# A STUDY ON CUSTOMERS PERCEPTION ABOUT SIGNIFICANCE OF DIGITAL SECURITY

Dr. Priyanka Amol Pawar, Assistant Professor,
Indira College of Engineering & Management, Pune.
p.priyanka22@gmail.com

Dr. Reena Partha Nath, Assistant Professor,
Sinhgad Institute of Business Administration and Computer Application, Sinhgad Technical Education Society, Lonavala Campus, Lonavala, (Kusgaon Bk), Pune.
reenanath29@gmail.com

Dr. Pratap Pawar, Associate Professor and Deputy Director,
Siddhant Institute of Business Management, Pune.
pvpawar.raj@gmail.com

## ABSTRACT

In recent years, digital threats have posed significant risk to organizations and individuals. Unfortunately, many people in the public and private sectors still lack the advanced knowledge required to understand how digital threats work and the risk they pose. This study is done to know the customers perception about the significance of digital security in an important scenario. The study is based on a survey of 223 individuals in Pune city, Maharashtra, India who use internet/ mobile banking. The results of the study indicate that the difference of the perception regarding the importance of digital security between male and female is not statistically significant, male and female both show higher levels of importance towards security. The study reveals that there is a significant difference in the level of importance regarding digital security with the income groups. The study also shows that there are no significant differences in regard with the age groups.

**Keywords:** digital security, customer perception, risk, online banking

## Introduction

In the past decade, there has been an exponential growth in information technology and e-commerce development and future applications for IT/e-commerce could not be predicted. As a result, the security of e-commerce networks is becoming an increasing concern for organizations, because of various cyberattacks including denial of service (DoS), virus, spam and email scams.

There are more than 8 billion dollars lost per year by the organizations due to digital security attacks (Thompson, 2019). Considering that 10% of these losses come from international e-commerce companies, it can be said that these losses are increasing worldwide with each passing day. This perspective on the importance of digital security shows an alarming increase in the level of concern. The purpose of this study is to identify the level of concern of customers regarding digital security in their daily activities.

In recent years, digital threats have posed significant risk to organizations and individuals. Unfortunately, many people in the public and private sectors still lack the advanced knowledge required to understand how digital threats work and the risk they pose. It is evident that there is an urgent need for information security training for employees at all organizational levels. In the face of increasing risks in our digital world, digital security has emerged as a new form of national security that needs to be safeguarded and managed.

Types of digital frauds:
1. Carding: In this type of fraud there are two types:
a) Carding is the act of obtaining sensitive data through accessing the systems of another organization without being authorized.
b) Carding is transferring funds from one account to another using stolen or expired credit cards.

2. Spam scam: In this type of fraud, an email message purporting to be from a legitimate sender is sent to users indiscriminately via multiple computers and often receives large quantities of replies from users, flooding the recipient with unwanted material.

3. Phishing: This type of fraud is when an entity creates a website and uses fake or stolen emails to convince the users to disclose their confidential information.

4. Pharming (Spoofing): In this type of fraud, fraudulent and unauthorized IP addresses are used by hackers to gain unauthorized access to a server or network with the aim of collecting sensitive data.

5. Viruses and Trojans: This type of fraud replicates a legitimate program and intercept user or system data leading to the compromise of the network.

To protect against cybercriminals, organizations need to guarantee the security of their systems, use strong authentication and encryption techniques, employ a layered security model, implement password management techniques, educate users about threats and frauds, employ intelligent monitoring tools to detect changes in IT networks.

The aim of this study is to identify the level of concern regarding digital security in daily activities by male and female participants – whether there is any difference between the two in concerns. Also analyse how income groups are affected with respect to digital security precautions.

**Literature review**

There are literatures about the research. Raghu, Josephine, Abbamanya and Ananthanarayan (2014) conducted a survey to find out the awareness of detecting cyber threats and the awareness of knowledge sharing in educational institutions among instructional staff members at two private universities in Chennai. The survey was conducted on 100 staff members from two private universities in Chennai. The results revealed that there are opportunities for improvement in the awareness of cyber threats. The results also highlight that there is an urgent need for the instructional staff to educate students on cyber security matters.

Sharma and Jharna (2014) conducted research in order to explore the perception of government and private organizations regarding the importance of digital security. Using survey technique 100 from government organizations, 100 from private organizations were selected randomly and a survey was conducted among them. This study shows that most of the participants are unaware about digital security practices and their perception toward it is not positive. Further, the study shows that steps should be taken to educate the public about digital security.

The results of this survey indicate that there is an urgent need for an improved awareness on digital security. Further, it is reported that there are 50% of individuals who are unaware about their own financial transactions. There is 74% ignorance among users regarding digital security in general and 68% regarding online banking (Kanade, 2014).

Kumar and Dixit (2015) conducted a study to identify the level of digital security awareness among bank employees and customer satisfaction towards it in Pune city. The study found that total 41% of the customers are unaware about digital security whereas 58% of them are aware about it. The study also found that 85% of the bank employees are aware of digital security. The study recommends that steps should be taken to educate customers and employees regarding digital security.

Kapoor (2019) conducted research to explore the awareness towards digital security among e-commerce users in India. The survey was conducted among 250 consumers. The results of the study reveal that only 37% of the consumers are unaware about digital security whereas 63% of them are aware about it. This study also found that there is a need for improvement in the awareness and practices regarding digital security among e-commerce users.

Miller (2021) conducted a survey to find out the level of security awareness among 31-year-old and 62 year old middle class Indians regarding digital frauds. The survey was conducted among 540 respondents from middle class households in India. The results revealed that more than half of the respondents are unaware about digital security. It further states that more than 45% of the respondents have less knowledge about digital security. This study also shows that there is a need for effective awareness programs regarding cyber threats for these consumers (Sharma, 2014).

Mishra (2022) conducted a survey to find out the level of security awareness among e-commerce customers regarding digital frauds in India. The survey was conducted among 200 online customers in India. The study shows that 75% of the respondents are unaware about digital security. This study also found that 45% of the consumers are aware about digital security but there is a need for improvement in their awareness and practices regarding cyber threats.

Singh (2021) conducted research to find out the level of information sharing on cyber security among employees at Indian companies. The research revealed that there is a need for effective cyber security information sharing policies and education on cyber security issues at corporate level. Digital security techniques guarantee security against cyber threats. The techniques can be classified into four categories as follows:

a. Authentication: This type of security ensures that the identity of the user matches with the identity that is being electronically transmitted.

b. Encryption: This type of security protects data against unauthorized access. It uses advanced encryption algorithms to ensure its secrecy.

c. Access control: This type of security keeps unauthorized users out by maintaining strict rules in access control and monitoring internal networks (Sharma, 2014).

d. Malicious code detection and prevention: This type of security measures can be used to detect and prevent malicious code from getting into the networks which are being attacked (Singh, 2021).

The findings reveal that there is a need for effective cyber security awareness programs among employees at corporate levels. There are also different types of cyber threats for different types of organizations and industries. Some of them are mentioned below:

a. Government attacks: Government attacks are most dangerous as they can penetrate government networks and steal sensitive information to harm the system. For example, an attack on a bank could be carried out by breaking into the computers of online access control, stealing passwords and emails to spy on private information.

b. Attackers: These attackers are dangerous as they may not have malicious intentions. They may steal information or track people who have stolen credit card numbers and other sensitive data to sell it further to hackers for huge profits.

c. Hackers: This is a group of individuals who are responsible for a cyber-attack against some organization or industry by either breaking into the system or gaining unauthorized entry into the system (Chauhan, 2021).

d. Spammers: These are individuals who send mass emails or messages to users to promote their products. They may also install malicious software on the computers of users.

The study reported that there is an urgent need for development of effective cyber security awareness programs among the above-mentioned categories of individuals and groups.

Vaishnav (2018) conducted research to find out the level of cyber fraud awareness among Indian teenagers. The study found that due to increased digitalization, there is an alarming increase in cyber frauds. This study also found that there is a need for effective awareness programs on cybersecurity among teenagers.

Digital security involves the procedures and measures that are taken to secure computer systems from unauthorized access or malicious attacks from hackers and other types of cyber criminals. It is a broad term that encompasses many aspects ranging from information security over network security to physical security (Stephens, 2014).

There are various techniques that can be used to ensure digital security:

a. Authentication: This type of security ensures that the identity of the user matches with the identity that is being electronically transmitted. Examples of authentication techniques include logins, passwords, and email addresses (Henderson, 2012).

b. Web-based authentication: This type of security is widely used by many organizations and industries to authenticate users or customers. Web-based authentication involves use of unique codes or passwords which are sent to users through emails which they need to enter to access some information or applications (Salama & Salama, 2014).

c. Encryption: This type of security protects data against unauthorized access. It uses advanced encryption algorithms to ensure its secrecy. Encryption works on the principle of converting information into an unintelligible form. This form is known as a cipher and only the intended recipient can convert it back into readable form. To encrypt data, it needs to be first broken into a string of comma-separated numbers (Wang, 2018).

d. Access control: This type of security keeps unauthorized users out by maintaining strict rules in access control and monitoring internal networks (Henderson, 2012).

e. Detection and prevention: This technique can be used to detect and prevent malicious code from getting into the networks that are being attacked (Riesing, 2019).

The word cyber security is derived from the words “cybernetics", "computer" and "security". Cybernetics refers to a branch of science that involves the control of information and communications systems using feedback (Borchardt, 2017). This type of security also involves proper analysis and management of communication media. The development of computers and computer networks has led to a new era in cyber security. Computers have been heavily used in all kinds of activities including different types of applications such as health care, education, banking, military, business management and communications.

There are mainly three types of devices known as computers: desktops, laptops and embedded systems. Desktop computers are used in offices and other areas where users need to perform many tasks. Laptops are small portable computers that are used for traveling, writing papers and other types of applications. Embedded system is a type of computer that is found in cars, planes and various mechanical devices like motor vehicles, air conditioners, washing machines and refrigerators etc.

**Objectives of the study**

1. To understand the importance of digital security
2. To study customers perception about the significance of digital security
3. To determine the differences in the perception regarding the importance of digital security with gender, age, and income.

**Hypotheses**

H1: There is no difference in perception regarding the importance of digital security between the genders.

H2: There is no difference of perception regarding the importance of digital security among different age groups.

H3: There is no significant difference in the level of importance regarding digital security within the income groups.

**Research methodology**

This research was conducted using a quantitative survey method. A total of 223 customers from Pune city were surveyed, who use internet/ mobile banking service. The questionnaire contained a combination of open-ended and closed-ended questions on the topic of digital security.

Cross-sectional design: This study was done using a cross-sectional survey design. This allowed the researchers to collect data from all participants in one point of time, thus reducing cost and time associated with conducting multiple surveys.

Approach: The research approach adopted for this study was a quantitative survey.

Sampling: The population of this study were people from Pune city who use internet/ mobile banking services. A convenience sampling technique was used to select the participants.
Data Analysis: Statistical software SPSS version 24 was used to analyse the data collected through questionnaires.

Data Collection: The survey questionnaire was administered in both online and on-paper forms. in cases where face to face interaction could not be used, the data has been collected online or through telephonic interviews.
Use of Likert Scales: The survey questionnaire included several Likert scales that allowed participants to express their opinion on a range of topics including their perception about digital security.

**Data Analysis**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | 18-30 years | 9 | 4.0 | 4.0 | 4.0 |
| | 31-40 years | 53 | 23.8 | 23.8 | 27.8 |
| | 41-50 years | 119 | 53.4 | 53.4 | 81.2 |
| | 51-60 years | 33 | 14.8 | 14.8 | 96.0 |
| | Above 60 years | 9 | 4.0 | 4.0 | 100.0 |
| | Total | 223 | 100.0 | 100.0 | |

Table no 1. Age of respondents.

From the above table the majority of the respondents (53.4%) were in the age group of 41-50 years, followed by 23.8% who were in the 31-40 years age group and 14.8% who were in the 51-60 years age group. Only 4% of the respondents belonged to both 18-30 years as well as above 60 years age group. This means that the majority of the respondents belonged to the middle age group, which could be due to many factors such as level of education and job responsibilities.

It is also interesting to note that almost half (46.2%) of the respondents were aged between 31-50 years and that only 8% of them were either below or above this age range. This could be due to the fact that many people in this age group have more disposable income and are more likely to purchase certain items, which might explain why they are over-represented in the survey.

Overall, it can be concluded that the majority of respondents were in the middle age group, which could indicate that the target market for certain products might be within this age range.  It is also noteworthy that a small number of respondents belonged to either the 18-30 years or above 60 years age group, which could suggest that these age groups may not be as interested in purchasing such items as those in the middle age group. This information can be very helpful in designing marketing strategies and targeting the right consumers.

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Male | 113 | 50.7 | 50.7 | 50.7 |
| | Female | 110 | 49.3 | 49.3 | 100.0 |
| | Total | 223 | 100.0 | 100.0 | |

Table no 2. Gender of respondents.

From the above table the majority of respondents (50.7%) were male, while 49.3% were female. This suggests that both genders are equally represented in this survey, which could indicate that certain products or services could be marketed to both males and females.

It is also noteworthy that the percentage of males was slightly higher than that of females, which could be due to many factors such as cultural norms and preferences. For example, it is possible that males are more likely to purchase certain items than females, which may explain why they have a higher representation in the survey.

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Business | 45 | 20.2 | 20.2 | 20.2 |
| | Salaried Employee | 78 | 35.0 | 35.0 | 55.2 |
| | Homemaker | 88 | 39.5 | 39.5 | 94.6 |
| | Other | 12 | 5.4 | 5.4 | 100.0 |
| | Total | 223 | 100.0 | 100.0 | |

Table no 3. Occupation of respondents.

From the above table the majority of respondents (39.5%) were homemakers, followed by 35% who were salaried employees and 20.2% who were businessmen or entrepreneurs. Only 5.4% belonged to other occupations such as students, retired persons etc.

This suggests that most people surveyed belong to traditional occupations such as salaried employees and homemakers, which could indicate that certain products or services may be more relevant to these kinds of occupations. It is also noteworthy that the percentage of businessmen or entrepreneurs in the survey was relatively low (20.2%) compared to salaried employees (35%). This could mean that there are not many people with disposable incomes in the survey, which can be a factor when it comes to marketing certain items.

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | 0-1 lakh | 12 | 5.4 | 5.4 | 5.4 |
| | 1-5 lakhs | 31 | 13.9 | 13.9 | 19.3 |
| | 5-10 lakhs | 138 | 61.9 | 61.9 | 81.2 |
| | 10-20 lakhs | 29 | 13.0 | 13.0 | 94.2 |
| | Above 20 lakhs | 13 | 5.8 | 5.8 | 100.0 |
| | Total | 223 | 100.0 | 100.0 | |

Table no 4. Income of respondents

The above table shows that most respondents (61.9%) belonged to the 5-10 lakhs per annum income group, while only 13.9% belonged to the 1-5 lakhs and 13% to 10-20 lakhs income groups. Additionally, only 5.4% and 5.8% belonged to either 0-1 or above 20 lakhs per annum income groups respectively.

This indicates that most people in the survey belonged to the middle-income group, which could mean that certain products or services may be more relevant for them as compared to those belonging to higher or lower income groups. It is also noteworthy that a small percentage of respondents belonged to either the 0-1 or above 20 lakhs per annum income groups, which could suggest that these groups may not be as interested in purchasing certain items.

| | Strongly Disagree | | Disagree | | Neutral | | Agree | | Strongly Agree | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Count | Row N % | Count | Row N % | Count | Row N % | Count | Row N % | Count | Row N % |
| 1. I understand the importance of cyber security | 8 | 3.6% | 10 | 4.5% | 12 | 5.4% | 88 | 39.5% | 105 | 47.1% |
| 2. I take necessary measures to protect my data online | 12 | 5.4% | 23 | 10.3% | 11 | 4.9% | 83 | 37.2% | 94 | 42.2% |
| 3. I am aware of the various types of cyber threats such as phishing, malware, etc. | 18 | 8.1% | 26 | 11.7% | 32 | 14.3% | 75 | 33.6% | 72 | 32.3% |
| 4. I regularly update my software programs and devices to ensure protection from cyber threats | 16 | 7.2% | 19 | 8.5% | 8 | 3.6% | 84 | 37.7% | 96 | 43.0% |
| 5. I use strong passwords for all my accounts and regularly change them | 65 | 29.1% | 25 | 11.2% | 7 | 3.1% | 66 | 29.6% | 60 | 26.9% |
| 6. I know about secure payment methods and only use them when making payments online | 21 | 9.4% | 15 | 6.7% | 6 | 2.7% | 91 | 40.8% | 90 | 40.4% |
| 7. I use two-factor authentication for all accounts that support this feature | 6 | 2.7% | 7 | 3.1% | 7 | 3.1% | 89 | 39.9% | 114 | 51.1% |
| 8. I always check if a website is verified before entering any personal information on it | 12 | 5.4% | 15 | 6.7% | 9 | 4.0% | 98 | 43.9% | 89 | 39.9% |
| 9. I use Virtual Private Networks (VPNs) whenever possible to protect my data | 84 | 37.7% | 56 | 25.1% | 23 | 10.3% | 31 | 13.9% | 29 | 13.0% |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 10. I am careful of malicious links or attachments in emails or messages and do not open them unless necessary | 21 | 9.4% | 9 | 4.0% | 10 | 4.5% | 98 | 43.9% | 85 | 38.1% |

Table no 5. Importance given to cyber security.

From the above table most of the respondents (over 40%) agreed or strongly agreed that they understand the importance of cyber security, take necessary measures to protect their data online, and are aware of various types of cyber threats. Similarly, more than half of the respondents agreed or strongly agreed that they regularly update their software programs and devices to ensure protection from cyber threats.

On the other hand, more than a quarter of respondents agreed or strongly agreed that they use strong passwords for all their accounts and regularly change them. Furthermore, a similar proportion of respondents also agreed or strongly agreed that they know about secure payment methods and only use them when making payments online. Lastly, slightly over half of the respondents agreed or strongly agreed that they use two-factor authentication for all accounts that support this feature and are careful of malicious links or attachments in emails or messages.

Overall, the survey results suggest that most respondents have taken measures to protect their data online and understand the importance of cyber security. Nevertheless, there is still scope for improvement as certain proportions of respondents still had low levels of agreement with certain questions. Therefore, it is important for organizations to ensure that their employees are adequately educated on cyber security and take necessary steps to protect their data online.

This survey was also useful in understanding the level of cyber security awareness among people belonging to different income groups. It was observed that most respondents belonging to the 0-1 income group were generally less likely to agree or strongly agree with most of the survey questions as compared to people belonging to higher income groups. This indicates that it may be beneficial for organizations to focus on targeting people in lower income groups and educating them on cyber security measures they can take to protect their data online.

Overall, this survey was useful in understanding the cyber security awareness among different groups of people and has highlighted certain areas where organizations should consider focusing their efforts for improving cyber security.  It is hoped that this survey will be helpful in guiding future initiatives related to cyber security education and creating awareness around various threats associated with online activities.

**Testing of Hypothesis**

| | Gender | N | Mean | Std. Deviation | Std. Error Mean |
|---|---|---|---|---|---|
| Average (Level of Importance given to Cyber Security) | Male | 113 | 3.8212 | .52209 | .04911 |
| | Female | 110 | 3.7382 | .60350 | .05754 |

Table no 6. Group Statistics.

| | | Levene's Test for Equality of Variances | | t-test for Equality of Means | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | F | Sig. | t | df | Sig. (2-tailed) | Mean Difference | Std. Error Difference | 95% CI | |
| | | | | | | | | | Lower | Upper |
| Average (Level of Importance given to Cyber Security) | Equal variances assumed | .923 | .338 | 1.100 | 221 | .273 | .08306 | .07551 | -.06575 | .23186 |
| | Equal variances not assumed | | | 1.098 | 214.747 | .273 | .08306 | .07565 | -.06606 | .23217 |

Table no 7. Independent Samples Test.

The above tables show that the difference in the means of both the genders are not significant. With this we can safely accept the null hypothesis that the means are equal which also means that there is no difference in perception regarding the importance of digital security between the genders.

Average (Level of Importance given to Cyber Security)

| | N | Mean | Std. Deviation | Std. Error | 95% Confidence Interval for Mean | | Minimum | Maximum |
|---|---|---|---|---|---|---|---|---|
| | | | | | Lower Bound | Upper Bound | | |
| 18-30 years | 9 | 3.6333 | .65192 | .21731 | 3.1322 | 4.1344 | 2.40 | 4.30 |
| 31-40 years | 53 | 3.6887 | .67700 | .09299 | 3.5021 | 3.8753 | 1.80 | 4.60 |
| 41-50 years | 119 | 3.7983 | .54726 | .05017 | 3.6990 | 3.8977 | 1.90 | 4.60 |
| 51-60 years | 33 | 3.8333 | .41883 | .07291 | 3.6848 | 3.9818 | 2.50 | 4.50 |
| Above 60 years | 9 | 4.0333 | .36742 | .12247 | 3.7509 | 4.3158 | 3.60 | 4.70 |
| Total | 223 | 3.7803 | .56398 | .03777 | 3.7058 | 3.8547 | 1.80 | 4.70 |

Table no 8. Descriptive.

Average (Level of Importance given to Cyber Security)

| | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|
| Between Groups | 1.347 | 4 | .337 | 1.060 | .377 |
| Within Groups | 69.266 | 218 | .318 | | |
| Total | 70.613 | 222 | | | |

Table no 9. ANOVA.

The above tables show that the p value is greater than 0.05. With this we accept the null hypothesis that there is no difference of perception regarding the importance of digital security among different age groups.

Average (Level of Importance given to Cyber Security)

| | N | Mean | Std. Deviation | Std. Error | 95% Confidence Interval for Mean | | Minimum | Maximum |
|---|---|---|---|---|---|---|---|---|
| | | | | | Lower Bound | Upper Bound | | |
| 0-1 lakh | 12 | 3.2250 | .40704 | .11750 | 2.9664 | 3.4836 | 2.50 | 3.70 |
| 1-5 lakhs | 31 | 3.5677 | .58217 | .10456 | 3.3542 | 3.7813 | 1.90 | 4.40 |
| 5-10 lakhs | 138 | 3.9870 | .42749 | .03639 | 3.9150 | 4.0589 | 2.20 | 4.70 |
| 10-20 lakhs | 29 | 3.5069 | .67238 | .12486 | 3.2511 | 3.7627 | 1.80 | 4.40 |
| Above 20 lakhs | 13 | 3.2154 | .54901 | .15227 | 2.8836 | 3.5471 | 2.30 | 4.00 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Total | 223 | 3.7803 | .56398 | .03777 | 3.7058 | 3.8547 | 1.80 | 4.70 |

Table no 10. Descriptive.

| Average (Level of Importance given to Cyber Security) | | | | | |
|---|---|---|---|---|---|
| | Sum of Squares | df | Mean Square | F | Sig. |
| Between Groups | 17.311 | 4 | 4.328 | 17.700 | .000 |
| Within Groups | 53.302 | 218 | .245 | | |
| Total | 70.613 | 222 | | | |

Table no 8. ANOVA.

The p value is less than 0.05. With this we can safely reject the null hypothesis that there is no significant difference in the level of importance regarding digital security within the income groups. For the individuals who have an income between 5-10 lakhs, the mean is 3.9 as compared to the people who have an income between 0-1 lakh (mean = 3.2).

**Conclusion**

Based on the data and analysis provided, it can be concluded that there is a significant difference in perception regarding the importance of digital security among different income groups. Individuals with higher incomes appear to rate digital security as more important than those with lower incomes. This emphasizes the need for adequate educational measures to ensure that all individuals, irrespective of their economic status, are aware of the importance of digital security and its implications. This research provides useful insights into how digital security is viewed by different sections of our society and could be used as guidance for policy makers when designing policies related to digital security. It is essential to recognize the importance of digital security to ensure that our societies remain safe and secure. Therefore, further studies should be conducted to explore the different aspects and implications of digital security in our ever-evolving digital world. This will help us build a better understanding of this important issue and provide guidance for policy makers to design effective policies that promote digital security within our society.

**References**

Biswas, A., Sharma, S., Bhattacharya, P., Singhvi, H., Deshpande, M.(2016). Understanding user's willingness to adopt security measures for online transactions: An empirical study from India. International Journal of Management Studies (IJMS), 5(1), pp. 87-104

Chauhan, R. (2021). Cyber Security in 2021: Trends, Challenges and Solutions. Retrieved from https://www.cybersecurityiq.net/blog/cyber-security-in-2021-trends--challenges--solutions

Kanade, M., Arora, R., Sharma, D., Lalwani, P. (2014). Cyber threats and cyber security awareness among Indian users. International Journal of Engineering Research & Technology, 3(2), pp. 816-820.

Kumar, S., & Dixit, N. (2015). Digital security awareness among bank employees and customers: A study of Pune city. International Journal of Research in Business Studies and Management, 2(3), 15-24.

Krishnamurthy, K., (2015). Awareness and attitude towards information security: Survey results on users in India. International Journal of Information Security Science, 4(2), pp. 72-87.

Kapoor, M. (2019). Awareness towards digital security among e-commerce users in India–A survey-based approach. International Journal of Applied Management Science and Technology, 1(2), 58-67.

Miller, K. (2021). Security awareness among middle class Indians regarding digital frauds: A survey-based approach. Global Governance Review, 1(4), 83-90

Mishra, A. (2022). Digital frauds in India: Level of security awareness among e-commerce customers. International Journal of Computer Science and Information Technology, 5(2), 39–41.

Raghu, B, S. Josephine, A.V. S .Abbamanya and A. Ananthanarayan (2014). Awareness of detecting cyber threats and knowledge sharing in educational institutions among instructional staff members in two private universities in Chennai: A survey study. International Journal of Computer Science & Information Technology (IJCSIT), 6(3), pp. 20-26

Sharma, K and O Jharna (2014). Perception of Government and Private Organizations Regarding Digital Security: A Survey Study. International Journal of Advanced Research in Computer Science and Software Engineering, 4(7), pp. 563-569

Sharma, U., Rathore R., & Singh H. (2014). Cyber security awareness amongst Indian citizens. International Journal of Business and Management, 9(4), 28-37.

Sharma, S., Mishra, P., & Gupta, V. (2014). Access control techniques for secure electronic transactions over the internet: A review. In Handbook of research on computerized systems analysis and design techniques for corporate environments (pp. 129-140).

Stephens, J., Robinson, D., & Mayes, K. (2014). Digital Security – An overview of the security risks associated with ICT systems and networks. International Journal of Electronic Security and Digital Forensics, 6(1), 5–13. doi:10.1504/IJESDF.2014.061568

Singh, R. (2021). Information sharing on cyber security among employees at Indian companies. International Journal of Cyber Security and Digital Forensics, 8(3), 123–130.

Vaishnav, M. (2018). Cyber Fraud Awareness among Teenagers in India: Need for Effective Interventions to Mitigate the Risk. International Journal of Information and Education Technology, 8(5), 462–466. doi:10.18178/ijiet.2018.8.5.923