International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Cyber Security Awareness a challenging issue among the College Students: A Case Study

Baidyanath Dash

Asst-prof in Computer Science and Engineering

Abstract:
This paper focuses on cybersecurity awareness among college students. It reports the results of a quantitative survey that aimed to identify college students awareness and enthusiasm to learn cybersecurity at Utkal University in India. The survey aimed to see how students in this developing country are aware of cyberattacks how they can defend against them. How the cybersecurity awareness program is received by college students. Using a theoretical framework we examine new trends in threat intelligence protection of critical infrastructure the human element, in cybersecurity ethical issues and international cooperation.
In particular our work looks at these challenges from a Psychology perspective because we think that knowing how people see risks is key to making awareness campaigns. Changing behaviour is not about giving information about risks and how to react. First students have to be able to understand and use the advice. Second they must be. Ready to do it. The second part needs changes, in attitudes and intentions. These steps before behaviour change appear in psychological models of behaviour.

Keywords: Cybersecurity, Cybersecurity Awareness, Cybersecurity Education, Security tips, Cyber threats and Cybersecurity Awareness Programs.

Introduction:

Security is the important issue for everyone. Because of this government and private agencies must take action against those who break security rules. There is a growing number of IT security incidents around the world. This happens because of the rise in electronic data, mobile devices and other digital tools.
Nowadays organizations operate remotely. Contractors can work from thousands of miles and still stay in touch. This makes life easier and more convenient.. If there is no control over devices the entire workplace infrastructure becomes at risk. Cyberattacks can happen anytime.
Many people now use Wi-Fi to do their work. They. Receive information without thinking about safety. A lot of data moves through these unsecured networks. This is dangerous.
The organization is especially vulnerable to cyberattacks. Why? Because employees might accidentally expose the network. They may connect to the internet without protection.
Governments and businesses around the world use Information and Communications Technologies (ICT) a lot. This makes security more important, than ever. Every organization must protect its data. Every organization must strengthen its defenses. Every organization must protect its network. Security must come first.

Literature Review:

Cybersecurity awareness among students has become a topic that many researchers study because our schools, our chats and our everyday social interactions rely more and more on tools. When students use classes, social media and cloud services the danger of cyberattacks like phishing, identity theft, malware and data breaches grows. Studies always show that students even though they use technology a lot do not always know how to stay safe. Cybersecurity awareness is a part of stopping cyber threats and keeping digital spaces safe. Many studies look at how much different groups know about cybersecurity.

The researcher looked at the tools that studies use to measure cybersecurity awareness the groups involved and the main results of each paper. When it comes to how cybersecurity awareness affects the security plans of universities only a few reviews have been done. Thani et al. (2021) Ran a survey of students in higher education and found that rules and training did not match up.. That study treated all schools the same, even the rural ones and did not explain the special conditions of rural universities.

Parents and teachers play a role in shaping how students act online. Kumar et al. (2023) Say that schools that add cybersecurity lessons to their classes see students who know more. Families, with younger kids help create good habits at home. Because cyber threats keep changing we need a way to teach cybersecurity.

This review pulls together findings from surveys, research papers and teaching reports from 2017 to 2024. The search brought up terms like "cybersecurity awareness," "student safety," and "cyber threat education." To cover the topic fully we used trusted sites such as IEEE Xplore, Springer and Google Scholar.

Many ways were used to measure cybersecurity awareness in students. Surveys and questionnaires are common. Daengsi et al. (2022) Sent a survey to workers in a global company to see how well they spot phishing. The results showed that 75% could not spot phishing emails. In another study, by Alharbi & Tassaddiq (2022) people tried social engineering attacks and the researchers could see how they responded.

Adewopo et al. (2025) Also did a review called " analytical review of cybercrime and cyber policy in West Africa " which looked at cybersecurity awareness and studied how peoples actions help spread or stop cyber threats.. Even though their research is the starting point for cultural awareness programs in schools they did not use a structured SLR method and did not use proper methods to pick and look at current research.

Core Findings from the Literature

- Baseline Awareness Levels: Most studies show that students have some idea about threats like phishing, malware and identity theft. They do not know how to handle them. For example surveys often say that than 60% to 65% of students cannot tell a phishing email from a real one or they use the same password for many accounts. [1 2 3]
- The "Human Firewall" Deficit: Research shows that students, those who are undergraduates or taking online classes usually do not do security training unless their school makes them. This leaves them at risk from tricks used by hackers and from using Wi-Fi. [1 2 3]
- Demographic and Academic Factors: Research says that students who study IT or computer-related subjects and those who are in years of study have better knowledge about cybersecurity than first-year students or those, in other fields

Objectives of the study:

In 2024 Childers, G. And colleagues [11] looked at how important development and cybersecurity education are for K–12 teachers. Even though there has been a lot of focus on teaching cybersecurity to students there is still a need to support teachers. Teachers need training to feel confident and use effective methods when teaching cybersecurity. The study explored how increasing teachers self-confidence could help them design and deliver cybersecurity lessons effectively.

Liluashvili, G.B. (2021) [12] Pointed out that cyberattacks on education institutions have increased. Between 2005 and 2020 over 1,300 breaches were recorded in the United States. These attacks led to the compromise or theft of about 24.5 million records. The study focused on the kinds of cyber threats that target schools and colleges. These threats can lead to security failures and financial losses. The research highlighted the need for well-designed safety plans to reduce these dangers.

The following points were taken into account for the study:

1. To assess how aware secondary school students are about cyber safety and security.
2. To look at differences in safety and security awareness among secondary students based on different subgroups.
3. To examine differences in aspects of cyber safety and security awareness among secondary school students.
4. To compare how aware undergraduate students and postgraduate students are about security.
5. To compare security awareness between male and female students, in higher education.
6. To find out which cyber security topics rural students know the least about.

Research Questions:

This research is very important for making plans that will make online safety better. It needs an understanding of the complicated problems involved. This research will help school kids and college students a lot. Also the study wants to look at how good the current online safety education programsre in schools. The goal is to match these programs with models and suggest changes to make students better at handling online risks.

The important questions that were looked at in this study are

- To find out if the online safety education program is needed.
- Who is the group of people this research is for?
- Where did the research take place?
- What software or materials were used in the research?
- How did the research help people know about risks?

Did the researcher explain why they chose their way of doing the research?

In addition to these questions other questions should also be thought about in this study from the students point of view and the organizations point of view. These questions are listed here.

RQ1 and RQ2 are questions that want to solve the need for online threat awareness in regular and school settings.

Research Question 1 (RQ1):

What are the different challenges and problems that people face when dealing with safety, good habits and security in different areas?

RQ1 is about trying to understand the problems and worries that people who work on online safety good habits and security face in different situations. The changing online world brings challenges that need to

be studied. This involves people and places like social areas, technology areas and education areas. To make plans for online safety it is very important to know these challenges.

Research Question 2 (RQ2):

How do the online safety education programs in schools match up with models and what can be done to make them better?

The goal of RQ2 is to check how well the online safety education programs in schools follow models and to suggest ways to make them better. This topic is completely, about what students and schools think about safety education.

RESEARCH GAP:

A research gap is an area in a subject that hasn't been studied enough. It is a place where there is not information or where the information is not clear. It includes questions that are not answered topics that are not looked into or results that don't match. Finding these gaps helps people learn more fix problems with studies and decide where to look next. These gaps can appear because the ways of doing research are old because new tools are available or because what people care about changes over time.

The problem is that many studies look at awareness, policy and technology on their own. They do not look at how research on awareness and research on policy and research on technology can all be connected as one thing.

Key Research Gaps in Student Cybersecurity Awareness

- **The Cognition-Execution Disparity:** Research shows a difference where students know a lot about security but do not act on it—like not using multi-factor authentication or not reusing passwords.
- **Inefficacy of Static Informational Training**: Traditional ways of teaching like lectures or videos do not work well. Students often ignore them. Studies from the University of Chicago Computer Science Department show that interactive methods work better.. There is no research on how well these methods work over a long time.
- **Vulnerability to Advanced Social Engineering:** Even though students can spot phishing emails 90% have trouble with more complex attacks like targeted emails fake job offers or false invoices.
- **Neglect of Rural and Gender Disparities:** Most studies focus on cities or schools that are tech-savvy. Research from the Banaras Hindu University Repository shows that students in areas have less knowledge. Also female students score lower than students showing a need for more studies in these areas.
- **Absence of NonPunitive Experiential Frameworks**: There is not research, on how to include hands-on learning and models that teach security without making students feel stressed. This needs to be done in classes that are not related to technology.

Research Methodology:

This study used a research approach combining a thorough literature review with theoretical analysis. We brought together findings from peer-reviewed journals, government reports and industry white papers. This study also uses a mixed-method research design mixing both qualitative approaches to look at cybersecurity awareness among students. The research mainly uses a questionnaire survey, supported by secondary data from recent scholarly literature. A survey was carried out with 80 students who're internet users to gauge their awareness of cybercrimes in the Odisha region. The ages of the respondents range from 14 to 23 years. Convenience sampling was used to choose the respondents for the survey.

Opinions about agreement levels were collected on a Likert scale. Analyzed using percentages. According to word frequency results the top three words in the literature are Information, Data and Security which show that the literature review went in the direction.

Research Design:

Sample and Data The study data came from 380 students, both undergraduate and postgraduate from CHSE and Utkal University in Bhubaneswar, Odisha, India. A stratified random sample was used for this -sectional study. In this study smart technology users in the transformation phase were chosen as the sample respondents. The process of splitting a population into subgroups called strata is a key feature of stratified random sampling. The strata are based on traits or attributes, such as income or education level. The strata were chosen using education level criteria.

A descriptive and analytical design was used to evaluate students' knowledge, attitudes and behaviors related to cybersecurity. The study aims to identify awareness levels and to examine factors that influence secure practices.

Population and Sample The target population includes undergraduate and postgraduate students from academic disciplines. A sample size of about 100 to 150 students is considered enough, for analysis. It was chosen using convenience sampling because of accessibility and time constraints.

Data Collection Methods

Primary Data:

Awareness of cyber threats (phishing, malware, etc.)

- Password and privacy practices
- Experience with cyber incidents
- Exposure to cybersecurity training

Secondary Data:

- Obtained from journals, conference papers and online academic databases to support findings.
- Data Analysis Techniques
- The collected data is analysed using:
- Descriptive statistics (percentage, mean frequency distribution)
- analysis (awareness vs behavior)
- Graphical representation (charts and tables)

Method of Analysis:

I chose to use the PLS-SEM technique with Smart PLS 3.3.9 software because my sample size was small the data was not normally distributed and the models were complicated. Even though other methods such as correlation, regression and analysis of variance (Hair et al., 2014) exist PLS-SEM is often used for data analysis. It allows me to study the relationship between measured variables and hidden variables that cannot be examined with approaches (Hair et al. 2014). I can also. Immediately add mediator effects to the model using PLS-SEM (Hair et al., 2014). A two-stage model, with a measurement model and a structural model is used to examine the data. The structural model tests the hypotheses through path analysis while the measurement model evaluates the latent variables.

Significance and Scope of the Topic:

Digital platforms are now a major part of learning and social life and students are becoming targets for cybercriminals. Programs that bridge the gap between connectivity and user safety help turn passive technology users into active cyber-resilient citizens.

The study on cyber safety awareness among students, undergraduates and postgraduates is very important in today's digital age. Adolescents use tools, social media and various digital platforms a lot. While they navigate social settings they face many cyber risks such, as cyberbullying, phishing scams and privacy breaches. I want to evaluate how well they understand and prepare for these threats. By finding gaps in their knowledge I hope to give insights that can guide the creation of more effective educational programs and policies that fit their specific needs.

Scope of Cybersecurity Awareness Programs:

The scope sets the limits the actions to take and the reach across fields for these cybersecurity learning programs.

Scope Category: Personal Cyber Hygiene

Core Operational Focus: Foundations of device and network safety.

Key Practical Applications:

- Creating complex passwords
- Securing home networks and avoiding risky public Wi-Fi
- Implementing regular software updates

Scope Category: Academic Lifecycle Security

Core Operational Focus: Protecting institutional platforms during enrollment.

Key Practical Applications:

- Onboarding safety for Learning Management Systems (LMS)
- Securing institutional emails and cloud applications
- Safe practices on shared campus computers

Scope Category: Behavioral & Critical Thinking

Core Operational Focus: Resisting manipulation and identifying deceit.

Key Practical Applications:

- Spotting engineering and pretexting schemes
- Developing skepticism toward unsolicited requests and links
- Reporting suspicious network anomalies without fear of penalties

Scope Category: Cross-Curricular Integration

Core Operational Focus: Moving beyond computing classes into all domains.

Key Practical Applications:

- Integrating digital safety benchmarks across humanities, arts and sciences
- Applying scenario- project-. Gamified problem-based learning models

Scope Category: Vocational & Professional Shift

Core Operational Focus: Preparing students for security expectations, in environments.

Key Practical Applications:

- Understanding workplace data compliance regulations
- Practicing operation of corporate digital tools

- Engaging in simulated Capture-The-Flag (CTF) events and cyber ranges

Theoretical Framework:

Practical Steps Everyone Should Follow

These are the must-do practices for cybersecurity awareness and making digital safety stronger: The steps follow.

1. Strong password management: A rule for keeping sensitive data safe.
2. Multi-factor authentication (MFA): important for adding another layer of safety against unauthorized entry.
3. Safe browsing habits: Important for protecting data from cyber threats.
4. Regular software updates: Must for keeping information security and cyber defence working.
5. Data backup: important, for stopping cybercrime especially ransomware attacks.

Why Cyber security Awareness Matters:

Cybersecurity awareness starts with a well-informed workforce and community; they act as the line of defence. Cybersecurity awareness helps prevent cyber-attacks by cutting down phishing attempts and lowering malware infections. Cybersecurity awareness also strengthens strategies that protect sensitive data. Technology can block attacks but human behaviour is often the weak link. A weak password, clicks, unsafe downloads and casual sharing of sensitive information are major causes of breaches. This is why cybersecurity awareness and cybersecurity education are essential to reduce risk and strengthen information security systems.

The benefits of cybersecurity training programs include protecting organisational data preventing financial fraud and identity theft reducing malware incidents and ensuring compliance with legal frameworks. In the end cybersecurity awareness stops cyber-attacks by giving individuals the power to follow digital practices and spot threats early.

Common Cyber Threats:

Understanding threats is essential in cybersecurity education and cybercrime prevention. The following points cover the threats.

1. Phishing: Phishing is a challenge for cybersecurity awareness. Attackers pretend to be trusted entities. Try to steal credentials and data. They create emails or websites that look real tricking victims into giving financial information.

Safety Tips:

1. Carefully check the URL before clicking it.
2. Never react to a message that shows urgency.
3. Do not trust offers that look "too good to be true".
4. Do not hesitate to report phishing to law enforcement agencies if you become a victim.
5. Verify the email address in emails that are addressed to recipients.
6. Look for typing errors (Acc0unt, ema1l, dep0sit, passw0rd).
7. Notice grammar and unprofessional language; it may be a sign of phishing.

2. Malware: Malware is a category that threatens digital security and cyber defense systems. It includes viruses, Trojans, spyware and ransomware. Malware is code that threat actors insert into applications, programs or systems. Once installed malware can infect systems. Carry out harmful operations.

1. Safety Tips:
1. Avoid clicking emails, links and sites from unknown sources.
2. If you click a link your mobile can be hacked or your data can be stolen.
3. Browse secure and authorised websites.
4. Keep your computer software and browser up to date.
5. Keep backups of your data.
6. Install pop-up or ad-blockers to stop advertisements on websites.
7. Install antivirus and anti-malware solutions on devices. Keep them updated.
8. Hover over images or links to see the destination URL.
9. Do not install apps from links received in chats or social media posts.

3. Malicious Mobile Applications: Infected mobile apps can contain malware that steals data, login credentials or auto-subscribes to premium services.

Safety Tips:

1. Before downloading any application check for the Play Protect feature on the Play Store.
2. Download applications from trusted sources such as legitimate websites or authorised app stores.
3. Avoid downloading apps from SMS, emails or social media messages.
4. Be careful about granting permissions during app installation.
5. Read user reviews and comments before installing any application.

4. Vishing: Vishing is when fraudsters call victims pretending to be from trusted organisations such as banks, tax authorities or gas companies. They ask for bank account details and financial information about debit or credit cards, including expiry dates. The fraudster then tells the victim to share the OTP that was sent to the phone for a deposit. Once the victim shares the OTP money is taken from the account.

Safety Tips:

1. Never share OTP, PIN, CVV or debit/credit card details, with anyone.
2. Do not share OTPs or UPI PINs for receiving money.
3. Do not answer calls that ask you to confirm or share bank account or card details or other sensitive information.
4. Do not give information to claim a prize, lottery, gift or to update KYC.
5. Do not call service provider numbers found online. search engines can show numbers.
6. Use the customer care service numbers that are listed on authorized websites of the institute organisations, banks, etc.
7. If any incident happens the user should call 1930 change the password of the account away or block the card or freeze the account to stop financial loss.
8. Users should look over bank and credit card statements regularly. Report any strange items.
9. Beware of calls that ask for information or want to install remote access apps pretending to help.

5. **Identity theft:** It is a problem in data protection and cyber safety, where personal information is stolen.
6. **Social engineering:** It is the use of tricks in cyber attacks showing why people need to learn about cyber safety. Scammers use bots to fool users into sending money to accounts they control like through internet banking or UPI transfers. Fraudsters create profiles of the victim:

1. To spread fake information.
2. Sends friend requests to friends of the victim to gain money.

3. To damage the victims reputation.

Safety tips:

1. Avoid sharing information such as address, mobile number, personal email ID and other sensitive identity details on social media.
2. Do not post pictures publicly on social media accounts.
3. Never accept friend requests without verification and confirmation.
4. Never click on links or download apps received through messages until you check that the source is real.

Use passwords for each social media account and email.

5. Enable multi-factor authentication for media accounts.
6. Disable profile visibility from searches.
7. Log out after each session.

Never share media credentials with anyone.

8. Keep the privacy settings of the media profile at the most restricted level especially for public viewing.
9. Be very careful when sharing photographs, videos status updates, comments, etc.
10. Criminals can gather information about users, from their posts and profiles.

7. **One-click & Zero-click attacks:** Advanced threats underline the importance of information security and cyber defense systems.

8. Attacks Targeting Children: Cyberbullying is a type of harassment that involves sending, posting or sharing harmful, false or mean content about another person. It can also involve sharing private information that causes embarrassment or humiliation.

Safety tips:

1. Review social media privacy settings. Limit access to family and known friends.
2. Teach children about password safety.
3. Check children's social media. Keep track of them.
4. Ensure children do not share identifiable information such as trackable location.
5. Stop engagement on social media.
6. Do not accept "Friend Requests" from strangers on media.
7. When bullied log off the site save the chat, messages or e-mail and inform parents, teachers or trusted elders.
8. Do not respond. Block the e-mail or messages.
9. Think carefully before sharing
10. Use privacy settings. Control the posts you publish online.
11. Never share your password. Even friends may misuse it.
12. Being kind to others online helps keep you safe.
13. Talk to a trusted adult about any messages or posts you encounter online. A trusted adult can help remove bullying.

9. Attacks Targeting Persons with Disability students: Fraudulent individuals often pose as authorized representatives to scam people with disability. They. Email victims and request personal information. Fraudsters also offer promising opportunities like working from home or earning extra income.

Safety tips:

1. Before engaging with any person or business online or over the phone ensure no confidential information is shared without confirming the identity of the receiver.
2. Be aware of types of threats and learn to spot a scam.
3. Call 1930 if you become a victim.
4. Do not click on links or attachments.
5. Do not download any application received through chats, email or social media platforms.

Cybersecurity Basics for Students:

Students must understand cybersecurity principles to navigate this digital world safely. Much of social life happens online so a strong grasp of cyber security helps protect against potential threats.

1. Understanding Password Security:

Password security is a cornerstone of safety. The many online accounts and services mean understanding the risks of passwords and the benefits of a password manager is crucial. Weak passwords can be easily compromised, allowing access to sensitive information. A password manager however helps create and manage unique passwords greatly improving online security.

The Risks of Weak Passwords

Weak passwords pose a threat to online security. They are often easy to guess or crack, giving hackers a gateway to information. Recent statistics show that 81% of data breaches result from reused or weak passwords. Using passwords can lead to severe outcomes, such as financial loss, identity theft or compromised accounts. Ensuring passwords are strong and unique is a step in protecting online presence.

2. Multi-factor Authentication:

Multi-Factor Authentication (MFA) secures user accounts with layers of protection. It verifies identity through than one independent credential. MFA, a form of two-factor authentication reduces the risk of forced logins.

MFA uses authentication methods creating an added layer of security against hacking and data breaches. For example if MFA is activated on a Gmail login after entering the password the system will require a push notification response on a phone or a specific code, from SMS to grant account access.

Therefore with MFA, if a perpetrator manages to circumvent the second authentication method the third layer would remain to ensure protection. Moreover most of these authentication modes are challenging for any criminal to access since they are among items such as biometric data enabling robust security.

Multi-factor Authentication benefits:

Multi-factor Authentication plays a role in implementing information security. It is a resource against data breaches and cyber-attacks. Apart from that Multi-factor Authentication comes with other benefits such as:

- It is easy to implement.
- It protects consumer identity.
- It helps businesses meet compliance.
- It complies well with Single Sign-On (SSO) Solutions.
- It is a solution to implementing cybersecurity.
- It ensures remote work stays secure.
- It helps simplify cloud-based data sharing and storing.

There are ways that you can implement MFA, such as:

- One-Time Password (OTP)
- Push notification

3. Secure Browsing: Always look for the 'https' and padlock symbol in your browser's address bar when submitting information online. This signifies that your connection to the site is encrypted and more secure.

4. Software Updates: Regularly updating your devices' software ensures you have the security patches helping protect against known vulnerabilities that cybercriminals could exploit.

Cybersecurity Awareness Tips for Students:

The path to becoming cyber- starts with learning and understanding the basics of cybersecurity.. To truly make a difference this knowledge must be implemented. Here are some tangible steps you can take as a student to boost your cybersecurity awareness and help create a digital environment:

1. **Stay Informed:** Cybersecurity is dynamic with threats emerging regularly. Stay updated on the cyber threats and security practices by following reliable cybersecurity blogs, podcasts or news outlets.
2. **Use Secure Connections:** Whenever possible avoid using Wi-Fi for activities that require you to enter personal or sensitive information. If you must use Wi-Fi consider using a Virtual Private Network (VPN) to secure your connection.
3. **Regularly Update and Back up Your Data:** Ensure your devices are constantly updated with the software versions as these often contain security enhancements. Additionally regularly backing up your data can help mitigate the damage if your device is compromised.
4. **Learn About. Implement Privacy Settings:** Each social media platform and online service has different privacy settings and options. Take time to understand these settings and customize them according to your comfort level and needs.
5. **Participate in Cybersecurity Training:** Many schools and online platforms offer cybersecurity training. Participate in these pieces of training to deepen your understanding of cybersecurity and learn skills for staying safe online.

Discussion:

The survey results reveal insights into the state of cyber security awareness among rural students in higher education particularly regarding their familiarity with essential concepts and practices. Total 296 students participated in this research. The mean score was 16.30 with a standard deviation of 4.97. The awareness levels varied significantly across the population with 39.29% of individuals scoring below the mean and 60.82% scoring above it. These findings suggest an important observations in cyber security awareness that needs to be addressed.

Given the increasing relevance of literacy integrating these concepts into the education system would be a critical step toward enhancing the overall cyber security awareness of students. While the rural student population in education demonstrates a moderate level of cyber security awareness there is a clear need for improvement particularly in specific areas where knowledge gaps persist. Implementing interventions and including cyber security topics, in the curriculum could help bridge these gaps and ensure students are better prepared to navigate the digital landscape safely.

Future Directions:

This study has limitations, like many earlier studies. The current study tried to gather a sample to fix the problem of non-random sampling. The number of responders varied because of data gathering challenges. Yet the larger sample should help lessen problems. Also remember that as students move through their years students can find more part-time jobs. This study did not count that factor because undergraduate part-time jobs differ from full-time internships or jobs in character, intensity and frequency. This study was done in one country. Future studies should include countries to compare cybersecurity awareness. Future studies should also include cities to bring more unique findings.

The future of threat intelligence lies in real-time insights that can fit into an organization's security operations without difficulty. Cybersixgill (n.d.) stresses the need for real-time, actionable threat intelligence. Their method uses dark-web sources to give warning of possible threats showing that threat intelligence gathering is growing. Artificial Intelligence (AI). Machine Learning (ML) will play a larger role in threat intelligence. These tools can handle amounts of data, spot patterns and forecast potential threats faster and more accurately than human analysts alone. As Nurse et al. (2017) Say, "AI and ML techniques can greatly improve the ability to detect and respond to cyber threats in real-time" (p. 22).

Another emerging trend is the use of threat intelligence platforms (TIPs) that collect and examine data from sources. These platforms give a view of the threat landscape and help organizations rank their security priorities more effectively. The future of threat intelligence also focuses more on proactive threat hunting. Of waiting for alerts security teams search for hidden threats inside their networks. This method, with advanced analytics helps organizations spot and react to threats faster.

The growing cybersecurity threats that institutions, especially schools and colleges students face are examined in this review. The review also shows how important cybersecurity awareness programs are for reducing risks. It gives recommendations to improve cybersecurity education in schools by analysing current programs and looking at future trends. In answer to Research Questions 1 and 2 the review looks at obstacles to promoting cyber safety and resilience with special focus on the educational system.

The studies show that cyber threats keep changing with hackers using methods such as phishing and ransomware. Technology, such as intelligence and blockchain is seen as essential, for fighting these threats. Human error is a worry so education and training are recommended to stop mistakes that could cause breaches.

Conclusion:

The increasing cybersecurity threats that educational institutions, especially schools, colleges students are facing are thoroughly examined in this review, which also highlights the critical role that cybersecurity awareness programs play in reducing hazards. It offers feasible recommendations to improve cybersecurity education in educational settings by critically analysing current programs and envisioning future trends. In response to Research Questions 1 and 2, it examines international obstacles to promoting cyber safety and resilience, paying particular attention to the educational system.

The studies reveal that cyber threats are constantly evolving, with hackers using advanced techniques like phishing and ransomware. Technology, like artificial intelligence and blockchain, is seen as crucial for defending against these threats. Human error is a big concern, so education and training are recommended to prevent mistakes that could lead to breaches.

References:

1. Renaud, K., et al. (2022). Promoting the use of security tools among students: A behavioral approach.
2. Computers & Security, 118, 102752. https://doi.org/10.1016/j.cose.2022.102752
3. Sharma, P., & Gupta, S. (2022). Examining students' password management practices. International Journal of Cybersecurity Intelligence & Cybercrime, 5(2), 23–38.
4. Singh, A., & Sharma, R. (2023). Understanding students' cybersecurity behaviors in remote learning environments. Journal of Information Security, 13(1), 31–45.
5. Tade, O., & Aliyu, A. (2020). Exploring university students' cybersecurity practices. African Journal of Information Systems, 12(1), 45–60
6. Williams, C. (2021). Investigating password practices among students. Journal of Digital Security, 14(3), 78–92.
7. National Cybersecurity Alliance. (2023). State of cybersecurity awareness in education: Annual report.
8. https://staysafeonline.org/reports
9. Kritzinger, E., 2014, August. Online safety in South Africa-A cause for growing concern. In 2014 Information Security for South Africa (pp. 1-7). IEEE.
10. Parimalam, S., Kasmin, I.F., Abidin, Z.M.Z. and Vasudavan, H., 2022. Cybersecurity Awareness Among Teenagers and Children Using Self-Learning System. International Journal of Data Science and Advanced Analytics, 4, pp.131-138.
11. Rahman, N.A.A., Sairi, I.H., Zizi, N.A.M. and Khalid, F., 2020. The importance of cybersecurity education in school. International Journal of Information and Education Technology, 10(5), pp.378-382.
12. Knott, J., Yuan, H., Boakes, M. and Li, S., 2023, March. Cyber Security and Online Safety Education for Schools in the UK: Looking through the Lens of Twitter Data. In Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing (pp. 1603-1606).
13. Ahmed, O.S., 2021. Teacher's awareness to develop student cyber security: A Case Study. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(10), pp.5148-5156.
14. De Barros, M.J.Z. and Lazarek, H., 2018, January. A cyber safety model for schools in Mozambique.
15. In Proceedings of the 4th International Conference on Information Systems Security and Privacy, Funchal, Portugal (pp. 22-24).
16. Crick, T., Davenport, J.H., Irons, A. and Prickett, T., 2019, October. A UK case study on cybersecurity education and accreditation. In 2019 IEEE Frontiers in Education Conference (FIE) (pp. 1-9). IEEE.
17. Alqahtani, M. A. (2022). Factors Affecting Cybersecurity Awareness among University Students. Applied Sciences (Switzerland), 12(5). https://doi.org/10.3390/app12052589
18. Alsharida, R. A., Al-rimy, B. A. S., Al-Emran, M., & Zainal, A. (2023). A systematic review of multi perspectives on human cybersecurity behavior. Technology in Society, 73. https://doi.org/10.1016/j.techsoc.2023.102258
19. Annabelle, L. (2019). Why is methodology important in research? Retrieved from https://www.quora.com/Why-is-methodology-important-in-research
20. Bagchi, B. K. (2017). Why is methodology important in research? Retrieved from https://www.quora.com/Why-is-methodology-important-in-research.

21. Kelley, K. (2023). What is Cybersecurity and Why It is Important? simplilearn. https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-cyber-security. Retrieved on 30/01/24.
22. Kesharwani, S. (2020). 14C A New Cyber Initiative- By Government of India in 2020. 6, 25– 31.
23. Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity awareness framework for academia. Information (Switzerland), 12(10), 1–20. https://doi.org/10.3390/info12100417
24. Khalid, F., & El-Maliki, T. (2020). Teachers' experiences in the development of digital storytelling for cyber risk awareness. International Journal of Advanced Computer Science and Applications, 2, 186–191. https://doi.org/10.14569/ijacsa.2020.0110225.
25. Kritzinger, E., 2020. Improving cybersafety maturity of South African schools. Information, 11(10), p.471.
26. Javidi, G. and Sheybani, E., 2018, October. K-12 cybersecurity education, research, and outreach. In 2018
27. IEEE Frontiers in Education Conference (FIE) (pp. 1-5). IEEE.
28. Catota, F.E., Morgan, M.G. and Sicker, D.C., 2019. Cybersecurity education in a developing nation: The Ecuadorian environment. Journal of Cybersecurity, 5(1), p.tyz001.
29. Pusey, P. and Sadera, W.A., 2011. Cyberethics, cybersafety, and cybersecurity: Preservice teacher knowledge, preparedness, and the need for teacher education to make a difference. Journal of Digital Learning in Teacher Education, 28(2), pp.82-85.
30. Ali, A. and Umar, Z., 2021. Understanding Cybercrime and Youth: A Perception Based Approach. Pakistan Journal of Social Research, 3(3), pp.130-136.
31. Kritzinger, E., 2015, July. Enhancing cyber safety awareness among school children in South Africa through gaming. In 2015 science and information conference (SAI) (pp. 1243-1248). IEEE.