challenges. *CSI Communications, 39.*

Razzaq, A., Hur, A., Ahmad, H. F., & Masood, M. (2013, March). Cyber security: Threats, reasons, challenges, methodologies, and state-of-the-art solutions for industrial applications. In *2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS)* (pp. 1-6). IEEE.

Sharma, A., Sharma, S., & Chaudhary, M. (2020). Are small travel agencies ready for digital marketing? Views of travel agency managers. *Tourism Management, 79*, 104078.

Soldatova, A. V., Budrin, A. G., Budrina, E. V., Solovieva, D. V., & Semenov, V. P. (2020, September). Information Technologies in the Management of Digital Marketing Communications. In *2020 International Conference Quality Management, Transport, and Information Security, Information Technologies (IT&QM&IS)* (pp. 534-537). IEEE.

Srivastav, P., & Gupta, H. (2021, September). Role and Applications of Digital Marketing in Digital Era: A Review. In *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)* (pp. 1-5). IEEE.

Sayyad, S., Mohammed, A., Shaga, V., Kumar, A., & Vengatesan, K. (2018, December). Digital Marketing Framework Strategies Through Big Data. In *International Conference on Computer Networks, Big data and IoT* (pp. 1065-1073). Springer, Cham.

Sharma, A. (2018). Research on Digital Marketing Trends & Utilization. *International Journal of Research and Analytical Reviews*, *5*(2), 1263-1270.

Trim, P., & Lee, Y. I. (2016). *Cyber security management: a governance, risk and compliance framework*. Routledge.

Westerlund, M., & Rajala, R. (2014). Effective digital channel marketing for cybersecurity solutions. *Technology Innovation Management Review*, 22-32.

Zamsuri, A., Syafitri, W., & Pane, E. S. (2021). Evaluation of Information Security Awareness on Digital Marketing (Case Study of MSME in Indonesia). *Advances in Humanities and Contemporary Studies*, *2*(1), 192-210.

Zeebaree, S., Ameen, S., & Sadeeq, M. (2020). Social media networks security threats, risks, and recommendation: A case study in the Kurdistan region. *International Journal of Innovation, Creativity and Change*, *13*, 349-365.

Pallathadka, H., Kumar, S., & Pallathadka, L. K. (2021). Cyberbullying Vis-A-Vis Emotional Unrest: A Study on Digital Justice. *Journal of Cardiovascular Disease Research*, *12*(02), 541–549.

Pallathadka, H., & Pallathadka, L. K. (2022). Adaptation of Digital Banking Channels by Indian Consumers – An Empirical Study. *International Journal of Psychosocial Rehabilitation*, *26*(01), 83–92.

Pallathadka, H. (2020). A Survey Of Undergraduate Students On Online Learning During Covid-19 Pandemic In The Indian State Of Manipur. *European Journal of Molecular & Clinical Medicine*, *07*(08), 5914–5927.

Kumar, S., Pallathadka, H., Pallathadka, L. K., & Kumar, V. (2021). An Empirical Investigation On Consumer Behavior Concerning Online Shopping During Covid-19 In India. *International Journal of Aquatic Science*, *12*(03), 3087–3096.

Pallathadka, H., & Pallathadka, L. K. (2022). Challenges and Opportunities of Online Learning in India. *International Journal of Psychosocial Rehabilitation*, *26*(01), 55– 67.

Pallathadka, H. (2020). A Study on Buyer Behavior in Green Marketing Products. *European Journal of Molecular & Clinical Medicine*, *07*(01), 4540–4548.

Kumar, S., Pallathadka, H., Kumar, V., & Pallathadka, L. K. (2021). Consumer Behavior Vis-À-Vis Online Shopping During COVID-19 : An Empirical Investigation through Digital Mode in India. *Design Engineering Toronto*, *2021*(9), 1776–1784.

Pallathadka, H., & Pallathadka, L. K. (2022). Role of Digital Marketing on Consumer Purchase Intention. *Journal of Contemporary Issues in Business and Government*, *28*(2), 236–246.

Kumar, S., Pallathadka, H., & Pallathadka, L. K. (2022). Legal Perspective of Porn Production in India: A Study with Special Reference to Onlyfan.com. *Journal of Contemporary Issues in Business and Government*, *28*(3), 351–365.

Pallathadka, H., & Pallathadka, L. K. (2022). Review Consensus Effects on E-Wom and Consumer Goods E-purchase Satisfaction: A Quantitative Investigation. *Journal of Contemporary Issues in Business and Government*, *28* (2), 214-222.