DISCOVERING RELATIONSHIP BETWEEN SOCIAL MEDIA USAGE AND CYBERSECURITY AWARENESS: AN ASSOCIATION MINING ANALYSIS

-Prerna Popli, Student, Department of Management Studies, RDIAS
-Akanksha Upadhyaya, Associate Professor, Department of Management Studies, RDIAS
-Manoj Kumar Mishra, Assistant Professor, OPJU, Raigarh, Chhattisgarh

ABSTRACT

The term cyber security pertains to the protection of computer systems, networks, devices, data, and other related entities from potential threats, hazards, or assaults. The level of awareness of cyber security pertains to the extent to which a user possesses knowledge regarding the potential threats that may compromise the security of their network. In contemporary times, the utilization of social media platforms has witnessed a significant surge, thereby raising apprehensions regarding the safety of online activities and the perpetration of cyber offenses. The aforementioned circumstance necessitates the implementation of cyber security measures in conjunction with the cultivation of a positive digital social environment. Despite the convenience of accessing information from any location, there exists a potential risk of unauthorized disclosure of personal data to unintended recipients. Despite the prevalence of cybercrime as a significant threat to individuals, a considerable number of individuals remain unaware of its existence. Despite the fact that security is a subject that is addressed in distinct modules within numerous general computer science programs, it remains uncertain whether the implementation of cyber security measures is necessary. The objective of this research is to examine the correlation between the utilization of social media platforms and the level of consciousness regarding cybercrimes among individuals. The research employed the Apriori algorithm to detect associations, and the findings indicated robust associations among various variables pertaining to knowledge of cyber security. The statistical significance of the associations was evaluated through the utilization of three metrics, namely confidence, lift, and leverage. The results of the study could be utilized to enhance the knowledge of social media users regarding cyber security and emphasize the significance of staying up-to-date with cybercrimes and safeguarding oneself while utilizing social media platforms.

Keywords: Cyber security, social media, social media sites, cyber-attacks, Cybercrime, Association mining, apriori

INTRODUCTION

Today internet has captured the entire world in its web. From smallest thing to the global news everything is now available on internet. Its has taken over the encyclopaedia's which people used to refer sometimes back. Not only this it has left behind the era of postcards or letters and switch to modern period ways of communication which are namely Instagram, Facebook, Telegram, WhatsApp and so on.

But this step towards modernization also has some loop holes i.e., Cyber threat. Every year there are several cases of internet frauds, malware, scamp, virus, spyware, ransomware, phishing and insider threats. This arises the need of cyber security along with healthy social life. Cybersecurity refers to preserving the security, confidentiality, and accessibility of computing resources that are either owned by a company or connected to the network of another business. (Kaur & Ramkumar, 2022) Cyber refers to everything using computers, particularly the internet, and security is centred around being safe from harm or threat. In general, cyber security refers to safeguarding against threat, danger, or attack any computer, network, system, data, or device. The level of a user's knowledge of the threats to their network is referred to as cybersecurity awareness.

Depending on the level of technological development and crimes in each nation, distinct obstacles to cyber security exist. protection against cybercrime covers both public and private protection for the nation. The most prevalent types of cybercrime stem from accessing accounts on social networks and bank account information.

Although everyone is now extremely concerned about the risk of cybercrime, many people haven't even heard of it. The practise of displaying personal information on social networking sites has become the primary method used by hackers and scammers to obtain personal information. In spite of the fact that security is covered in isolated modules in many general computing science degrees, the need for active implementation of the cyber security method is still not evident. (English & Maguire, 2023)

This study primarily examines the level of knowledge that people of all ages have concerning cybercrime and cyber security. 159 replies to a questionnaire distributed to the group are gathered for this.

LITERATURE REVIEW

(Rosanne English and Joseph Maguire, 2023) In this study, the authors provide a method for investigating the expectations of learners of online Safety courses at two institutions in the United Kingdom. The intention is to attract attention towards the issues raised by students so that curricula can be changed to better address their needs. The goal of this paper was to make sure that students gain a grasp of fundamental cyber security ideas so they can support workplace security procedures. In order to achieve various accreditation standards, it is also important to make sure that persons who desire to pursue careers in security are appropriately prepared by developing comprehension of more difficult and abstract areas of cyber security. Furthermore, it's important to manage the expectations and perceptions that students frequently already have.

(Thilini B. G. Herath, Prashant Khanna and Monjur Ahmed, 2022) According to the study, there are numerous cyber threats that can affect users of social media sites including lost productivity, cyberbullying, cyberstalking, stolen identity, social networking stress, erratic branding, image damage, security breaches, worms, network outages, malware, and unauthorized possession of social media accounts. The study's other conclusions include the possibility that demographic parameters such as age, gender, and educational attainment may not always have a significant impact on internet users' cyber awareness.

(Diptiben Ghelani, 2022) This study examined a number of subjects, such as information security and locales where safety planning is likely to be addressed, including military sources. Nine security measures have been noted. The usage of various security techniques in organisations is investigated using the qualitative focus group method. Security officers from eight different companies were asked to explain their organisations' security policies in focus groups. The results show that many businesses employ a preventive strategy to maintain the availability of IT services. On an operational level, a few of the other techniques were applied to assist the preventative plan. Additionally, the papers analysed take an IT-based approach to cybersecurity rather than just a management-based one. A management perspective should assist organisations in properly implementing new organisational practises and change management procedures. This study can be used by future research as a foundation in resolving industry investigations and advancing the current state of the art.

(Jagpreet Kaur, K.R. Ramkumar, 2021) The major goal is to give scholars a glimpse of the intriguing developments and difficulties that cybersecurity presents. The most popular approaches and techniques for dealing with security-related issues, their difficulties, and new technologies like computer science and quantum physics are all covered in detail. This comprehensive overview of cybersecurity provides a way for fresh researchers to continue the process of enhancing this field with cutting-edge methods for potential applications. Although there is a dearth of polynomial-based encryption in the literature, a future wave of security algorithms may be based on them. We discovered that adding polynomials to the spectrum of security methods has a very broad application.

(Talal Alharbi and Asifa Tassaddiq, 2021) The study's objective was to examine and assess graduates' levels of awareness of security and user interaction. Academic institutions need information security because most users don't understand the fundamentals of cyber security or how to safeguard their gadgets from viruses, Trojan horses, scams, etc. Responses were collected from 576 college students to an online survey questionnaire. The snowball sample method was followed to increase the sample length. It is assessed that the behaviour of people even in the presence of a good level of awareness is the main obstacle to overcome in managing cyber security threats and challenges. This paper specifically focuses on level of awareness and predictors: use of security tools, phishing, cryptology, browser security, social networking, and cyber security knowledge

(Abdulaziz Alzubaidi, 2021) This study aims to assess Saudi Arabia's current level of internet safety awareness in terms of cyber-security procedures, awareness level, and incident reporting. With regard to cybercrime activities, this study offered a comprehensive review of the present internet safety data from a number of people from various Saudi origins, age groups, areas, and genders while also considering the rise in internet users since 2018. It also outlined the rationale for choosing TAM being an approach over others. It has been found that the model based on TAM is more significant than the UTAUT model. UTAUT model focuses on the demographical elements of the respondents like age, gender schooling, and so on in addition to expertise and information associated with the cyber services. Therefore, it is concluded that TAM model is found to be highly significant than that of UTAUT model in case of current research study.

(Yuchong Li, Qinghui Liu, 2021) This study's objective is to assess and analyse the standard advancements made in the area of cyber safety as well as to evaluate the challenges, limitations, and advantages of the suggested solutions. Furthermore, rising trends and modern-day developments of cyber safety and safety threats and provocations are provided in this paper. The concept of security, the omission of the geographical component of cyberthreats, and the degree of exposures posed by cyberthreats can all be used to analyse the occurrence of power dissipation.

(Moti Zwilling, Dušan Lesjak, Fatih Cetin, Hamdullah Nejat Basim, Galit Klien, Wiukasz Wiechetek, 2020) The aim of this research is on facts associated with cyber security awareness, expertise and behaviour. The centre of attention was on a comparative technique to assess cultural variations in cyber security awareness, expertise and behaviour. Additionally, the findings indicates that higher cyber knowledge is attached to the extent of cyber awareness, beyond the variations in respondent country or gender and cyber awareness is attached to safety tools. The end result indicates that the variables did no longer show multicollinearily. It is observed that all the nations confirmed negative but significant correlation.

(Pieter Potgieter, 2019) The purpose of this paper is that pupil's shortfall to interact with cyber security awareness initiative. He additionally advised that educational institutions can make a contribution to unfold awareness amongst college students via presenting Cyber safety awareness material. The responses were collected from 43 students enrolled for the computer security subject at central college of technology unfastened nation, were approached to take part in the research. The end results indicated that the uses of those platforms via the respondents were restricted. However, Facebook, YouTube, Websites and e-mails were the most popular media according to the results.

(Rohit, Anvesh Babu, Ranjith Reddy, 2019) The cyber-terrorism ought to make institutions to lose billions of bucks within the area of companies. This study outline the elements of cyber terrorism and incentive. Case studies associated with cyber protection also are lay out in this paper. A few solutions associated with cyber protection and cyber terrorism also are described in it. This study attempts to bring together all available information on cybercrime, provide historical context, and generate reports based on the data analysis of various attacks that have been widely reported over the past five years. In the next years, cybercrime has the potential to cause significant harm in the information age. The experts have calculated an approximate loss of nearly 6 trillion dollars. Therefore, there is a very bright future for those who deal with cybercrime-related issues and put in place all necessary security measures.

(K. Senthilkumar and Sathishkumar Easwaramoorthy, 2017) By focusing on numerous online security threats, the study's main objective is to monitor undergraduates in Tamil Nadu's awareness of cyber safety. This poll investigates the degree of security awareness among university students, and some advice is provided to address these issues. This study indicates that the college students in Tamil Nadu are having above common degree of attention on Cyber associated risk issues that can assist them to shield themselves from the cyber-assaults. Cyber security attention amongst the university students in Tamil Nadu is analysed by means of thinking about distinctive security problems that are e-mail phishing, password strength, hostile codes and so on. The cyber security recognition amongst university students in Tamil Nadu is measured as 69.45% from both males and females.

(Y. POORNIMA, Y. NAVEENA, Mr.V.HARSHA VARDHAN, 2017) Cyber protection prevention require extra heed to solve difficult long-time period issues regarding layout, incentives, consensus, and environment. In this study, the control of Cyber protection risks, government function and long-term issues are talk through. The cyberspace is a crucial area for massive number of terrorists to assault on influential data infrastructure. The present legal guidelines are insufficient to halt the cybercrime and, as a result urging a heed to adjust the prevailing legal guidelines via which those activities may be placed on a test. As a consequence, it calls for a collaboration of countries to work collectively and minimize the ever developing threats and danger at an attainable stage. The department of homeland security (DHS) is the primary federal attention of information sharing for civilian systems via its national Cyber security and Communications Integration Centre (NCCIC). The department of Justice (DOJ) is the lead corporation for enforcement of applicable legal guidelines.

(Samaher Al-Janabi and Ibrahim Al-Shourbaji. 2016) The point of interest of this research is to examine the data on security awareness amongst educational researchers, students and employee in academic surroundings within the centre East. Additionally, to apprehend the extent of awareness of information security, its related threat and effect at the organization. 760 which include academic Star, researchers, undergraduate students and employees. The questionnaire was made to obtain the level of cyber security and awareness for the targeted participants groups. This research gave a critical pointer approximately the extent of information safety attention in the EE in connection with information safety attention as well. therefore, EE's want for information safety awareness may be within the form of a set of protection measures and suggestions to fix their sensitive records and to make sure that information are stored safely in addition to boom the attention stage.

(Jigar Shah, 2016) This study seeks to identify the solutions to troubling questions like, "Is the citizen actually aware that he or she is are at risk to various cybercrimes? "; "If person is conscious, to what extent?"; and, "If not aware of online crimes, what steps can be embraced in order to make residents more aware and updated." A conceptual explanation of how to uphold and implement awareness campaigns among internet users regarding cybercrimes was also advised by this study. This study thus demonstrates that web users in Anand are not fully informed about current cybercrimes and cyber security. 100 teenage internet users were surveyed on their knowledge of cybercrimes. No matter the safety precautions taken, if a person does not know how to handle the personal information, they give online or in public spaces, they run the risk of being taken advantage of. Thus, the experts in the interview insisted on the role of government in initiate proper mechanisms to build and coach ethical hackers for a holistic approach of cyber security.

(G. NIKHITA REDDY, G.J. UGANDER, 2014) This research particularly specializes in provocation confronted via cyber safety in the today's technology. It additionally specializes in the cyber protection strategies, ethics and the traits that are converting the face of cyber safety. pc protection is a huge subject matter that is turning into greater dominant due to the fact the society is turning into fairly interconnected, with networks being used to deliver out vital transactions.

(Deepa.T.P., 2014) According to an assessment by the government's Ministry of Information Technology, India would require five lac cyber protection executives by 2015 in order to keep up with its quickly expanding online economy. Over 2 lakh new employees are anticipated to be hired in the financial sector alone, with the remaining 3 lakh to be hired in the telecom, utility, power, fuel & gas, airline, and government sectors. The statistics of this research ensures that India as a fast-growing country especially in the field of information technologies and E-commerce has a high alert for Security for its online channels to monitor over frauds and financial losses. This paper also talks about counteroffering, economic crimes, money laundering, hacking, internet fraud, etc

(Noluxolo Kortjan, 2013) The key aim of this research was to advise web safety attention along with academic structure for SA in order to help in developing a cyber-safety lifestyle in SA amongst all of its users of the net. Moreover, to perceive the position of attention and academics in a Cyber safety lifestyle and to assess the tasks that a few advanced nations have in area for cyber safety attention and training.

(Priti Saxena, Bina Kotiyal, R H Goudar, 2012) The attribute for cyber-protection are era, operations and attention, education and training. This research emphasis on the problems associated with cyber-safety in India and additionally provides numerous techniques to convey attention at founder tiers in academic system. as a result, there may be a heed of cyber safety curriculum inside the destiny in order to assist in growing the cyber protection knowledge in the teenagers and eventually the IT zone gets greater profound, securely professional experts no longer most effective within the security zone however additionally within each quarter, as a way to improving the communication, the mind compatibility abilities of the personnel and the employers.

OBJECTIVE OF STUDY

The objective of the study is to examine the existence of a relationship between the use of social media platforms and awareness towards cybercrimes. The study aims to identify associations between the frequency of using social media platforms and awareness towards cybercrimes among individuals who frequently use social media. The study also seeks to determine the level of cyber-security knowledge while using social media platforms. To achieve this, the researchers used the Apriori algorithm using Weka tool to identify associations among the variables.

METHODOLOGY

Al-Masalha, Hnaif, & Kanan (2020) and Arpaci & Aslan (2022) conducted research that emphasized the relationship between social media usage and awareness of cybercrime, indicating a necessity to explore these connections. In order to accomplish this objective, the study utilized the apriori algorithm to examine a primary dataset consisting of 159 participants. The adequacy of the sample size in the study was determined based on the commonly accepted guideline of obtaining a minimum of 100 responses. The survey instrument employed in the research consisted of preliminary inquiries aimed at screening out participants who exhibit negligible or sporadic utilization of social media platforms. The participants were requested to indicate the social media platforms on which they possess accounts and the frequency at which they utilize them. According to the statistical data released by Statista in 2022, Facebook, Instagram, and YouTube were identified as the foremost social media platforms in India. Figure 1.1 illustrates the proportion of traffic directed towards the aforementioned platforms.

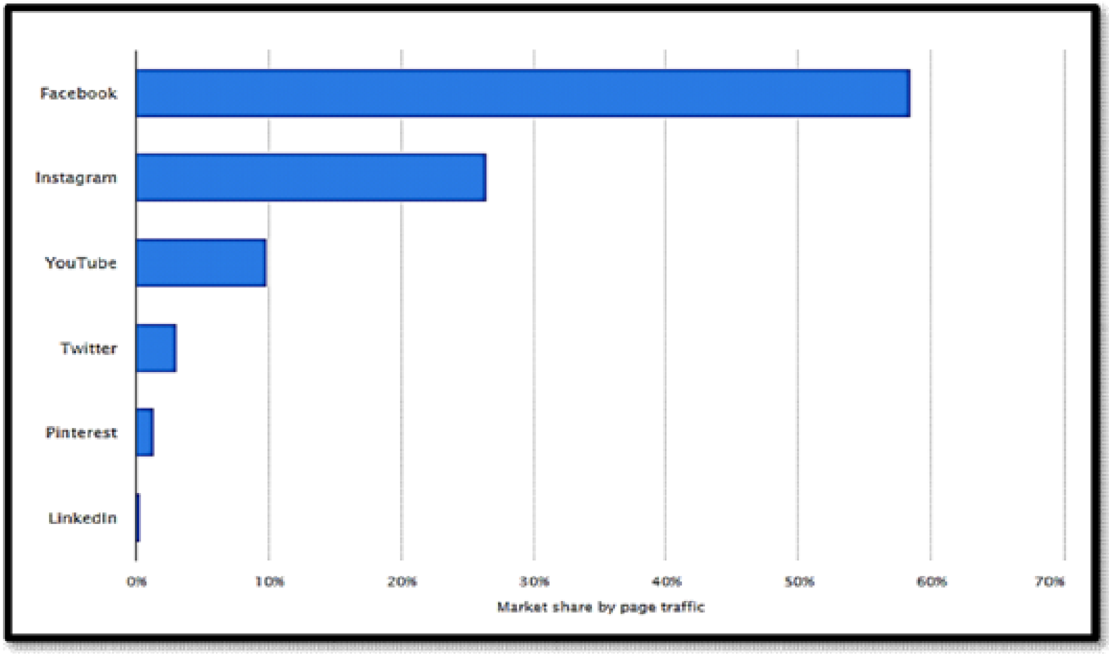

Fig. 1.1. Leading social media sites across India 2022.

Source: https://www.statista.com/statistics/1115648/india-leading-social-media-sites-by-page-traffic/

The research employed a 5-point Likert scale to assess the frequency of utilization of social media platforms. The scale utilized a range of values, with "Never used" assigned a score of 1 and "Always used" assigned a score of 5. Participants who reported using social media either occasionally, frequently, or always were deemed eligible to participate in the subsequent survey that aimed to assess their knowledge of cybercrimes in relation to social media platforms. The survey utilized a 5-point Likert scale to evaluate various factors associated with cyber security knowledge. These factors included but were not limited to awareness of cyber security, comprehension of diverse forms of cyber-attacks, familiarity with security tools, understanding of the consequences of cybercrime, knowledge of regulations and guidelines pertaining to cyber security and cybercrime, and technical proficiency. The dataset was gathered via the distribution of a questionnaire through social media platforms and email. Respondents were given a one-month period to participate.

DATA ANALYSIS

Association mining is a data analysis technique used to identify patterns and relationships among variables in a dataset. In this case, the dataset consists of responses from 159 individuals regarding their knowledge of cyber-security and related topics. Weka is a popular data mining software used to analyze such datasets. The output of association mining in Weka is a set of rules that indicate the strength of the association between variables in the dataset. These rules are expressed in terms of their confidence, lift, and leverage.

In the results presented, three rules have been generated that indicate a strong association between different variables related to cyber-security knowledge.

Association Rule	Confidence	Lift	Leverage	Conv.
{I know how to use security tools at various social media platform= Strongly Agree} ^ { I am aware about impacts of cybercrime = Strongly Agree} =>{ I am aware about different means of cyberattack like phishing, fraud, hacking, etc=Strongly Agree}	1	4.97	0.09	14.38
{I am aware about different means of cyberattack like phishing, fraud, hacking, etc=Neutral} ^ { I am aware about impacts of cybercrime = =Neutral } => { Rate yourself on your technological knowledge. =Neutral }	1	2.41	0.06	9.94
{I am aware about different means of cyberattack like phishing, fraud, hacking, etc=Strongly Agree} ^ {. I am aware about impacts of cybercrime. (The use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy.) =Strongly Agree} => {I know how to use security tools at various social media platform. =Strongly Agree}	0.9	3.77	0.08	5.07

DISCUSSION

The evaluation of the importance of rules in association mining is commonly assessed through three metrics, namely confidence, lift, and leverage. The confidence metric quantifies the ratio of occurrences within the dataset in which the antecedent of a given rule, situated on the left-hand side, implies the consequent of the same rule, located on the right-hand side. Stated differently, it quantifies the frequency with which the rule holds true for the given dataset. The confidence interval lies within the bounds of 0 and 1, where a score of 1 signifies the rule's infallibility. The lift metric quantifies the strength of the relationship between the antecedent and consequent of a rule, while accounting for the occurrence frequency of each item in the dataset. The term "support" refers to the frequency of occurrence of a particular itemset in a dataset. In the context of association rule mining, the support of a rule is the proportion of transactions in the dataset that contain both the antecedent and consequent of the rule. The lift of a rule is a measure of the degree of dependence between the antecedent and consequent of the rule, and is defined as the ratio of the observed support of the rule to the expected support if the antecedent and consequent were independent. When the lift value is greater than 1, it signifies a positive correlation between the variables. Conversely, a lift value less than 1 indicates a negative correlation. The concept of leverage pertains to the quantification of the dissimilarity between the observed support of a given rule and the anticipated support that would have been obtained if the antecedent and consequent were not related. The degree of dependence between the antecedent and consequent is a metric that can be used to assess their association strength (Witten, Frank, & Hall, 2016; Tan, Steinbach, & Kumar, 2013; Agrawal, Imielinski, & Swami, 1993). A high value of this metric indicates a strong association between the two variables.

Collectively, these three metrics aid in evaluating the importance of the regulations produced by association mining. Typically, rules that exhibit elevated levels of confidence, lift, and leverage are deemed to be more consequential and substantial, as they signify a robust correlation between the variables. The obtained rules are of significant value as they offer valuable insights into the interdependent relationships among variables. These rules can be utilized to devise effective strategies aimed at enhancing the level of cyber-security awareness among individuals.

According to Rule 1, individuals who express a high level of agreement regarding their proficiency in utilizing security tools across multiple social media platforms and their comprehension of the consequences of cybercrime are also inclined to possess knowledge regarding diverse methods of cyber-attacks such as hacking, phishing, and fraud. The confidence level of the rule is 1, indicating that all participants who express a strong level of agreement regarding the initial two variables also exhibit agreement concerning the third variable. The lift coefficient of 4.97 denotes a robust correlation between the variables, while the conviviality coefficient of 14.38 implies that the rule is exceedingly significant.

According to Rule 2, individuals who hold a neutral stance regarding their familiarity with various forms of cyber-attacks and the consequences of cybercrime are also inclined to evaluate their technological expertise as neutral. The aforementioned rule exhibits a confidence level of 1, indicating that respondents who express a neutral stance towards the first two variables also hold a neutral stance towards the third variable. The lift value of 2.41 denotes a moderate association between the variables, while the conv value of 9.94 indicates the statistical significance of the rule.

According to Rule 3, individuals who exhibit a high level of agreement regarding their knowledge of diverse forms of cyber-attacks and the consequences of cybercrime are more inclined to possess proficiency in utilizing security tools across multiple social media platforms. The aforementioned regulation exhibits a confidence level of 0.9, indicating that 18 out of 20 participants who express a strong agreement regarding the initial two variables also demonstrate concurrence concerning the third variable. The lift value of 3.77 denotes a moderate association between the variables, while the conv value of 5.07 indicates the rule's significance.

To summarize, the aforementioned regulations propose that there exist robust correlations among the variables pertaining to cyber-security knowledge among the participants in the given dataset. The regulations may be utilized to acquire comprehension regarding the variables that impact one's knowledge of cyber-security and to formulate tactics for enhancing cyber-security consciousness among individuals.

CONCLUSION

Technology can be considered a double-edged sword. The process of interacting, connecting, or exchanging data with other systems or devices over the internet has become significantly streamlined. The act of disseminating data to external systems carries with it the inherent risk of unauthorized access by third parties. The potentiality of cybercrime, which encompasses unauthorized online activities such as fraudulent schemes, hacking, malware dissemination, ransomware attacks, phishing, and the like. The term cybersecurity pertains to the protection of computer systems, networks, devices, data, and other related entities against potential threats, hazards, or attacks. The degree of an individual's comprehension regarding potential hazards to their network is commonly known as cybersecurity awareness.

The objective of the research paper was to ascertain the correlation between the utilization of social media platforms and the level of consciousness regarding cybercrimes. The research utilized the Apriori algorithm to analyze the main dataset consisting of 159 participants. The research revealed a robust correlation among various factors pertaining to cyber-security literacy. The Weka software's association mining technique produced three rules that demonstrate a robust correlation among various variables pertaining to knowledge of cyber-security. The metrics of confidence, lift, and leverage were utilized to measure the significance of these rules. To conclude, the research emphasizes the necessity for individuals to possess knowledge regarding cyber security when utilizing social media platforms. The findings indicate that possessing expertise in security tools, being cognizant of diverse modes of cyber-attacks, and comprehending the ramifications of cybercrime are crucial in augmenting an individual's awareness of cyber security. The results of this investigation have the potential to assist both individuals and organizations in devising efficacious tactics to alleviate the hazards associated with cybercrime.

References

1. Alzubaidi, A. (2021, January). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. ScienceDirect. https://www.sciencedirect.com/science/article/pii/S2405844021001213
2. Al-Janabi, S., & Al-Shourbaji, I. (2016). A Study of Cyber Security Awareness inEducational Environment in the Middle East.Researchgate. https://www.researchgate.net/publication/292672963_A_Study_of_Cyber_Security_Awareness_in_Educational_Environment_in_the_Middle_East
3. Kumar .K., S., & Easwaramoorthy, S. K. (2017). A Survey on Cyber Security awareness among college students in Tamil Nadu. Iopscience.Iop. https://iopscience.iop.org/article/10.1088/1757-899X/263/4/042043
4. Kortjan, N. (2013, November). A Cyber Security Awareness and Education Framework for South Africa. Core.Ac.Uk. https://core.ac.uk/download/pdf/145053774.pdf
5. Li, Y., & Liu, Q. (2021, November). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. ScienceDirect. https://www.sciencedirect.com/science/article/pii/S2352484721007289
6. Potgieter, P. (2019, October 25). The Awareness Behaviour of Students on Cyber Security Awareness by Using Social Media Platforms: A Case Study at Central University of Technology. Easychair. https://easychair.org/publications/paper/wVsR
7. POORNIMA, Y., NAVEENA, Y., & VARDHAN, V. H. A. R. S. H. A. (2017, May). Cyber Security Issues and Challenges in India. Ijser. https://www.ijser.org/researchpaper/Cyber-Security-Issues-and-Challenges-in-India.pdf
8. Shah, J. (2016, December). A Study of Awareness about Cyber Laws for Indian Youth. Ijtsrd. https://www.ijtsrd.com/papers/ijtsrd54.pdf
9. Saxena, P., Kotiyal, B., & Goudar, R. H. (2012, January). A Cyber Era Approach for Building Awareness in Cyber Security for Educational System in India. Researchgate. https://www.researchgate.net/profile/Bina-Kotiyal/publication/271298620_A_Cyber_Era_Approach_for_Building_Awareness_in_Cyber_Security_for_Educational_System_in_India/links/5e10abf7299bf10bc38f707e/A-Cyber-Era-Approach-for-Building-Awareness-in-Cyber-Security-for-Educational-System-in-India.pdf
10. T.P., D. (2014, January). Survey on need for Cyber Security in India. Researchgate. https://www.researchgate.net/publication/267313908_SURVEY_ON_NEED_FOR_CYBER_SECURITY_IN_INDIA
11. Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., & Basim, H. N. (2020, February 14). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. ResearchGate. https://www.researchgate.net/publication/339273589_Cyber_Security_Aw areness_Knowledge_and_Behavior_A_Comparative_Study
12. English, R. and Maguire, J. (2023) "Exploring student perceptions and expectations of cyber security," Proceedings of 7th Conference on Computing Education Practice [Preprint]. Available at: https://doi.org/10.1145/3573260.3573267.

13. Kaur, J. and Ramkumar, K..R. (2022) “The recent trends in Cyber Security: A Review,” Journal of King Saud University - Computer and Information Sciences, 34(8), pp. 5766–5781. Available at: https://doi.org/10.1016/j.jksuci.2021.01.018.
14. Agrawal, R., Imielinski, T., & Swami, A. (1993). Mining association rules between sets of items in large databases. ACM SIGMOD Record, 22(2), 207-216.
15. Tan, P. N., Steinbach, M., & Kumar, V. (2013). Introduction to data mining. Pearson Education.
16. Witten, I. H., Frank, E., & Hall, M. A. (2016). Data mining: practical machine learning tools and techniques. Morgan Kaufmann.
17. Al-Masalha, H., Hnaif, A. A., & Kanan, T. (2020). Cyber-crime effect on jordanian society. Int. J. Advance Soft Compu. Appl, 12(3).
18. Arpaci, I., & Aslan, O. (2022). Development of a scale to measure cybercrime-awareness on social media. Journal of Computer Information Systems, 1-11.