

# Study of Cyber security Awareness with Risk Assessment Model Among College Students

Gunita Pahwa<sup>1</sup>, Abhishek<sup>2</sup>, Manya Kaur Chopra<sup>3</sup>, Tanya Handa<sup>4</sup>, Yogita Thareja<sup>5</sup>

<sup>5</sup>, Assistant Professor, Vivekananda Institute of Professional Studies-TC, New Delh

\*\*\*

**Abstract** - This is a digital campus, where we submit our work, pay utilities, chat with friends, and therefore, our lives are mostly conducted using personal devices. So when we, as students, are using them all the time, it makes me think: are they actually safe with that kind of dependency on them? The paper examines the level of awareness that students have regarding cybersecurity and its alignment with the actions they take to ensure their gadgets are secure.

We used a questionnaire in Google Forms, which we distributed the questionnaires. The poll inquired into the level of familiarity of respondents with phishing, malware, weak passwords, and social engineering, and examined daily habits such as password hygiene, software updates, multi-factor authentication, and reactions to suspicious emails. We did not think of awareness as a mere concept; we knew that it could, or may not, become a consistent action.

Based on those answers, we assembled a risk assessment model, which approximates the vulnerability of every device. The model combines the indicators of knowledge not only with actual actions but also with a composite score of security. It is not a crystal ball, but it makes one feel exposed, according to what we reported.

The thing that we discovered is that being able to use the buzzwords in the realm of cybersecurity is not enough to guarantee that we are practising safely. Measuring that gap, we have a clearer picture of the degree of safety of our devices and provide some recommendations on how colleges can reinforce their awareness procedures.

**Keywords:** Cyber security Awareness, Student Behavior, Device Security, Risk Assessment Model, Phishing and Social Engineering, Password Hygiene, Awareness–Action Gap

## 1. INTRODUCTION

College life in the digital era seems to be overwhelmed by the use of technology. We post grades and lecture notes on university servers; we are in classes on learning platforms and we communicate via emails, messaging applications and group chats. In essence, both phones and laptops are our study accessories and our personal data banks, in most cases, extensions of our personal selves.

Although that integration may be convenient, we are exposed to cyber threats.

Cyber security concerns are not an imaginary phenomenon: phished emails look like they come through an official university, there are malicious links in study-group discussions, and the Wi-Fi on campus can reveal our passwords. Malware may be contained in even harmless downloads. All it is captured in the academic papers and policy discussions, but nobody knows how to be safe without awareness alone. Awareness is sometimes believed to be a one-dimensional entity of paying attention to the risks, being aware of the consequences, and attempting to avoid them.

In practice, it isn't. There are those students, who understand that having weak passwords is dangerous, but they find themselves using them again, and there are those who install antivirus software and are not in the habit of updating their operating system. Such discrepancies lead to a question: are the measures of self-reported mindfulness levels of students consistent with their real security practices? College is an ideal place to examine this since we are all active Internet users who can manage our grades, finances, and social lives online by using the Internet, but we hardly ever apply standardized policies on using devices or have compulsory security measures.

The majority of studies on cyber security mindfulness dwell on the effectiveness of training or knowledge assessments. That is not the best way of describing the connection between what we know and what we do on a day-to-day basis. We must check

whether the person who detects a phishing signal is the person who does the follow-up as to the authenticity of the email, or is it the person who knows about two-factor authentication, who has already implemented the device. This intersection is the subject of the present research.

The information was collected by using a structured questionnaire based on Google Forms, assessing the level of knowledge of the students concerning typical cyber pitfalls and their reported protection behavior. The questionnaire included questions on learning about phishing and malware, password habits, software updates, authentication procedures and reactions to suspicious messages. We also wish that by examining the abstract cognition and habitual action, we could transcend superficial indicators of mindfulness.

There are, however, pitfalls of relying on self-reported data. The students may be either more vigilant or less exposed than they are. The reactions could be based on what they believe they need to do and not what they are doing. Although we cannot say that we are totally correct, aggregate patterns may provide useful information when used with caution.

This paper is an implementation of a threat-assessment framework based on such survey results. The model integrates knowledge clues with behavioral variables to provide estimates of device security posture as opposed to merely indicating that students are concerned or ignorant. All responses contribute to a compounded score, which indicates possible exposure to cyber risks. The qualitative understanding is coded into a systematic framework, through which it is possible to engage in relative analysis among participants.

The model is not supposed to represent all the aspects of cyber threat; it is just an abstract tool that helps to correlate mindfulness to measurable behavior. Numerous students are digitally savvy, which does not necessarily mean that they are well-informed with regard to their security. There can be a comfort level in technology and risky behavior. Constant exposure to the digital arena may also cause us to get used to some of the threats since they may no longer be easily detected. Therefore, anecdotal inferences are not as efficient as empirical evaluation.

Incidents of cybersecurity in universities may have more far-reaching consequences as well. One hacked account will provide access to the university systems, steal sensitive information or lead to the loss of money. One vulnerable device can be used to cause more damage in an interconnected network. Although we are researching a case of individual student mindfulness, the results might be used to direct institutional policies and cybersecurity programs.

It is rational and realistic to develop this threat-assessment model. Analytically, it allows us to investigate the association of knowledge and behavior. In practice, it marks the regions that require specific interventions. However, changing threats should also be met with mitigation strategies, and the model must be accordingly changed.

When outlining this study, we should be wary: the model is investigative, and it does not substitute rigorous testing of the vulnerabilities. It is not a conclusive measure but a calculated estimate which helps in explaining the association between perception and protection. Finally, the research question is as follows: to what extent, in practice, are students secure, considering what they know and what they purport to do? It is with the aim of illuminating the disparity in the awareness and on-the-job protection that we aim to explore cybersecurity mindfulness and preventative measures, and establish the linkage of these to a systematic evaluation.

## 2. PROBLEM STATEMENT

We are always on phones, laptops, and tablets studying, paying bills, and being in contact with friends. Such devices store confidential data and are commonly connected to the open Wi-Fi, which is not necessarily secure. However, we do not actually know the extent to which we actually know about cybersecurity.

The conversations frequently emphasize the fact that since we spend a lot of time on the Internet, we should be good at recognizing cyber threats. That might be overblown. Being aware of such words as phishing or the necessity to use a strong password does not mean that you will not fall into awkward links or use the same password on multiple accounts. These trends indicate that there may exist an actual disparity between what is known and what is actually followed.

A high number of university outreach efforts disseminate information and posters about cyber safety and pay minimal attention to whether students alter their behaviors. This leaves us with a few indicators that students actually understand how to defend themselves and whether they are actually in danger.

It is not just a matter of knowing whether we are conscious of the threat that is at stake, but also of how this knowledge is applied to how safe our devices are. To the extent that we have no good means to view how knowledge is transformed into action, we can only obtain a superficial rather than a profound view of the situation.

The proposed paper attempts to address this issue by exploring cybersecurity awareness among students in colleges and a basic model of risk assessment. The model relies on self-reported habits to get an estimation of how susceptible each student can be to a device

### 3. OBJECTIVES

In this study, we have a series of objectives that we wish to transcend beyond mere observations. We would like to explore further our real thinking on cybersecurity on campus. These goals are stated as follows:

To determine the extent of our knowledge of cybersecurity. We will evaluate our understanding of the most common threats on the internet, such as phishing, malware, etc.

To investigate the safety habits that we apply in our daily lives online. That includes such aspects as password management, software updates and our response to suspicious messages. These practices demonstrate how attentive we are regarding our gadgets.

To identify discrepancies between what we know and what we really do. In essence, are we as aware of the theoretical and practical activities of protection or are there discrepancies between what we know and what we are actually doing?

To create an initial risk assessment framework with the help of the survey. The model brings together what we know and what we actually do, projecting a possible level of riskiness of our devices. We are not targeting accuracy in our predictions; we just want to have a clear and structured idea of the level of security in our devices.

To contribute valuable information that can enable colleges to tighten their focus on awareness programs.

All in all, these objectives are regarding the study of cyber security awareness in a real, practical sense, namely by quantifying and relating it to our real college-life behavior.

### 4. LITERATURE REVIEW

Cyber security has become a major concern in today's digital era. Internet, smartphones, social media and online platforms are heavily used by college students for academics, communication and entertainment. Due to this, students are more vulnerable to cyber threats like phishing attacks, malware, identity theft, ransom ware, and data breaches. That is why ensuring cyber security awareness has become an important area of research.

Many previous studies have assessed cyber security awareness among college students via questionnaire-based surveys. In these studies, it has been noticed that students have basic theoretical knowledge of cyber security terms like hacking, viruses and phishing, etc. But their behavior is not that secure at a practical level. According to the research findings, students mostly use weak passwords, use the same password for multiple accounts, ignore software updates and also click on suspicious or unknown links. From this, it is clear that being aware is not enough; one must use and follow safe practices also.

Some studies have also highlighted that students from a technical background have a better awareness level than students with a non-technical background. But even students with computer-related courses do not follow secure practices in each and every situation. It clearly shows that there is a gap that exists between awareness and real-life behavior. And to measure this gap systematically, we need a structured evaluation model.

An important part of cyber security research is the development of risk assessment models. Traditional cyber security risk assessment frameworks have been designed mainly for organizations and enterprises. In these models, assets are identified, vulnerabilities are analyzed, threat likelihood is calculated, and then the overall risk level is determined.

Risk is generally divided into categories like low, medium and high risk. These models are detailed and structured but are mostly designed for the institutional level.

Recent research has focused on quantifying risks using scoring systems and weighted parameters. Risk level is calculated by considering variables like password strength, antivirus usage, software updates, phishing awareness and privacy settings. But the majority of studies apply on organizational context and focus less on the behavior of an individual college student.

In existing literature, awareness studies and risk assessment frameworks have been studied separately. Awareness studies focus on and measure the knowledge level mainly, while risk models focus on system-level analysis.

Research that combines both aspects is very limited, especially for college students. This is what we call a research gap.

That is why the present study aims to measure cyber security awareness and to integrate it with a structured risk assessment model. With this approach, risk classification can be performed on students' knowledge, along with their practical behavior. This integrated model helps educational institutions to design targeted awareness programs and to improve the digital safety level of students.

## 5. METHODOLOGY

The objective of this study is to measure cyber security awareness among college students and develop a structured risk assessment model on the basis of their online behavior. In this section, research design, data collection process, sampling method, tools used, scoring model and data analysis are explained.

### 1. Research design

This study is based on a quantitative research design. A questionnaire-based survey is adopted for data collection. Quantitative approach was chosen because we had to collect numerical data, perform statistical analysis, and classify students into risk categories.

The research nature is cross-sectional, as the data were collected over a specific time period, and no long-term tracking was done.

### 2. Population and sampling

The target population of this study is college students who use the internet, smartphones, laptops and online platforms on a regular basis. Participants can be from different academic streams, including technical and non-technical backgrounds. The convenience sampling technique is used as a sampling method. The link to the Google Form is circulated among WhatsApp groups, college groups and academic networks. Students have voluntarily filled out the survey.

### 3. Data Collection Tool

A structured questionnaire is designed for primary data collection. The questionnaire was created on Google Forms, and mainly closed-ended questions were included in that.

The questionnaire was divided mainly into 2 sections.

**Section A:** Basic information, like age group.

**Section B:** Cyber security practices and behavior.

Real-life practices are measured in this section.

If they use the same password for multiple accounts

If they regularly update software.

If they verify suspicious links.

Have they installed an antivirus?

This section is most important for the risk assessment model.

#### **4. Risk Assessment model development**

The major contribution of this research is to develop a simplified risk assessment model which is specifically designed for college students.

##### **Step 1: Scoring Mechanism**

A numerical score is assigned to each awareness and behavior-based question.

Secure practice/ correct awareness = 2 points.

Moderate practice = 1 point

Risky practice/ Lack of awareness = 0 points.

The total score of each participant is calculated from this scoring system.

##### **Step 2: Total score calculation**

The total cyber security score is calculated by adding scores of all relevant questions.

Example:

Maximum possible score = 20

Individual participant score = 14

##### **Step 3: Risk Classification**

Students are divided into 3 categories based on their total score

Low risk-High awareness+ secure practices.

Medium risk- Moderate awareness+ Inconsistent practices

High risk- Low awareness + risky online behavior

Score ranges are also divided proportionally (for example):

---

0-7->		High		Risk
8-14	->		Medium	Risk
15-20 -> Low risk				

This classification model is simple and practical, which converts awareness into a measurable risk level.

## 5. Data Analysis Techniques

Collected responses are exported from Google Forms and then analyzed in Excel. Incomplete responses were removed in the data cleaning process.

The following analysis techniques were used:

### 1. Descriptive Statistics

Total number of respondents

Percentage distribution

Mean awareness score

Risk category percentage

### 2. Frequency Analysis

Response percentage is calculated for each question to identify common patterns.

### 3. Risk Distribution Analysis

Overall distribution is evaluated after classifying students into low, medium, and high risk groups.

Charts and graphs(bar graph, pie graph) were used to visually represent results.

## 6. Ethical Considerations

Ethical guidelines were followed in research:

Volunteer participation.

Personal identity was not mandatory.

Email collection was kept an any missed.

Data is strictly used for academic purposes.

Privacy and confidentiality of respondents were maintained

## 7. Reliability and validity

Previously published awareness-based studies were referred to while designing the questionnaire. Questions were designed in simple and clear language to avoid ambiguity.

The risk assessment model is based on a logically structured scoring mechanism which considers both awareness and behavior. This integrated approach strengthened the construct validity of the study.

## 8. Limitations of Methodology

Convenience sampling was used, so the results may not fully represent the entire population.

Response bias is possible because of self-reported data.

The study is based on a limited sample size.

Still, this methodology provides an effective framework to measure student-level cyber security awareness and behavioral risk.

## 6. IMPLEMENTATION AND WORKING

In this segment, we will understand how the proposed cyber security awareness survey and risk assessment model were practically implemented and also how we traced the working process of the same.

### 1. Questionnaire Implementation

The research implementation process started with preparing and designing the questionnaire and deploying it over various online platforms. We developed the questionnaire using Google Forms because it was user-friendly, free and also offered automatic data collection. The following steps were used to develop the form:

- There was a clear title and description.
- There was a consent statement that explicitly said that the participant's involvement was voluntary.
- Entering emails was optional to confirm anonymity.
- Questions were divided into a logical order – the first group was that of demographics, then the questions related to awareness and the last group included behavior-related questions.

We previewed the form to make sure that there were no technical errors and all the options were visible.

### 2. Survey Distribution Process

The survey was distributed by circulating the survey link with the finalised questionnaire through:

- College WhatsApp groups
- Academic discussion groups
- Personal academic contacts

The respondents were informed that the survey was part of an academic research field and that it would not take more than 2-3 minutes to complete.

The data collection process was left open during a given period of time (3-4 days). We stopped the responses at this time period in order to commence the analysis process.

### 3. Data Collection and Cleaning

After the completion of the survey responses, we exported the Google Forms responses in an Excel format (.csv file). The steps involved in the data cleaning process were as follows:

- Eliminating unfinished answers.
- Checked for duplicate entries.

We used the final cleaned dataset in the analysis.

#### 4. Implementation of Scoring System

The scoring mechanism was the main component of the risk assessment model. At this stage, each response was given a numerical value.

##### Step 1: Determining Scoring Criteria

A scoring pattern was established based on every awareness and behavior-based question:

- Secure behavior – 2 marks
- Moderate behavior – 1 mark
- Risky behavior – 0 marks

The scoring rule was properly outlined on each question.

For example: "Do you use strong passwords?"

- Yes: 2

- Sometimes: 1

- No: 0

##### Step 2: Scoring Responses

- All the responses were allocated different numerical values in the Excel sheet.
- And each question was provided with a separate column.

##### Step 3: Validate Scoring Consistency

- We made sure that all the responses were appropriately scored.
- Random entries were confirmed to prevent errors in any calculation.

#### 5. Total Score Calculation

To determine the overall cybersecurity score of each participant:

- Scores of all questions related to awareness and behavior were summed up.
- A new column named 'Total Score' was added.
- We then applied the Excel formula (=SUM), which automatically summed the total.

For example, when summative potential is 20 and a student has a score of 12, his/her level of awareness and behaviour would be 'moderate'.

## 6. Process of Risk Categorization

The total score of the students was used to divide them into categories. The range of scores was logically split into:

- 0-7: High risk
- 8-14: Medium risk
- 15-20: Low risk

Risk classification was done automatically in the Excel spreadsheet using the IF formula.

Through this procedure, the level of risk was automatically identified for each participant.

## 7. Statistical Implementation

The data was analyzed using descriptive statistical tools.

### (A) Frequency Distribution

The following was calculated in relation to each question:

- The percentage of students who use strong passwords.
- Proportion of students with 2FA enabled.
- Proportion of students who were able to recognize phishing emails.

This assisted in determining behavioral patterns.

### (B) Percentage Analysis

The total percentage of risk categories was summed up:

- % of students with Low Risk
- % of students with Medium Risk
- % of students with High Risk

This description symbolized the general cyber security position.

### (C) Mean Score Calculation

To calculate the level of awareness in general:

- The average score (Mean) of all participants was computed.
- This score assisted in knowing the level of cyber security of an average student.

The same was calculated by using the AVERAGE formula in Excel.

## 8. Graphical Representation

To visually illustrate the findings:

- Awareness questions were covered through bar charts.
- The distribution of risks was illustrated with the help of pie charts.

- Comparison was done using column charts.

These graphical representations made the findings more understandable and clear.

## 9. Model Working Summary

The process of the proposed Risk Assessment Model is rather simple and structured.

1. The questionnaire was filled out by the students.
2. All the responses were then automatically transformed into a numerical score.
3. The total score was calculated.
4. This score is then used to determine the risk category.
5. The general distribution is examined.

This is done to transform the model awareness into an outcome of risk that can be measured.

Conventional organizational paradigms are usually complicated, whereas this is a student-oriented model that is very easy and viable to apply.

## 10. Practical Application of the Model

This model can be very useful in learning establishments:

- Identifying high-risk students.
- Developing awareness programs.
- Organize cybersecurity training.
- Enhancing online security measures.

This model can be transformed into an automatic web-based application, which would allow students to find out their risk level by filling out the survey and immediately receiving their results in the future.

### 11. Limitations in Implementation

- The model relies on self-reported information.
- Sample size can be limited.
- Risk classification is not an enterprise model, but a simplified form of it.

This undergraduate-level cybersecurity test is quite practical and offers a flexible model to apply to it.

## 7. RESULTS AND ANALYSIS

The main purpose of this research study was to estimate the level of cybersecurity awareness among college students and create a systematized risk evaluation model, which was built on the basis of these results. Eighty-six students took part in the survey. The systematized analysis of the obtained responses was performed using descriptive statistics and categorical risk classification.

### 1. Demographic Response Overview

The study collected 86 valid responses. All the responses were assessed based on the scoring model after data cleaning. The highest possible score was 24, which was the general cyber security awareness.

### 2. Password Security Practices

The most basic aspect of cyber security is password usage behavior. Based on the results of the survey:

- 72 students (around 84%) stated that they Always use strong passwords.
- 12 students (around 14%) said that they Sometimes use strong passwords.
- The number of students who acknowledged that they do not use strong passwords was 2 (approximately 2%).

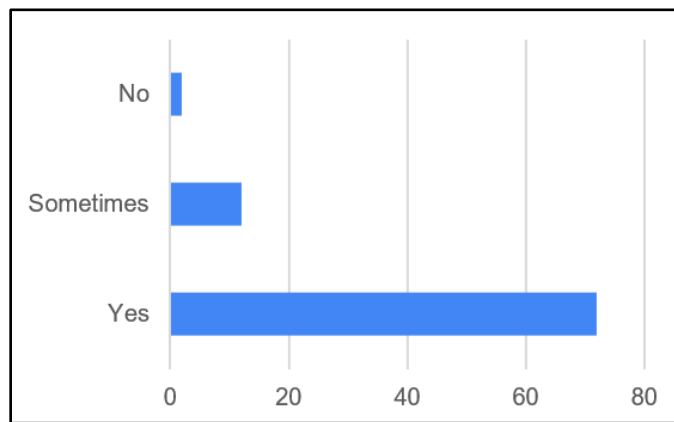


Chart -1: Password Security Responses

Analytical Interpretation: This data makes it obvious that most students know about the importance of password security and apply it. The 84% direct response of Yes is a positive signal. Nevertheless, the 16% (Sometimes + No) category can also be a possible weakness, particularly in case the passwords are predictable or duplicated.

On the whole, the hygiene of students with regard to passwords is satisfactory

### 3. Two-Factor Authentication (2FA) Adoption

Two-factor authentication provides an added level of security and reduces the risk of unauthorized access. Based on the results of the survey:

- 46 students (about 53%) mentioned that they enable 2FA Always.
- 35 students (approximately 41%) said they Sometimes use 2FA.
- 5 students (around 6%) said that they Never use 2FA.

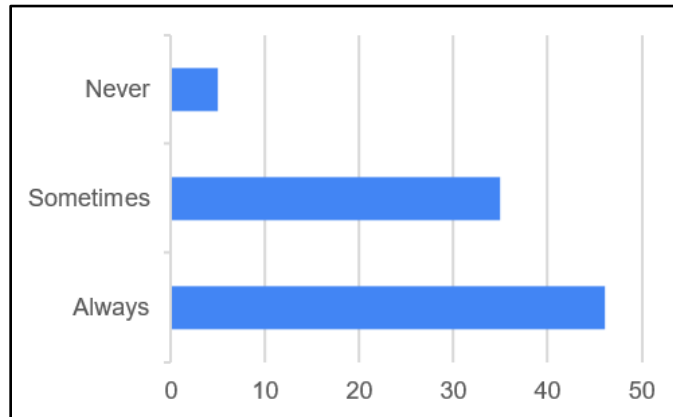


Chart -2: Two-Factor Authentication Responses

Analytical Interpretation: 2FA is used consistently by more than half of the students, but 41% of the Sometimes respondents mean that there is no consistency. Cyber security represents a situation whose mere implementation makes it a vulnerability. The rate of 6% non-adoption is relatively low, yet the long-term outlook of digital safety is alarming.

This information indicates that consciousness exists, and it is meaningful to enhance behavioral consistency.

#### 4. Use of Antivirus or Security Software

Antivirus software is used to offer system-level security against malware, ransom ware and spyware attacks. Survey results show:

- There were 49 students (around 57%) who replied in the affirmative.
- Whereas, 37 students (approximately 43%) answered No.

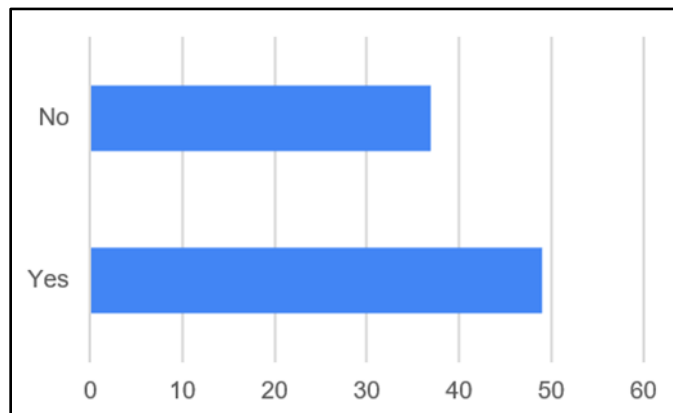


Chart -3: Antivirus Software Usage Responses

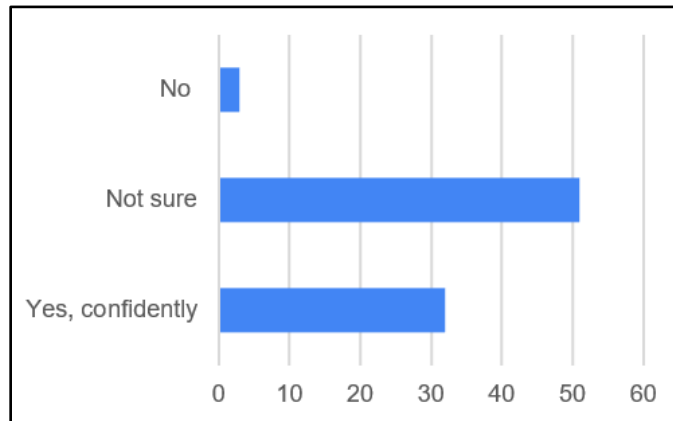
Analytical Interpretation: This demonstrates that over half of the students take care of the device-level protection. The 43% who did not use antivirus however, illustrate huge security lapses. Antivirus protection is strongly advised in a learning institution because of the prevalence of public wi-fi and file sharing.

It means that the level of implementation of technical protective measures is not universal and is moderate.

### 5. Phishing Awareness Threat Identification

The process of Phishing detection is a very important indicator of practical cyber security awareness. The survey responses show:

- There were 32 students (roughly 37%) who claimed they would be able to establish a fake site with confidence.
- 51 out of 100 students (around 59%) were also not certain whether they can recognize any fraudulent sites.
- No was answered by 3 students (approximately 4%).



**Chart -4:** Phishing Awareness Responses

Analytical Interpretation: This finding means that most of the students (59%) are unable to spot phishing attacks. The detection ability of only 37% of the students is confident. This makes it clear that, despite the fact that after performing the simple cybersecurity measures, there is a low level of advanced threat recognition. Phishing enlightenment should also be enhanced in order to ensure that students are more safeguarded against real-life cyber threats.

### 6. Overall Score Distribution

The responses of the participants were rated. The maximum score was 24. The ranges of scores were categorized into 4 groups:

**Table -1:** Overall Score Distribution

Score Range	Number of Students
0-6	0
7-12	11
13-18	54
19-24	21

**Analytical Interpretation:**

- None of the students has an extremely low awareness (0-6) level, which is a good sign.
- The percentage of students in the lower awareness bracket (7-12) was 11 (13%).
- Most of the students, i.e. 54(63%), belong to the moderate awareness (13-18) group.
- The number of students who are under the high awareness (19-24) is only 21 (24%).

The general level of awareness of the students is average, except that high-level cybersecurity is confined to a small percentage. The moderate level of awareness cannot be considered adequate for long-term digital safety.

**7. Risk Assessment Model Classification**

With the risk assessment model that we created, students were categorized into 3 groups:

**Table -2:** Risk Assessment Classification

Risk Level	Number of Students	Percentage of Students
High Risk	2	2.33
Medium Risk	45	52.33
Low Risk	39	45.35

Analytical Interpretation: The findings of the risk model are as follows:

- There is a low-risk population (2.33%), which is an encouraging factor.
- Most of the students (52.33%) are placed under the Medium Risk category.
- The category of Low Risk comprised 45.35%, which was fairly satisfactory.

A high percentage of medium risk is an indication that, despite the simple security measures taken by the students, their actions are not completely safe.

**8. Correlation Between Awareness and Risk**

Based on the analysis, it can be clearly said that the higher awareness score is directly related to the risk of being less risky. The students whose scores were either 19-24 were predominantly in the low-risk group. On the same note, the students with low scores were grouped under the medium or high-risk category.

This indicates that a well-modelled scoring model is useful in predicting the risk. It could be used practically in learning institutions in terms of cybersecurity surveillance.

Findings indicate clearly that theoretical knowledge does not aid students in maintaining the security of their devices, and there is a need for life-structured cybersecurity awareness programs and training to be undertaken.

### 8. CONCLUSION

The primary objective of this research study was to evaluate cyber security awareness amongst college students and to classify the risk level using a structured risk assessment model. A survey-based analysis revealed that students possess basic cyber security awareness, but there are noticeable gaps in practical implementation and advanced threat recognition.

The password security results indicate that the majority of students create strong passwords, which is a positive behavioral indicator. Students have a solid grasp of the fundamental concepts of digital hygiene. However, the inconsistent behavior of some students suggests that there are gaps in awareness and consistent practice. The two-factor authentication (2FA) adoption results show a mixed pattern. Although more than half of the students regularly enable 2FA, a significant percentage either use it occasionally or do not use it at all. In the context of cyber security, partial implementation can create vulnerabilities, which is why improving behavioral consistency in the adoption of 2FA is necessary.

The usage of antivirus or security software indicates a moderate level of adoption. Slightly more than half of the participants maintain device-level protection; however, a considerable percentage of students' devices remain potentially unprotected. Frequent internet usage, public Wi-Fi access, and file sharing are common in academic environments, increasing the importance of protecting devices.

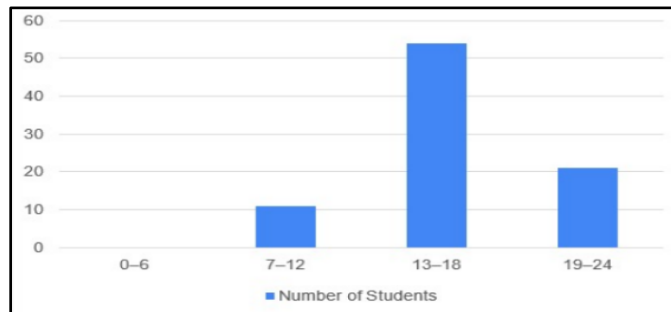


Chart -5: Score Distribution

The most critical finding is related to phishing awareness. The majority of students cannot confidently identify phishing attacks. This result highlights that possessing only theoretical awareness is not enough if real-world threat detection skills are weak. In today's digital ecosystem, phishing is the most common cyber -attack method, especially for targeting students. Therefore, there is a strong requirement for focused awareness programs and practical training sessions.

Score distribution analysis shows that the majority of students fall into the moderate level awareness category, whereas the high awareness level category is limited to a comparatively smaller group. Through the risk assessment model, it has been concluded that most students are classified in the medium-risk zone. This situation is neither alarming nor satisfactory. It indicates that students are not completely vulnerable but are not completely secure either.

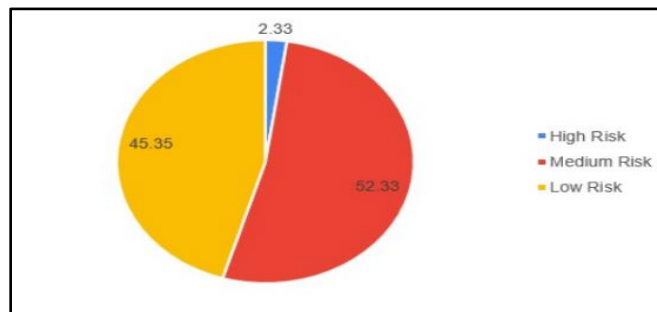


Chart -6: Risk Assessment Model Classification

Overall, this study concludes that foundational cybersecurity knowledge is present amongst college students; however, there is an urgent need to strengthen advanced security practices and threat identification skills. Educational institutions should conduct structured cybersecurity awareness programs, workshops, and curriculum-level integration to reduce students' risk levels systematically.

This research clearly demonstrates that awareness alone is not sufficient; consistent implementation and practical exposure are equally important. If targeted training and institutional support are provided, then the medium-risk population can be shifted into the low-risk category, which is essential for long-term digital safety and a secure academic ecosystem.

## 9. FUTURE SCOPE

The findings of this research study reveal that while college students possess a moderate level of cybersecurity awareness, noticeable gaps between their knowledge and practical application still exist. Given these gaps, the future scope is extensive, with the potential to expand this topic into multiple dimensions.

One primary area for future research is the conduct of longitudinal studies. The present research is based on a cross-sectional design, wherein data is collected within a specific time period. In future research, students can be observed for a longer timeframe, typically one to two years, to determine if awareness programs, workshops, or institutional policies have a lasting impact. This will also allow accurate measurement of behavioural changes and risk reduction.

Another important area for future research is intervention-based research. While this study focused on evaluating awareness level and risk assessment model, structured cybersecurity training modules can be provided to students using an experimental design in the future. By providing this training and comparing pre-test and post-test results, researchers can measure actual improvement. This would help identify the most effective training method for students.

A third direction for expansion involves comparative research across diverse groups such as postgraduate students, working professionals, or faculty members, rather than limiting the study to undergraduates. Moreover, a comparison between private and government institutions could reveal how different environments influence student awareness and risk levels.

Although the present risk assessment model is mainly dependent on a questionnaire-based scoring system, it can definitely be enhanced in the future. Features like weighted scoring technique, machine learning algorithms, or predictive analytics can also be integrated into the model. For instance, developing an artificial intelligence-based model can be used not only to predict future vulnerabilities based on students' behavioural patterns but also to help institutions design proactive cybersecurity strategies.

Future research could also explore the behavioural and psychological aspects of cybersecurity awareness. In many cases, students possess basic awareness, yet they do not follow safe practices. This could be due to many factors, such as prioritising convenience, a lack of perceiving threats, or being too overconfident in their digital skills. Henceforth, behavioural frameworks like risk perception theory or technology acceptance models could be used in future studies to comprehend the gap between actual behaviour and awareness.

Moreover, integrating cybersecurity awareness in the academic curriculum can also be a part of future research. Future studies could also help evaluate how cybersecurity education improves students' awareness level and practical security behaviour. Additionally, research-emerging cyber threats like AI-generated phishing emails, deepfake scams, and advanced social engineering attacks can be used to assess the students' preparedness.

Overall, the future scope of this research goes beyond simply measuring cybersecurity awareness amongst students. This study provides multiple opportunities for future research, including behavioural analysis, advanced risk assessment models, curriculum-based cybersecurity education, and an emerging understanding of cyber threats. A safer and more resilient digital academic environment can be created through continuous research and institutional support.

**REFERENCES**

- [1] S. Furnell and K. Clarke, "Power to the people? The evolving recognition of human aspects of security," *Computers & Security*, vol. 31, no. 8, pp. 983–988, Nov. 2012, doi:10.1016/j.cose.2012.08.004.
- [2] A. Moallem, N. B. N. Bakar, and S. Sadiq, "The importance of cybersecurity awareness among students," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 9, pp. 1–7, 2019.
- [3] M. Al-Janabi and I. Al-Shourbaji, "A study of cyber security awareness in educational environment in the Middle East," *Journal of Information & Knowledge Management*, vol. 15, no. 1, 2016.
- [4] J. Kumar and P. Kumar, "Cybersecurity awareness among college students: A survey analysis," *International Journal of Computer Applications*, vol. 182, no. 44, pp. 10–15, 2019.
- [5] A. Alharbi, "Users' awareness of cybersecurity threats and practices," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 4, pp. 1–6, 2020.
- [6] P. van Schaik, D. Jeske, J. Onibokun, L. Coventry, J. Jansen, and P. Kusev, "Risk perceptions of cyber-security and precautionary behaviour," *ScienceDirect*, vol. 75, pp. 547–559, Oct. 2017. [Online].