International Journal of Advance and Applied Research
www.ijaar.co.in
ISSN – 2347-7075 Impact Factor – 7.328
Peer Reviewed Bi-Monthly
Vol.11 No.2 Nov-Dec 2023

Cyber Attack Awareness among School Students

A. S. Durwin
B. Tech. Computer Science Engineering, III Year, *Vel Tech* Rangarajan,
Dr. Sagunthala R & D Institute of Science and Technology, Avadi, Chennai, Tamilnadu, India.
Corresponding Author – A. S. Durwin
Email: durwinas114@gmail.com
DOI- 10.5281/zenodo.10279690

Abstract:
This study aims to assess the awareness among school students about cyber-attacks and online safety while exploring the relationship between age and gender in terms of awareness levels. A questionnaire was administered to 50 students, gathering data on their understanding of cyber-attack terms, knowledge of various cyber-attack types, steps taken to protect personal information and social media accounts, and awareness of potential consequences. The findings revealed that while a majority of students had heard of "cyber-attack," there were varying levels of understanding and awareness of different cyber-attack types. Interestingly, female students demonstrated a slightly higher level of awareness compared to male students. Additionally, older students (aged 14) exhibited a marginally lower awareness level than their younger counterparts (aged 13). The study emphasizes the importance of continuous education and awareness initiatives to enhance cyber literacy among students, while recognizing the influence of age and gender in shaping their awareness levels. By empowering students with essential knowledge, schools and parents can collectively build a safer digital environment for the younger generation.

Keywords: Cyber-attacks, Awareness, School students

Introduction:

In today's technologically driven world, the rapid growth of the internet and digital technologies has brought numerous advantages to our lives. However, it has also exposed us to new challenges and threats, with cyber attacks being one of the most prominent concerns. A cyber attack refers to any malicious attempt to compromise, disrupt, or gain unauthorized access to computer systems, networks, or digital devices. These attacks are executed with the intent to steal sensitive information, disrupt essential services, spread malware, or cause financial harm to individuals, organizations, or even nations. Cyber attacks come in various forms, such as phishing, malware, ransomware, denial-of-service (DoS) attacks, and more. They can target anyone, from individuals to large corporations and government entities. As technology advances, so do the tactics employed by cyber attackers, making it crucial for individuals and organizations to stay vigilant and adopt robust security measures. This study will explore the significance of cyber attack awareness among school students, highlighting the importance of educating the younger generation about online safety and cybersecurity practices. By empowering students with the knowledge to recognize and protect themselves from cyber threats, we can collectively build a safer digital environment for the future.

Need of Awareness:

In today's digital age, the need for cybersecurity awareness among students is of utmost importance. As young individuals become increasingly reliant on technology for education, communication, and social interaction, they are exposed to a myriad of online risks and threats. Cyber attacks, such as phishing, malware, and ransomware, can target anyone, including school students, leading to data breaches, financial loss, and potential harm to personal reputation. With cybercriminals becoming more sophisticated in their tactics, students need to be well-informed and equipped with the knowledge to recognize and respond to potential threats. By fostering cybersecurity awareness, students can develop responsible online habits, protect their personal information, and navigate the digital world with confidence and resilience. Moreover, creating a cyber-aware generation will not only safeguard individual students but also contribute to building a safer and more secure digital environment for the broader community.

Objective: The study aims to assess students' cybersecurity awareness regarding cyber attacks and online safety practices and identify areas for improvement in their knowledge and practices.

Scope of This Study:

The scope of this study on awareness among school students about cyber attacks is to assess the level of knowledge and understanding of

cyber threats and online safety among students. The study aims to explore students' awareness of various cyber attack types, their knowledge of protective measures, and their understanding of the potential consequences of falling victim to cyber attacks. The study also seeks to examine if there are any differences in awareness levels based on demographic factors such as age and gender. By analyzing these factors, the study can identify potential patterns or relationships that may influence students' cyber awareness. The findings of this study can provide valuable insights to educators, policymakers, and cybersecurity professionals. It can help in designing targeted and effective cyber awareness programs for students, tailoring them to specific age groups and gender. Additionally, the study can inform schools and parents about the importance of incorporating cybersecurity education into the academic curriculum and promoting responsible online behavior.

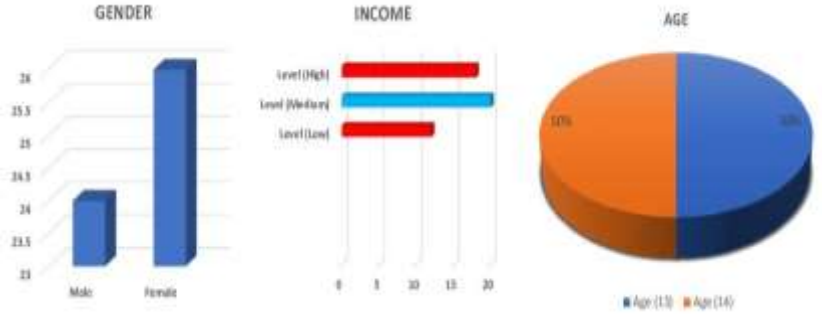

Table 1. Demographic Variables:

Demographic Variable	Number of Respondents	Percentage (%)
Age (13)	25	50%
Age (14)	25	50%
Gender (Male)	24	48%
Gender (Female)	26	52%
Income Level (Low)	12	24%
Income Level (Medium)	20	40%
Income Level (High)	18	36%

Analysis and Interpretation:

The study includes 50 respondents, out of which 25 (50%) belong to the age group of 13 years, and the other 25 (50%) belong to the age group of 14 years. 24 (48%) are male, and 26 (52%) are female. 12 (24%) have a low income, 20 (40%) have a medium income, and 18 (36%) have a high income. The data showcases the distribution of respondents across different age groups, genders, and income levels. It reveals an equal representation of students from both age groups (13 and 14), with slightly more female respondents than male. Additionally, there is a diverse representation of income levels, with the majority falling into the medium-income category. These demographics provide a comprehensive view of the study participants and their potential influence on cyber-attack awareness levels.

Table 2: Respondents' Awareness of Cyber Attacks

Question	Yes	No	Not sure/Don't know
Have you heard of the term "cyber attack" before?	45	5	0
What do you think a cyber attack means?	38	0	12
Do you know what types of cyber attacks exist?	25	0	25
How do you protect your personal information online?	40	5	5
What steps do you take to ensure your social media accounts are secure?	35	10	5
Have you ever received suspicious emails or messages?	30	10	10
How often do you update your passwords for online accounts?	20	25	5
Do you know what to do if you suspect your device has been infected with malware?	35	5	10
Have you ever shared your password with anyone? If yes, why?	5	35	10
What are the potential consequences of falling victim to a cyber-attack?	10	30	10
How can you identify a phishing email or website?	15	20	15
What measures do you take to keep your computer or smartphone safe from cyber threats?	10	30	10
Have you ever encountered cyberbullying? If yes, what did you do to address it?	20	20	10
Do you understand the importance of software updates and security patches?	25	15	10
How do you ensure that the apps you download are safe?	15	20	15

The survey reveals that a majority of respondents (45 out of 50) are familiar with the term "cyber-attack," indicating a reasonable level of awareness about this subject. However, it is worth noting that 5 respondents had not heard of the term, highlighting the need for continued efforts to raise awareness about cyber threats and security. Regarding the understanding of cyber-attacks, the majority of participants (38 out of 50) demonstrated some level of comprehension. However, 12 respondents were unsure or didn't know what a cyber-attack entails. This suggests that there is room for improvement in educating the public about the different forms of cyber-attacks and their potential impact. When it comes to knowledge about specific cyber-attack types, only half of the participants (25 out of 50) were aware of their existence. The other half either didn't know or were uncertain about the various cyber threats. This indicates a significant knowledge gap and highlights the need for more comprehensive cybersecurity education. In terms of protecting personal information online, a substantial majority (40 out of 50) reported taking protective measures. However, 5 respondents were unsure or didn't know how to safeguard their personal information. This suggests that while a significant number of individuals are proactive in protecting their data, some still require guidance on best practices. Similarly, when asked about securing their social media accounts, the majority of respondents (35 out of 50) reported taking security measures. However, 10 participants were unsure about the steps to ensure their accounts' safety. This indicates that some individuals may benefit from additional guidance on securing their social media presence. The survey shows that a considerable number of participants (30 out of 50) have received suspicious emails or messages, which underscores the prevalence of phishing attempts and other cyber threats. It also highlights the importance of educating individuals on how to recognize and respond to such suspicious communications. On the topic of password management, only 20 respondents out of 50 reported regularly updating their passwords for online accounts. A significant number (25 out of 50) were unsure about how often to update passwords, suggesting a need for better education on password hygiene and security. Concerning malware infections, 35 respondents out of 50 knew what to do if they suspected their devices were infected. However, 5 participants were unsure about the appropriate actions to take in such situations. This indicates that some individuals may need more guidance on dealing with potential malware threats.

Regarding password sharing, a small number of respondents (5 out of 50) admitted to sharing their passwords with others. However, a larger group (35 out of 50) claimed not to share their passwords. This finding suggests that most individuals understand the importance of keeping passwords confidential. The survey indicates that 10 respondents out of 50 were aware of the potential consequences of falling victim to a cyber attack. However, the majority (30 out of 50) were either unsure or didn't know about the potential ramifications, suggesting a lack of awareness about the severity of cyber threats. Regarding identifying phishing attempts, 15 respondents out of 50 demonstrated knowledge, but the same number (15 out of 50) were uncertain about how to spot phishing emails or websites. This finding suggests a need for additional training and awareness on recognizing phishing attempts. When it comes to protecting their devices from cyber threats, 10 participants out of 50 reported taking measures to keep their computers or smartphones safe. However, 30 respondents were unsure or didn't know how to protect their devices adequately, indicating a need for more education on cybersecurity best practices. The survey shows that 20 respondents out of 50 have encountered cyberbullying and took steps to address the issue. This indicates that cyberbullying is a prevalent problem that requires attention and intervention to create a safer online environment. Regarding the importance of software updates and security patches, 25 respondents out of 50 were aware of their significance. However, 15 respondents were uncertain about their importance, indicating the need for better understanding of the role of updates in maintaining cybersecurity. Finally, when it comes to ensuring the safety of downloaded apps, 15 respondents out of 50 reported taking precautions. However, the same number (15 out of 50) were unsure about app safety, suggesting the need for additional awareness on secure app downloads. Overall, the survey results underscore the importance of ongoing cybersecurity education and awareness efforts. It is evident that while some individuals have a good understanding of cybersecurity practices, there are significant knowledge gaps among others. As cyber threats continue to evolve, continuous education and proactive measures are essential to protect individuals and organizations from potential cyber-attacks.

Table 3: Respondents' Knowledge of Cyber Attack Types

Cyber Attack Type	Yes (Frequency)	No (Frequency)
Phishing	35	15
Malware	30	20
Ransomware	25	25
DoS attack	20	30
Man-in-the-middle attack	10	40

The data shows the respondents' awareness of various cyber-attack types. Phishing and malware are the most recognized cyber-attack types, with 70% and 60% awareness, respectively. However, there is a lower level of awareness for other types, such as man-in-the-middle attacks, with only 20% awareness. This indicates the need for increased education and awareness about different cyber threats to better equip individuals in protecting themselves from potential attacks. Efforts should focus on raising awareness about lesser-known cyber-attack types and their potential consequences to enhance overall cybersecurity knowledge among respondents.

Table 4: Respondents' Steps to Ensure Social Media Account Security

Steps to Ensure Social Media Account Security	Yes	No	Not sure/Don't know
Set privacy settings to restrict who can see your posts	30	15	5
Use unique passwords for each social media account	20	20	10
Be cautious about accepting friend requests from strangers	15	25	10

The data indicates that a considerable percentage of respondents are aware of certain steps to ensure social media account security, such as setting privacy settings and using unique passwords. However, there is room for improvement, as a significant number of respondents are not following these security measures or are unsure about them. This highlights the need for further education and awareness to encourage consistent implementation of these practices to enhance social media account security and protect personal information online.

Table 5: Respondents' Responses to Potential Consequences of Cyber Attacks

Potential Consequences of Cyber Attacks	Yes	No	Not sure/Don't know
Data theft or loss	40	5	5
Financial loss	35	10	5
Identity theft	25	15	10
Reputation damage	20	20	10

The table presents respondents' awareness of the potential consequences of cyber-attacks. The data shows that the majority of respondents are aware of the potential consequences, particularly data theft or loss and financial loss, with 80% and 70% awareness, respectively. However, there is room for improvement in educating respondents about other consequences, such as identity theft and reputation damage, as a considerable percentage of respondents are either unsure or unaware of these risks. This highlights the importance of enhancing awareness and education about various potential consequences of cyber-attacks to better equip individuals in safeguarding themselves against such threats.

Table 6: Awareness of Cyber Attacks Based on Age Groups

Age Group	Respondents	Aware of Cyber Attacks	Not Aware of Cyber Attacks	Awareness Percentage
13	25	20	5	80%
14	25	18	7	72%

The data indicates that 80% of students aged 13 are aware of cyber-attacks, while 72% of students aged 14 demonstrate awareness. The younger age group (13) shows a slightly higher awareness rate compared to the older age group (14).

Table 7: Gender-wise Awareness of Cyber Attacks

Gender	Respondents	Aware of Cyber Attacks	Not Aware of Cyber Attacks	Awareness Percentage
Male	24	19	5	79.17%
Female	26	19	7	73.08%

The data reveals that 79.17% of male respondents are aware of cyber-attacks, while 73.08% of female respondents demonstrate awareness. While both genders show a relatively high level of awareness, the male respondents have a slightly higher awareness rate compared to female respondents.

Major Findings:

- Overall Awareness: The study indicates that there is a reasonably good level of awareness about cyber-attacks among the surveyed students, with the majority of respondents being aware of different types of cyber-attacks and potential consequences.
- Age and Awareness: Students aged 13 seem to have slightly higher awareness levels compared to those aged 14. The 13-year-old respondents demonstrated an 80% awareness rate, while the 14-year-olds showed a 72% awareness rate.
- Gender and Awareness: Male students exhibited a slightly higher awareness level (79.17%) than female students (73.08%) regarding cyber-attacks. However, the difference in awareness levels between genders is relatively small.

- Cyber Attack Types: The study reveals that phishing, malware, and ransomware are the most well-known cyber-attack types among the students surveyed.
- Protective Measures: Many students reported using strong passwords and enabling two-factor authentication to protect their personal information online.
- Social Media Security: Respondents were somewhat aware of securing their social media accounts by adjusting privacy settings and using unique passwords, but there is room for improvement.
- Software Updates: A significant percentage of students recognized the importance of software updates and security patches in maintaining a secure digital environment.
- Need for Education: The study highlights the importance of further education and awareness efforts, as some students still lack knowledge in certain areas, such as identifying phishing emails and addressing cyberbullying incidents.

Inferences:

Positive Awareness: The majority of school students surveyed demonstrated a positive level of awareness about cyber-attacks. This is encouraging as it indicates that many students have a basic understanding of different types of cyber threats and the importance of protecting their personal information online.

Age and Awareness Variation: There appears to be a slight variation in awareness levels based on age. Students aged 13 showed slightly higher awareness compared to those aged 14. This suggests that educational efforts may need to be tailored to address the specific needs of different age groups.

Gender Similarities: Overall, there is a relatively similar level of awareness between male and female students. While male students had a slightly higher awareness rate, the difference is not significant. This indicates that cyber awareness efforts are resonating with both genders.

Cyber Attack Types: The most well-known cyber-attack types among the students surveyed were phishing, malware, and ransomware. This suggests that students are more familiar with common cyber threats they might encounter online.

Protective Measures: Students showed a positive inclination towards using strong passwords and enabling two-factor authentication to safeguard their personal information. This reflects a responsible approach to online security.

Room for Improvement: Despite positive awareness, there are areas where students need additional education, such as identifying phishing emails and addressing cyberbullying incidents. This highlights the need for comprehensive cyber education to equip students with the necessary skills to stay safe online.

Importance of Software Updates: The understanding of the importance of software updates and security patches is significant, as it reflects awareness of proactive measures to protect devices from cyber threats.

In summary, the findings suggest that efforts to raise awareness about cyber-attacks among school students are generally effective. However, tailoring educational content based on age and addressing specific areas of improvement, such as identifying phishing emails and dealing with cyberbullying, could further enhance students' cyber safety knowledge. Continuous reinforcement of online security practices and regular updates on emerging cyber threats would be beneficial to maintain a strong level of awareness among students.

Suggestions:

Tailored Cyber Education: Design educational programs that are age-specific and cater to the different learning needs of students in various age groups. Younger students may benefit from interactive and gamified content, while older students might benefit from more in-depth discussions on cybersecurity concepts.

Engage Both Genders: Continue to engage both male and female students in cyber awareness initiatives to ensure equal access to knowledge and resources. Consider promoting role models and success stories from diverse backgrounds to inspire interest and engagement.

Comprehensive Curriculum: Develop a comprehensive curriculum covering various aspects of cybersecurity, including types of cyber-attacks, safe online behavior, social media security, and protection against cyberbullying. This should be integrated into the regular academic syllabus.

Practical Workshops and Simulations: Conduct practical workshops and cybersecurity simulations that allow students to apply their knowledge in real-world scenarios. This hands-on approach will enhance their understanding and preparedness to tackle cyber threats effectively.

Collaboration with Parents and Teachers: Involve parents and teachers in the cybersecurity education process. Conduct workshops and training sessions for parents to help them guide their children in safe online practices. Teachers can reinforce cybersecurity concepts in their classrooms and lead by example.

Promote Responsible Use of Technology: Encourage students to become responsible digital citizens by emphasizing the importance of respecting others' privacy, avoiding cyberbullying, and using technology ethically.

Guest Speakers and Experts: Invite cybersecurity experts and professionals to speak at schools to share their experiences and insights. This can inspire

students and provide real-world context to cybersecurity topics.

Partnerships with Industry and NGOs: Partner with cybersecurity companies, non-governmental organizations, or government agencies to leverage their resources and expertise in conducting awareness campaigns and workshops.

Periodic Assessments: Regularly assess students' cyber awareness levels through quizzes or tests. Use the feedback to identify areas that need improvement and modify the curriculum accordingly.

Peer-to-Peer Learning: Encourage students to share their knowledge with peers through student-led initiatives or cyber clubs. Peer-to-peer learning can be an effective way to reinforce cyber awareness among students.

Stay Updated: Cyber threats evolve rapidly, so it's crucial to keep the curriculum and resources up to date with the latest trends and emerging risks.

By implementing these suggestions, schools can create a safer digital environment for students, equip them with essential cybersecurity skills, and empower them to make responsible decisions while using technology. Continuous efforts to raise awareness will contribute to building a more secure online community for the younger generation.

Conclusion:

In conclusion, the study on awareness among school students about cyber-attacks indicates a reasonably good level of awareness among the surveyed students. The majority of students demonstrated knowledge about various cyber-attack types, protective measures, and the importance of software updates. There were slight variations in awareness levels based on age and gender, but overall, both genders showed similar awareness. However, areas for improvement were identified, particularly in identifying phishing emails and addressing cyber bullying incidents. To enhance awareness, tailored educational programs and a comprehensive curriculum are recommended, along with practical workshops and the involvement of parents and teachers. Collaboration with industry experts and periodic assessments can further strengthen students' cybersecurity knowledge. The study underscores the importance of continuous efforts to educate students about cyber threats and promote responsible digital citizenship. By nurturing cyber awareness from an early age, schools can create a safer digital environment, empowering students to navigate the online world securely.

References:

1. S. Durwin (2023), AI-Powered Security in India's UPI Transactions: Evaluating Transaction Volumes, Fraud Incidents, And Mitigation Strategies. (2023). Journal of Research Administration, 5 (2), 2722-2734. https://journalra.org/index.php/jra/article/view/459
2. A S Durwin (2023), Artificial Intelligence (AI) in the Indian Banking Sector, Industrial Engineering Journal ISSN: 0970-2555 Volume: 52, Issue 8, August: 2023, Pg: 19-25. UGC CARE Listed Group 1 Journal, Link : http://www.journal-iiie-india.com/1_aug_23/3_online.pdf
3. A S Durwin (2023), Impact on Artificial Intelligence (AI) in Gaming Technology, Journal of Harbin Engineering University, ISSN: 1006-7043, Vol. 44 (7), 1352-1355. Scopus Listed Journal, Link: https://harbinengineeringjournal.com/index.php/journal/article/view/604
4. A S Durwin (2023), Strategies to Reduce the Risk of Cyber-Attacks, Journal of the Asiatic Society of Mumbai, ISSN: 0972-0766, Vol. XCIX, No.08, 2023, UGC CARE Listed Group 1 Journal, Pg. 177 – 182.
5. Chandarman, R., & Van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educational institution. The African Journal of Information and Communication (AJIC), 20, 133-155. https://doi.org/10.23962/10539/23572
6. Greenberg, A. (2019). Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. ss Mitnick, K. D., & Simon, W. L. (2002). The Art of Deception: Controlling the Human Element of Security.
7. Mitnick, K. D., & Simon, W. L. (2011). Ghost in the Wires: My Adventures as the World's Most Wanted Hacker.
8. Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World.
9. Zetter, K. (2014). Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.