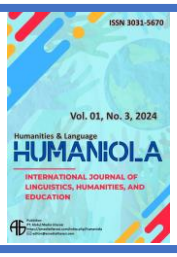
Humaniola Humanities and Language
International Journal of Linguistics, Humanities, and Education
Volume 1 Issue 3, June 2024
E-ISSN 3031-5670



Digital Transformation and Cyber Security: Unveiling Awareness

Padmavati S. Undale [1], & Vedant Shinde [2*]

[1,2] MIT Arts, Commerce and Science College, Alandi, Pune, India.
*Correspondence author: vedantshinde2783@gmail.com

ARTICLE INFO

Keywords:
Cyber-Crime Victims; Cyber Security Awareness; Technological Threat Knowledge

Article history:
Received 03 April 2024
Revised 05 May 2024
Accepted 20 June 2024
Available online 30 June 2024

DOI: https://doi.org/10.32734/ayr9wh15

ABSTRACT

The research paper extensively examines the critical exigency for cyber security measure and advocates for increased public awareness regarding the nature of cyber-crimes, along with the proactive measures to shield against these pervasive threats. Cyber security entails a strategic practice designed to fortify system, network and program files from potential infiltrations within digital networks. Cyber-crimes predominantly focus on illicitly accessing or obliterating sensitive information, posing to substantial risk to individual and organizations alike. This comprehensive study is based on a combination of primary and secondary data sources. The primary data set encompasses responses to a meticulously crafted questionnaire provided by 298 individuals across diverse age groups, while the secondary data comprises information collated from multitude of esteemed researcher. The findings gleaned from the data analysis reveal alarming instances of individual being subjected to abuse resulting from the compromise of their social media accounts, falling victim to various forms of financial fraud and incurring substantial monetary losses through investment in spurious accounts. The study highlights the paramount needs to assess the populace's level of awareness regarding cyber security guideline, with a considerable proportion of respondent demonstrating a commendable understanding of prescribed courses of action to undertake in the event of succumbing to cyber-crimes. The overarching objective of this study is to obtain a comprehensive understanding of cyber security.

How to cite:
Undale, P.S., & Shinde, V. (2024). Digital transformation and cyber security: unveiling awareness. *Humanities & Language: International Journal of Linguistics, Humanities, and Education*, 1(3), 191-197.

1. Introduction

In today's interconnected digital world cyber security plays a crucial role in safeguarding our software, online information and activities. Cyber security involves in protecting our computer, software, network and data from unauthorized access. It's like having a lock on your door to keep intruders out of your homes but in the virtual realm. By being aware of cyber security best practices and proactive measure, we can ensure our online experience are safe and secure. The reason behind all cyber-crime is that the particular software can be easily hack or lack of proper measure. The cyber security aims to reduce the cyber-crime making new system and new technology. The present research paper is to understand how much people are aware about such technology. In

worlds one of the safest software is used by bank then also such software gets hacked. So, to know the reason behind it

The primary aim of this research paper is to gain a comprehensive understanding of cybersecurity and its impact on both individuals and large organizations. As cyber-crimes continue to rise, there is a growing concern that if these trends persist, it could lead to a decline in online and technology usage. This paper seeks to inform and encourage people to embrace new technologies while emphasizing the importance of understanding cybersecurity.

The objectives of the study are as follows: to assess the level of cybersecurity awareness among people of various age groups; to identify those who have been victims of cyber-crimes; to gather suggestions from the public on how to combat cyber-crimes; and to understand public perceptions and responses to cybersecurity incidents.

2. Methodology

The present research is based on primary as well as secondary data of various researcher and through government publish data. Random sampling method was used to collect the data. Respondents are of thirteen to fifty years age group.

2.1. Data Collection

The primary data for this study was gathered using a structured questionnaire, which included both close-ended and a few descriptive questions. Responses were collected from 298 individuals ranging in age from thirteen to fifty years, providing detailed insights into cybersecurity awareness and experiences.

In addition to primary data, secondary data was sourced from published literature, government reports, and other relevant documents. These sources provided additional context and supported the analysis of the primary data.

3. Literature review

Mr. Ashwini Sheth, Mr. Sachine Bhosale and Mr. Farish Kurupkar (2021) in the report on “Cyber Security” discuss the concept of cyber security in the modern world, highlighting the vulnerabilities of cyberspace, the evolution of cyber threats, the cyber security challenges faced globally. It also explores the cyber situation in India, recent cyber-attacks, data breach statistics, hardware cyber security concern, future technology consideration for enhancing security measure.

Pallavi Murghai Goel (2019) in the report on “A Literature Review of Cyber Security” provides a literature review of cyber security, emphasizing the difference between cyber security and information protection. It discusses the broader scope of cyber security, including the protection of individual from cyber-attack, ethical implication, the importance of safeguarding marginalized groups. The paper also delves into distinction between information security & ICT security.

Somesh Rai, Dr. K. Singh & A. K. Verma in the report on “Global Research Trend on Cyber Security” discuss the global research trend on cyber security using scientometric analysis. It focuses on analyzing scholarly literature related to cyber security to understand its growth in various dimension. The study utilizes data from the database, covering 2720 document published on cyber security from 2001 to 2018.

Mr. Harsha Vardhan (2017) in the report on “Cyber Security Issues and Challenges in India” provides insights into the challenges of cyber security, emphasizing

the need for international cooperation to combat cybercrime and the modification of existing laws for more efficient regulation. It also discusses the interdependence of information and communication technology and the crucial role of cyber security in protecting this system. Additionally, it highlights the vulnerabilities in cyber security, such as acts by insider, supply chain vulnerabilities and unknown weakness, presenting cyber security as an ongoing battle between attacker and defender. The document also touches on existing counter cyber security initiatives.

Hadi Saeed Alqahtani (2016) in his report on "Latest Trend and Future Direction of Cyber Security Information System" highlights the significance of cyber security in protecting information system from threats and attacks. It emphasizes the impact of cyber security risk on organization, such as financial losses, and the need of collaborative strategies and security measure. Key points include the challenges of cyber defense, the emergence of new technological threats, and the development security control and responses practice.

"India Cyber Threat Report 2023" by Data Security Council of India (DSCI) and SEQRITE reveals 2023 threat areas and predictions about 2024. The threats in the digital transformations in the sectors such as banking, logistics are increased. It alerts about the increase in use of 'Artificial Intelligence' in scams may rise which includes mimicking voices.

Considering the above literature on cyber-crime and cyber security, the need was identified to research on cyber-crime victims and status of awareness about it amongst the diversified respondents.

4. Data Analysis and Interpretation

Table 1. Number. of respondent

Sr.no	Age group	Respondent	Percentage
1	13-21	171	57.40%
2	21-35	76	25.50%
3	35-50	51	17.10%

In the table 1, the data indicates a higher representation of respondent within the age group on 13-21, with a comparatively lower number of respondents from 35-50 age bracket. Moreover, the analysis reveals 76 respondents falling within the age group of 21-35.

Table 2. Victim of abuse language

Sr.no	Particular	No of respondent	Percentage
1	Often	10	03.40 %
2	Sometime	65	21.80%
3	Never	223	74.80%

In the table 2, the analysis reveals that the majority of respondent have never been victims of abusive language as a result of cyber-crime. However, 3.40% of total respondent reported frequent experience of abusive language due to cyber-crime, while 21.80% of respondent have encountered it on occasional basis.

Table 3. Victim of financial fraud

Sr.no	Particular	Respondent	Percentage
1	Often	12	4%
2	Sometime	53	17.80%
3	Never	233	78.20%

In the table 3, the data highlight a minority of respondent who have frequently encountered financial fraud resulting from investment in fraudulent accounts or schemes, with some respondent indicating occasional experience in this regard. Notably, a significant of majority of 78.20% of total respondent have not encountered financial fraud incident.

Table 4. Loss of money due to investing in false account

Sr.no	Particular	No of respondent	Percentage
1	Yes	36	12.10%
2	No	262	87.90%

In table 4, the data present the instances of respondent experiencing financial losses resulting from the investing in false account. The analysis reveals minimal occurrences of respondent encountering monetary losses due to such investment with the majority reporting no financial losses in this context.

Table 5. Do you know where to complaint for cyber-crime?

Sr.no	Particular	No of respondent	Percentage
1	Yes	148	49.70%
2	No	150	50.30%

In the table 5, the data indicate the extent to which respondent are aware for appropriate channel for reporting cyber-crime. The analysis reveal that significant portion of the respondent lack knowledge about relevant complaint mechanism, while approximately half of the respondent are familiar with the appropriate avenue for lodging complaints.

Table 6. Knowledge of cyber security guidelines

Sr.no	Particular	No of respondent	Percentage

1	In detail	34	11.40%
2	Up to some extent	180	60.40%
3	Not at all	84	28.20%

In the table 6, the data illustrate the level of awareness among respondent regarding cyber security guideline. Specifically, it indicates that 60.40% of total respondent possess a basic understanding of cyber security guidelines. Furthermore, approximately 28.20% of total respondent reported a lack of any knowledge pertaining to cyber security guidelines. Interestingly, only 11.40% of respondent exhibited a comprehensive understanding of these guideline. The finding underscores an imperative need to enhance awareness & knowledge of cyber security guideline.

Table 7. Loss of money due to sharing OTP

Sr.no	Particular	No of respondent	Percentage
1	Yes	22	7.40%
2	No	276	92.60%

In the table 7, the data reveal a minimal number of respondents who suffered financial losses resulting from their disclosure of one-time password (OTP). The majority of respondent did not experience monetary losses due to this security breach.

Table 8

Table 8. Victim of photo morphing

Sr.no	Particular	Respondent	Percentage
1	Yes	6	2%
2	No	292	98%

Certainly, the table indicate that a small percentage of respondent reported experiencing the issue of photo morphing, a type of cyber-crime used to export money from individuals. The survey result reveals a minimal incident of victimization related to this specific form of cyber-crime.

The responses received on descriptive question on how to overcome cyber-crime and promote cyber security are as follows:

- Government should start some initiative in order to make people educate about cyber security guideline.
- Update security guideline.
- Do not share personal and sensitive information on unknown website.
- Change password of accounts from time to time in order to avoid risk of cyber-crime.
- Do not use public WI-FI and also not share OTP with anyone.
- Multi factor authentication.

5. Findings

The research findings show a low prevalence of cyber-crimes such as photo morphing and victimization through abusive language among the surveyed respondents. Financial fraud incidents were reported by a minority, with 78.20% of respondents never having experienced such fraud. Instances of losses due to false accounts were minimal, indicating that most respondents managed to avoid financial losses. Awareness levels regarding cybersecurity guidelines varied, underscoring the need for comprehensive educational initiatives. The minimal financial losses from the disclosure of one-time passwords suggest some awareness of cybersecurity practices. Overall, the study highlights the critical importance of ongoing awareness programs to effectively mitigate cyber risks.

The study identifies several key areas to focus on for enhancing cybersecurity awareness:

1. Increasing cybersecurity skills among users.
2. Addressing the inadequate knowledge of cyber-crimes, such as where to report incidents and what actions to take.
3. Simplifying the complexities of cyber technologies.
4. Providing continuous guidance on vulnerabilities in IoT devices.
5. Educating on how to identify insider threats.
6. Conducting cybersecurity awareness sessions and integrating them into the education system.

6. Recommendations

To improve cybersecurity awareness, the study recommends the following actions:

1. Integrate cybersecurity education from primary to advanced levels, regardless of the field of study.
2. Implement continuous and rigorous awareness programs for groups that are easily victimized.
3. Ensure that helpline and support systems are readily available.
4. Incorporate emerging advanced technologies into cybersecurity strategies.
5. Foster proper collaboration and coordination with cybersecurity professionals.
6. Enforce strict adherence to cybersecurity regulations.

7. Conclusion

Cybersecurity is essential for protecting documents, private information, software, and other digital assets from cyber-crimes such as hacking and misuse of personal information. This research highlights the urgent need for cyber literacy among the public. The study reveals that many respondents lack awareness of cybersecurity guidelines, a critical need in the current situation. The research aims to identify the factors responsible for day-to-day cyber-crimes, emphasizing that the primary cause is the lack of knowledge about which information should be kept confidential.

References

Alqahtani H. S. (2016). Latest Trend and Future Direction of Cyber Security Information System, *Journal of Information Engineering and Applications*, *Vol.6* (No.) pg. 09 to 14. https://iiste.org/Journals/index.php/JIEA/article/view/34213/35183 .

Data Security Council of India (DSCI) and SEQRITE. (2023). *India Cyber Threat Report 2023*. https://www.dsci.in/files/content/knowledgecentre/2023/India_Cyber_Threat_Report_2023.pdf

Goel P. M. (2019). A Literature Review on Cyber Security. *International Journal Of Research And Analytical Reviews*, Volume 6 (Issue 2), pg. 136-140. https://www.ijrar.org/papers/IJRAR1CBP189.pdf.

Poornima Y., Naveen Y. and Harsha Vardhan V. (2017). Cyber Security Issues and Challenges in India. *International Journal of Scientific & Engineering Research*, *Volume 8* (Issue 5), p.g. 135-140. https://www.ijser.org/researchpaper/Cyber-Security-Issues-and-Challenges-in-India.pdf

Rai S., Singh K. and Verma A. K. (2019). Global Research Trend on Cyber Security: A Scienometric Analysis. *Library Philosophy and Practice*.pg. 01-20. https://digitalcommons.unl.edu/libphilprac/3769.

Sheth. A., Bhosale S. and Kurupkar F. (2021). Research Paper on Cyber Security, *Contemporary Research in India*, Special Issue April, 2021, pg. 246-251. https://www.researchgate.net/publication/352477690_Research_Paper_on_Cyber_Security

Singh, B, (2022). *India's cybersecurity and its impact on the economy*. https://www.gatewayhouse.in/indias-cybersecurity-and-its-impact-on-the-economy/