Enhancing Cyber Awarenesse: The Role of Higher Education Institutions in Building a Digitally Secure Generation

Ms. Rahi Deuri

Guest Faculty, Education, Gogamukh college

Abstract

The increasing reliance on digital platforms has heightened cybersecurity concerns, particularly in higher education institutions where students frequently engage in online activities. This study investigates the role of higher education institutions in enhancing cyber awareness and fostering a digitally secure generation. Using a descriptive research method, data were collected from 300 graduate-level students, faculty members, IT staff, and administrators across seven colleges in Dhemaji District. The findings reveal that while some institutions offer cybersecurity education, a significant portion lacks structured programs, leaving students vulnerable to cyber threats such as phishing, hacking, and identity theft. Additionally, many students demonstrate poor cybersecurity practices, such as password sharing and weak authentication measures. The study highlights institutional challenges, including limited curriculum integration, insufficient resources, and inadequate cybersecurity policies. Based on these insights, recommendations include integrating cybersecurity courses into curricula, conducting awareness programs, strengthening institutional policies, and improving cybersecurity infrastructure. These initiatives will contribute to developing a cyber-aware student community and ensuring a more secure academic environment.

Keywords: Cybersecurity awareness, higher education institutions, cyber threats, digital security, student engagement, cybercrime prevention, cybersecurity education, online safety.

1. Introduction

We live in a world where the internet is an essential component of our daily life. We grow accustomed to using the internet because it provides us joy and enjoyment, but it can also be a nightmare at times. Everyone is increasingly reliant on the internet world, which increases the potential of various issues. One of the major issue of the use of technology and internet is Cyber Crime. Cyber Crime is a common phenomenon in the world. Cyber Crime is that group of activities made by the people by creating disturbance in network, stealing others important and private data, documents, hack bank details and accounts and transferring money to their own (Goni Osman, 2022).Due to these rapidly emerging technologies, many organizations are unable to protect their private information and resources in an absolute & effective manner hence facilitating cybercrimes day by day (Harold & Micki, 2003).

As the digital world expands, cybersecurity threats have become a growing concern, particularly in higher education institutions where students actively engage in online activities. Despite the increasing risks of phishing, hacking, and identity theft, many students lack formal cybersecurity education and awareness.

Without proper knowledge, they may unknowingly engage in unsafe online practices, putting their personal and institutional data at risk.

This study aims to assess the current state of cybersecurity education in colleges, explore students' awareness and perceptions of cyber threats, and propose strategies to enhance cybersecurity education and awareness on campuses. The research focuses on seven colleges in Dhemaji District, using a descriptive research method to collect primary data from 300 graduate students, faculty, IT staff, and administrators. By analyzing the existing cybersecurity landscape, this study will identify gaps in institutional efforts and recommend practical solutions such as integrating cybersecurity into the curriculum, organizing awareness programs, and promoting safe online practices. Strengthening cybersecurity education will help build a digitally secure generation and create a safer academic environment.

2. Literature Review

Although limited research directly focuses on the role of higher education institutions in building a digitally secure generation, various studies explore cybersecurity strategies, student awareness, cyber threats, and institutional challenges. The following thematic review presents key findings from related literature.

2.1 Cybersecurity Frameworks and Institutional Strategies

Higher education institutions must adopt standardized cybersecurity frameworks to ensure a secure digital environment. Arina (2021) emphasized the need for a cybersecurity framework supporting ISO 27001 certification, which would provide international credibility in protecting institutional data. Similarly, Maranga et al. (2019) highlighted the prevalence of computer viruses, hacking, and phishing attacks in public institutions, emphasizing the necessity of structured security policies and preventive measures. These studies indicate that higher education institutions must implement standardized cybersecurity protocols to mitigate risks effectively.

2.2 Cybersecurity Awareness and Student Engagement

Student awareness and engagement in cybersecurity practices remain critical concerns. Rajashri et al. (2022) found that students often engage in risky online behaviors, such as sharing passwords and accessing unknown websites, due to a lack of cybersecurity awareness. This aligns with the findings of Berkle Elen et al. (2017), which revealed gender disparities in cybersecurity knowledge among IT students, with women showing lower interest in technology compared to men, particularly in Asian countries. These studies highlight the need for targeted awareness campaigns and training programs to enhance cybersecurity knowledge among students of all backgrounds.

2.3 Emerging Cyber Threats and Their Impact

Cyber threats are evolving rapidly, posing risks to individuals, institutions, and businesses. Jain Neelesh et al. (2014) categorized cybercrimes into malicious codes, denial-of-service attacks, cyberstalking, financial crimes, online gambling, cyber defamation, and more, demonstrating the increasing complexity of cyber threats. Additionally, Li Yuchong et al. (2021) emphasized that cyber threats are not limited to governments but also affect individuals and businesses, with vulnerabilities being sporadic, multidimensional, and capable of causing severe damage. These findings highlight the urgency for higher education institutions to integrate cybersecurity education into their curriculum and prepare students for real-world cyber challenges.

2.4 Challenges in Cybersecurity Education in Higher Institutions

The lack of structured cybersecurity education remains a significant barrier. Berkle Elen et al. (2017) identified disparities in cybersecurity knowledge based on gender and national culture, indicating the need for more inclusive educational programs. Rajashri et al. (2022) further demonstrated that many students are unaware of how to protect their digital identities, despite regular internet usage. These findings suggest that higher education institutions need to develop more inclusive and practical cybersecurity training programs to bridge knowledge gaps and promote safe online practices.

3. Significance of the Research

In today's digital age, cyber threats are becoming increasingly sophisticated, making cybersecurity awareness a crucial aspect of education. Higher education institutions serve as hubs for knowledge dissemination and technological advancement, yet many lack structured programs to educate students about online security. This study is significant as it examines the role of colleges in fostering cybersecurity awareness and creating a digitally secure student community.

With students frequently engaging in online activities such as social media, e-learning, and digital transactions, they are at high risk of cyber threats. The absence of formal training leaves them vulnerable to hacking, identity theft, phishing scams, and data breaches. By assessing students' current level of cybersecurity awareness, this research highlights gaps in knowledge and institutional efforts, providing insights into areas that require improvement.

Furthermore, this study is valuable for educational policymakers, administrators, and faculty as it offers practical recommendations for integrating cybersecurity education into academic curricula and campus activities. Institutions can use the findings to develop training programs, workshops, and policies that enhance students' ability to recognize and mitigate cyber risks.

Beyond academia, the study contributes to broader efforts in building a cyber-resilient society. As graduates enter the workforce, their cybersecurity awareness will influence organizational security and data protection strategies. By strengthening cybersecurity education at the college level, institutions play a pivotal role in preparing future professionals who are equipped to handle digital challenges responsibly.

Ultimately, this research bridges a critical knowledge gap, providing data-driven strategies to help higher education institutions take a proactive approach toward cybersecurity. The findings will not only enhance student safety but also contribute to a more secure and informed digital ecosystem.

4.Objectives of the study:

The objectives are -

a. To assess the current state of cyber security education in higher education institution
b. To explore students' attitudes and perceptions regarding cyber security threats and online safety.
c. To propose strategies for enhancing cyber security education and awareness on campuses.

5. Methodology

This section outlines the research methodology adopted for the study,
including the research design, population, sampling techniques, data collection methods, and data analysis procedures.

5.1 Research Design

The study employs a descriptive research design to analyze the role of
higher education institutions in enhancing cyber awareness and promoting digital security among students. The descriptive method was chosen as it allows for a systematic investigation of current cybersecurity ed-

ucation, students' perceptions, and institutional strategies.

5.2 Population of the Study

The population of this study consists of graduate-level students from various colleges in Dhemaji District. Additionally, college administrators, faculty members, and IT staff were considered for qualitative insights into cybersecurity initiatives.

5.3 Sample and Sampling Technique

Selection of Colleges:

The study includes seven colleges from Lakhimpur District, selected through a random sampling technique to ensure representation across different institutions.

Selection of Students:

Stratified random sampling was used to select students from different departments in the chosen colleges.

Total sample size: 300 students (approximately 43 students per college).

10 students were selected from each department within the colleges to maintain diversity in responses.

Selection of Administrators, Faculty, and IT Staff:

10 faculty members, 7 IT staff members, and 7 administrators were interviewed across the selected colleges.

These respondents were chosen through purposive sampling, as they possess direct knowledge of cybersecurity policies and education in their institutions.

5.4 Source of Data Collection

The study relies entirely on primary data, collected directly from students, faculty, IT staff, and administrators of the selected colleges. No secondary sources were used in data collection.

5.5 Data Collection Methods

1. Survey Method (For Students)

A structured questionnaire was designed to assess students' cybersecurity awareness, perceptions, and online safety practices.

The questionnaire included:

Closed-ended questions (Yes/No, Multiple Choice, Likert Scale)

Open-ended questions (to gather qualitative insights)

2. Interviews (For Faculty, IT Staff, and Administrators)

Semi-structured interviews were conducted to understand the role of institutions in cybersecurity awareness and digital security policies.

5.6 Validity and Reliability of Data

The research tools were developed based on existing frameworks and expert recommendations to ensure content validity. Although formal pilot testing and reliability measures such as Cronbach's Alpha were not conducted in this study, care was taken to align the instruments with standardized methods used in prior research. Feedback from education specialists was sought to refine the questionnaire and interview guides. Future research should incorporate pilot studies and statistical reliability tests to further validate the research instruments

5.7 Data Analysis Tools and Techniques

Quantitative Data Analysis

Descriptive statistics (percentages, frequencies, mean, and standard deviation) were used to analyze students' survey responses.

The data were presented in tables, bar charts, and pie charts to facilitate clear interpretation.

Qualitative Data Analysis

The responses from interviews were analyzed using the thematic analysis method to identify key patterns, opinions, and suggestions regarding cybersecurity education in higher institutions.

Thematic categorization was used to highlight common issues, trends, and proposed solutions.

6. Data Analysis and Interpretation

This section presents the analysis of data collected from 300 graduate students, 10 faculty members, 7 IT staff, and 7 administrators from seven colleges in Lakhimpur District. The data was analyzed based on the study's objectives, using descriptive statistical tools such as tables, percentages.

6.1 Assessment of the Current State of Cybersecurity Education in Higher Education Institutions

To assess the extent of cybersecurity education in colleges, students and faculty were surveyed regarding the presence of cybersecurity courses, workshops, and awareness programs.

Table 1: Availability of Cybersecurity Education in Colleges

Category	Number of colleges	Percentage
College with cyber security courses	3	42.86%
College without cyber security courses	4	57.14%

Interpretation:

42.86% of colleges (3 out of 7) have cybersecurity courses, meaning these institutions offer structured cybersecurity education to students.

57.14% of colleges (4 out of 7) do not have cybersecurity courses, indicating that the majority of institutions in the study lack formal cybersecurity training programs.

This data suggests a gap in cybersecurity education, which could leave many students unaware of digital security risks and best practices.

6.2 Students' Attitudes and Perceptions Regarding Cybersecurity Threats and Online Safety

Table 2 : Students Cyber Security Awareness and Online Safety Practices

Cyber security awareness & practices	Percentage
Awareness of phising and online scams	52%
Regularly change passwords	30%
Use two factor authentication	25%
Share password to others	60%
Use the same password for multiple accounts	65%

Interpretation:

Only 52% of students are aware of phishing and online scams, suggesting a lack of formal education on cyber threats.

30% regularly change passwords, and only 25% use two-factor authentication, indicating weak security practices.

60% admit to sharing passwords, and 65% use the same password for multiple accounts, showing high vulnerability to cyber risks.

Table 3 : Students' Awareness and Preventive Practices Related to Cybersecurity

College	High Awareness (%)	Moderate Awareness (%)	Low Awareness (%)	Practicing preventive measure
College A	25%	45%	30%	50%
College B	20%	40%	40%	42%
College C	18%	38%	44%	40%
College D	30%	50%	20%	60%
College E	22%	43%	35%	48%
College F	15%	35%	50%	38%
College G	17%	37%	46%	39%

Interpretation:

College D has the highest awareness and best cybersecurity practices, while College F has the lowest awareness and preventive actions.

Overall, a significant number of students remain unaware of cyber threats, and less than 50% actively implement cybersecurity measures.

There is a need for targeted cybersecurity training to improve student awareness and safe online practices.

6.3 Strategies for Enhancing Cybersecurity Awareness on Campuses

Table 4 : Preferred Methods for Cybersecurity Training

Training Method	Percentage of preference students
Workshops	40%
Subject course	30%
Awareness campaign	20%
Others	10%

Interpretation

40% of students prefer workshops, indicating that hands-on, interactive learning experiences are the most effective way to engage students in cybersecurity training.

30% favor cybersecurity as a subject course, suggesting that a structured, curriculum-based approach is also valued for in-depth learning.

20% prefer awareness campaigns, showing that some students respond well to general informational sessions and initiatives.

10% selected other methods, which may include self-learning through online resources, peer discussions, or expert talks.

6.4 Thematic Analysis of Qualitative Data

The qualitative data from faculty, IT staff, and administrators were analyzed using thematic analysis. Three key themes emerged:

1. **Institutional Challenges in Cybersecurity Education**

- Administrators highlighted the **lack of structured cybersecurity courses** due to limited curriculum integration.
- IT staff reported **insufficient resources and funding** for advanced cybersecurity infrastructure and training programs.

2. **Student Awareness and Behavioral Gaps**

- Faculty members noted that students **lack proactive security habits**, often neglecting strong password practices and two-factor authentication.
- IT staff observed that **social media and online gaming habits** make students more vulnerable to cyber threats.

3. **Need for Structured Cybersecurity Training**

- Respondents emphasized that **workshops, hands-on training, and awareness campaigns** are essential for improving cybersecurity knowledge.
- Administrators suggested the **integration of cybersecurity modules into existing courses** for long-term impact.

7. Discussion

The study highlights critical gaps in cybersecurity education within higher education institutions. While 42.86% of colleges offer cybersecurity courses, the majority (57.14%) lack formal training programs, leaving students vulnerable to cyber threats.

Student Awareness and Practices

Findings show low cybersecurity awareness and weak security habits among students.

Only 52% recognize phishing scams, and a concerning 60% share passwords, increasing their risk of cyberattacks. These results align with prior studies emphasizing the need for structured cybersecurity education.

Institutional Challenges and Training Needs

Qualitative insights reveal inadequate curriculum integration, limited funding, and insufficient cybersecurity infrastructure as major institutional challenges. Faculty and IT staff emphasize the need for interactive training methods such as workshops (preferred by 40% of students) and subject-based courses (30%).

Need for Policy-Level Interventions

The findings suggest that higher education institutions must prioritize cybersecurity education, implement structured training programs, and enhance institutional policies to ensure a digitally secure academic environment. Collaborative efforts between faculty, IT departments, and administrators are essential to improving student awareness and digital security practices.

8. Conclusion and Key Recommendations

The study highlights significant gaps in cybersecurity awareness among students in higher education institutions, with many lacking formal training and engaging in unsafe online practices. While some colleges offer cybersecurity courses, the majority do not, leaving students vulnerable to cyber threats such as phishing, data breaches, and identity theft. Institutional challenges, including **limited curriculum integration, insufficient resources, and weak cybersecurity policies,** further hinder the development of a cyber-aware academic community.

To address these issues, the study recommends the following key strategies:

1. **Integrating Cybersecurity into the Curriculum** – Introduce mandatory cybersecurity courses and incorporate basic cyber hygiene training across disciplines.
2. **Organizing Awareness Programs** – Conduct workshops, interactive training sessions, and peer-led initiatives to enhance student engagement.
3. **Strengthening Institutional Policies** – Implement strict data protection policies, access control measures, and two-factor authentication (2FA) across campus systems.
4. **Enhancing Collaboration** – Partner with cybersecurity experts, industry leaders, and government agencies to provide students with hands-on exposure.
5. **Improving Cybersecurity Infrastructure** – Invest in secure networks, firewall protections, and faculty training programs to build a resilient digital learning environment.

By prioritizing cybersecurity education and awareness, higher education institutions can equip students with the knowledge and skills needed to navigate the digital world securely, contributing to a safer and more cyber-resilient society.

References

1. Eric C. K. Cheng & Tianchong Wang (2022). Institutional Strategies for Cyber Security in Higher Education Institutions. *Information* 2022 13,192. https://doi.org/10.3390/info13040192
2. Mayieka Jared Maranga & Dr. Masese Nelson (2019). Emerging Issues in Cyber Security for Institutions of Higher Education. *International Journal of Computer Science & Network*, 8 (4). https://www.researchgate.net/publication/335664780
3. Narmeen Shafqat & Ashrof Masood (2016). Comparative Analysis of Various National Cyber Security Strategies, *International Journal of Computer Science & Network,* 14 (1) https://sites.google.com/site/ijcsis/ISSN 1947-5500
4. Rajeswari Raju, Nur Hidayah Abd Rahman & Atif Ahmad (2022). Cyber Security Awareness In Using Digital Platforms Among Students In A Higher Learning Institution, *Asian Journal of University Education*, 18. https://eric.ed.gov/?id=EJ1348600
6. Neelesh Jain & Vibhash Shrivastav (2014). Cyber Crime Changing Everything – An Empirical Study, *International Journal of Computer Application,* 4 (1). https://www.researchgate.net/publication/275709598
7. Yuchong Li & Qinghui Liu (2021). A Comprehensive Review Study of Cyber-Attacks and Cyber Security : Emerging Trends and Recent Developments. *Elsevir Ltd*, https://doi.org/10.1016/j.egyr.2021.08.126.