Digital Survey: Cyber Security Awareness Among Internet Users

Abhishek Ponde[1], Dipti Kotawadekar[2], Das Laxmi[3], Praful Sasane[4], Piyusha Wankhede[5]
[1]Department Of Computer Engineering
[2, 5]Department Of B.ed
[3]Department Of Mechanical Engineering
[4]Department Of LLB
[1, 3]Sinhgad Institute Of Technology, Lonavala, India
[2, 5] *Smt. Kashiba Navale College of Education*, Lonavala, India
[4] *Manikchand Pahade Law College Chhatrapati Sambhaji Nagar*, India

Abstract- *Because of the internet's increasing dependence on digital platforms, cyberthreats including malware and phishing have escalated. Many internet users are still at risk despite developments because they are unaware of their vulnerability. In addition to examining ways to improve responsible digital behaviour and encouraging education and awareness campaigns for a safer online environment, this study looks at students' awareness of cyber security in higher education..*

Keyword-*Cyber-crime, Cyber security, Awareness, Higher Education Students.*

I. INTRODUCTION

The increasing dependence on the internet has had a profound impact on social interactions, business, education, and communication. But as a result of this digital growth, there are now more cyberthreats, such as virus assaults, phishing, hacking, and identity theft [1]. Global internet penetration is still increasing, and being aware of cybersecurity issues has become essential to promoting responsible and safe online conduct [2]. Understanding possible cyberthreats and implementing security procedures to safeguard individual and organizational data are referred to as cybersecurity awareness. According to research, young people who use the internet frequently—especially college students—are extremely susceptible to cyberattacks because of their constant use of social media and digital platforms [3]. According to studies, demographic variables including field of study, geography, and educational attainment have a big influence on cybersecurity awareness levels. When it comes to internet security, urban students often know more than their rural counterparts [4]. Furthermore, people in technical education have greater understanding of cybersecurity than those in non-technical fields [5]. There is still a big disconnect between knowledge and actual implementation, even with the abundance of security technologies available. Even though many users are aware of the threats associated with cyberspace, they neglect to implement crucial security precautions like turning on two-factor authentication (2FA), changing passwords often, and staying away from unprotected networks [6]. This disparity emphasizes how urgently educational and awareness initiatives on cybersecurity are needed in schools and colleges [7]. Around the world, organizations and governments have started implementing measures to raise awareness of cybersecurity. Programs like India's Digital Personal Data Protection (DPDP) Act (2023) and National Cyber Security Policy (2013) are designed to protect personal data and encourage safe online conduct [8]. However, user involvement and adherence to cybersecurity best practices are crucial for these projects to be effective [9].

II. LITERATURE REVIEW

A. *Cybersecurity Awareness and its Importance*

Cybersecurity awareness is the ability to recognize cyberthreats and take preventative measures against dangers such as malware, phishing, and identity theft. Studies have shown that those with greater expertise are less likely to fall victim to cyberattacks [1]. Further study emphasizes that cybersecurity awareness campaigns need to focus on both knowledge transmission and behavioural modifications to guarantee successful implementation [2].

B. *Factors Influencing Cybersecurity Awareness*

Age, educational attainment, and academic discipline are some of the variables that affect cybersecurity awareness levels. Research indicates that students in technological fields are more conscious of cybersecurity than their non-technical peers [3]. Additionally, because they have greater access to technology and training programs, urban

users are often better versed about internet security than their rural counterparts [4].

C. ***Challenges in Cybersecurity Education and Adoption***

Despite the availability of cybersecurity education resources, many users fail to implement security practices in real-world scenarios. Research highlights that overconfidence in personal cybersecurity knowledge leads to risky behaviours such as ignoring security warnings, using weak passwords, and failing to enable two-factor authentication [5]. Furthermore, challenges such as **a lack of formal cybersecurity training, limited institutional support, and the absence of standardized security curricula** contribute to the gap between awareness and practice [6].

D. ***Government Policies and Cybersecurity Initiatives***

To raise awareness of cybersecurity, governments all across the world have implemented policies. Initiatives like India's Digital Personal Data Protection Act (2023) and National Cyber Security Policy (2013) are designed to inform and safeguard individuals against online dangers [7]. However, user participation and the successful execution of awareness campaigns are necessary for these policies to be effective [8].

E. ***Strategies for Improving Cybersecurity Awareness***

Researchers recommend using social media for awareness campaigns, holding frequent training workshops, and incorporating cybersecurity education into school curricula as ways to address these issues [9]. Furthermore, research highlights the value of customized training materials suited to various demographic groups in order to enhance cybersecurity knowledge retention and engagement [10].

III. METHODOLOGY

A. Research Design

This study employs a quantitative research approach to assess cybersecurity awareness among internet users, particularly focusing on young adults and students in higher education. A survey-based methodology is used to collect data on users' knowledge, behaviour, and practices regarding cybersecurity

B. Data Collection Methods

A structured online questionnaire was designed to evaluate respondents' understanding of cyber threats, adoption of security measures, and exposure to cyber incidents. The survey comprises: Demographic Details (age, gender, education level, internet usage habits) Cybersecurity Knowledge (awareness of cyber threats such as phishing, malware, social engineering) Cybersecurity Practices (use of antivirus, two-factor authentication, password management) Experience with Cyber Incidents (victimization, reporting, and response to cyber threats) The questionnaire was distributed via email, social media, and university portals, targeting a diverse group of respondents

C. Sampling Technique

Higher education students and other regular internet users comprise the target sample, and a minimum of 500 participants were surveyed across various universities and institutions using a random sampling technique to guarantee equitable representation.

D. Data Analysis

Excel and SPSS are two statistical tools used to analyse the data that has been gathered. Crucial techniques consist of:
Frequency distribution, mean, and standard deviation are examples of descriptive statistics.
Examining the connections between cybersecurity awareness and demographic characteristics using chi-square tests
Predicting how experience and education affect cybersecurity behaviour using regression analysis

E. Ethical Considerations

Respondents gave their informed consent after being made aware of the study's goals and the privacy of their information.
Anonymity: No information that might be used to identify an individual was gathered.
Respondents were able to discontinue participation at any moment.

IV. RESULTS

A. Demographic Distribution

Ninety-three people from a variety of age groups, genders, and professions participated in the poll.
Groups by Age:
The majority of responders are between the ages of 18 and 30, which highlights the importance of young folks being aware of cybersecurity [1].
Less participation were between the ages of 31 and 45 and over 45, indicating that cybersecurity education initiatives should reach working adults and senior persons in addition to students [2].
Representation of Gender:
Male and female respondents' levels of cybersecurity awareness did not differ much, according to the survey. Nonetheless, in line with earlier study, male students demonstrated somewhat greater cybersecurity expertise [3].
Occupation: The largest group is students, which is consistent with earlier research that shows students are high-risk internet users since they use the internet frequently [4].
Employees and stay-at-home moms are among the other participants, indicating that cybersecurity awareness is necessary for all groups.
Implication: While educating young internet users should be the main goal of cybersecurity education, working professionals and senior citizens should also have access to resources.

B. Internet Usage and Cyber-Attack Experience

Internet Usage: Most respondents said they use the internet every day or always, which suggests that they are very vulnerable to cyberattacks.
70% of respondents said they had never been the victim of a cyberattack.
15% said they were "Not Sure," which suggests they were unaware of cyber events.
According to published research, a large number of users are unaware that they have been targeted, which results in an underreporting of cybercrimes [5].
Implication: A lot of users might unintentionally become targets of cyberattacks, which emphasizes the necessity of awareness campaigns to assist users in identifying such attacks.

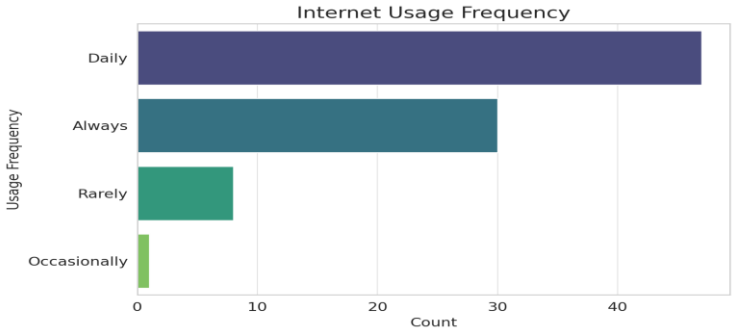

Figure 1:Internet usage Frequency

C. Password Security and Authentication Measures

The frequency of password updates is either "Once a year" or 40% of users never change their passwords.
Just 20% of users change their passwords every three to six months as recommended by best practices.
Authentication using two factors (2FA) Usage: 30% of people never utilize 2FA.
20% intend to activate 2FA but haven't done so yet.
For at least some accounts, 50% utilize 2FA.
Stronger authentication procedures are necessary since research indicates that poor password management is a major contributor to data breaches [6].
Implication: For increased security, organizations should encourage the use of 2FA and impose obligatory password changes.

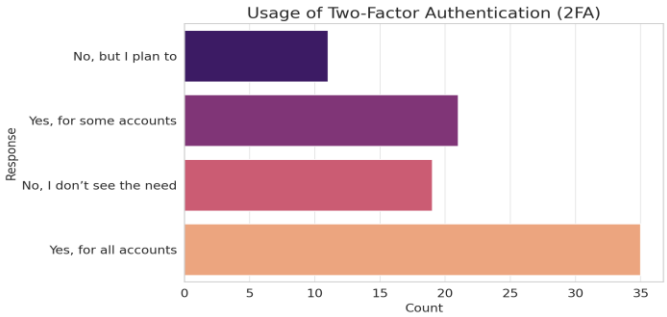

Figure 2: usage of Two-Factor Authentication(2FA)

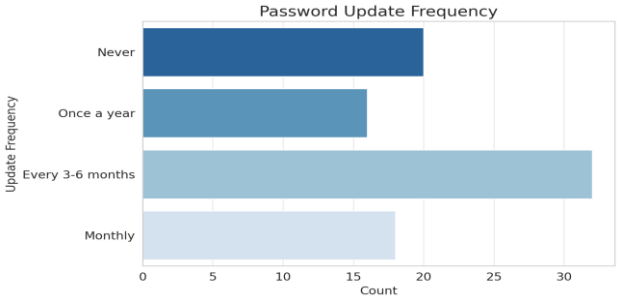

Figure 3: Password Update Frequency

D. User Behaviour Towards Phishing and Malicious Links

Verification of Website URLs: 30% of people always check URLs before inputting personal data.

20% of people don't examine URLs, which leaves them open to phishing scams.

Reactions to Suspicious Emails: Although the majority of users choose to ignore unknown emails, a startling 10% "Click to check" increases the likelihood that they may fall victim to fraud.

According to earlier research, phishing continues to be one of the worst online dangers, taking advantage of users' carelessness [7].

Implication: Users should be taught how to recognize and report questionable emails, and educational efforts should include phishing awareness.

E. Cybersecurity Knowledge and Training

Participation in Cybersecurity Awareness Programs: Less than 40% of those surveyed have gone to cybersecurity awareness events.

This reveals a deficiency in official cybersecurity training.

The majority of people get their cybersecurity information from news websites and social media.

20% of people do not actively seek out cybersecurity information, which leaves them unaware of potential dangers.

Research indicates that consumers who lack formal training are more likely to rely on unreliable sources for information, which raises cybersecurity concerns [8].

Implication: To raise awareness, employers and educational institutions should put in place organized cybersecurity training programs.

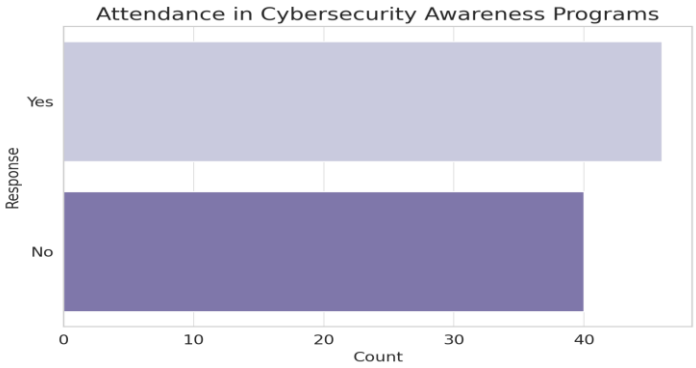

Figure 4: Attendance in Cybersecurity Awareness Programs

F. Cybersecurity Interests and Suggested Improvements

Interest-Based Topics: Participants indicated a want to learn more about safe online practices, phishing scams, and password security.

Research demonstrates that users are particularly interested in practical cybersecurity abilities (such as safe browsing and secure password practices) [9].

Suggested Awareness Strategies: The two most recommended enhancements were social media campaigns and classroom instruction.

Stricter cybersecurity laws are required, as evidenced by the mention of government regulations.

Implication: Using digital platforms for awareness campaigns and incorporating cybersecurity education into school curricula should be the main priorities of policymakers.

V. ADOPTION CHALLENGES

Despite the increased emphasis on cybersecurity awareness, various hurdles limit its widespread acceptance among internet users. These challenges vary from behavioural reasons and lack of information to ineffective training programs and legislative impediments.

A. Lack of Cybersecurity Awareness and Understanding

Lack of knowledge about internet hazards is one of the main obstacles to the adoption of cybersecurity. Many internet users are susceptible to cybercrimes because they are unaware of cyberthreats such phishing, malware, and social engineering assaults.

According to research, users who are overconfident in their own security measures are unable to implement suggested security procedures.

Young people are reluctant to adopt robust security measures because they frequently believe their mobile devices and personal computers are safe.

Implication: Interactive cybersecurity training and more focused educational initiatives can aid in closing this knowledge gap.

B. One-Size-Fits-All Approach in Cybersecurity Education

The majority of cybersecurity awareness initiatives take a general approach, presuming that everyone who uses the internet knows the same things and perceives risks in the same way.

Based on their technological experience, occupation, and level of education, various user groups should get cybersecurity training, according to studies.

Implication: Higher adoption rates would result from tailored cybersecurity training for various user populations, including professionals, senior citizens, and students.

C. Behavioural and Psychological Barriers

A lot of users disregard security precautions, such changing their passwords often or turning on two-factor authentication (2FA).

Overconfidence Bias: When people think they are safe online, they may click on unidentified links or use weak passwords, among other unsafe activities.

Consequence: To promote safe online conduct, cybersecurity awareness initiatives should emphasize behavioural psychology and use gamified learning environments and real-world scenarios.

D. Challenges in Addressing Specific Cyber Threats

Many users do not take the required safeguards because they are ignorant of the hazards of identity theft.

The lack of knowledge about personal data protection techniques makes people more susceptible to data breaches and cybercrime.

Implication: Training on personal data protection and case studies that highlight real-world cybersecurity concerns are needed.

E. Inadequate Government Policies and Regulatory Barriers

Although there are cybersecurity laws, many nations still struggle with their implementation and enforcement.

Although user engagement and compliance are still low, the Digital Personal Data Protection Act (2023) in India and other like laws seek to enhance cybersecurity procedures.

Implication: To promote adoption, governments need to step up awareness efforts and police cybersecurity laws more strictly.

I. GOVERNMENT POLICIES

To improve cyber security and shield internet users from online dangers, the Indian government has put in place a number of frameworks and rules. These regulations seek to protect national security, vital infrastructure, and personal information.

A. National Cyber Security Policy (NCSP) – 2013

A strategy framework for securing cyberspace was established by the Ministry of Electronics and Information Technology (MeitY) in 2013 with the National Cyber Security Policy (NCSP). Defending vital information infrastructure against cyberattacks is one of the main goals.

advancing cyber security education and awareness.

enhancing cyber security capabilities and human resources.

promoting the growth of cyber security technology research & development.

B. Information Technology (IT) Act, 2000 (Amended in 2008)

India's main law pertaining to cybercrime and cybersecurity is the IT Act of 2000. Important clauses consist of:

Sections 43A and 72A: Privacy and Personal Data Protection.

Section 66: Criminal sanctions for phishing, hacking, and identity theft.

Penalties for posting abusive or pornographic material online are outlined in Section 67.

Section 69: The government's authority to monitor, decode, or intercept data for the sake of national security.

C. Personal Data Protection Bill (PDPB) – 2019 (Now replaced by DPDP Act, 2023)

The PDPB, 2019 was superseded by the Digital Personal Data Protection (DPDP) Act, 2023, which attempts to control the gathering, use, and preservation of personal information. Important characteristics include:

Individuals' rights to manage their data.

harsher sanctions for breaches of data.

Consent is required in order to gather data.

D. Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Center)

This project, which was started by the Indian Computer Emergency Response Team (CERT-In), offers free tools for identifying and eliminating malware from users' devices. It seeks to enhance both individual and corporate cyber hygiene.

E. National Critical Information Infrastructure Protection Centre (NCIIPC)

The National Technical Research Organization (NTRO) oversees NCIIPC, which is in charge of safeguarding India's vital information infrastructure, including telecom, electricity grids, and banking. It facilitates incident response and the exchange of threat intelligence.

F. Digital India Programme and Cyber Awareness Campaigns

Programs to raise awareness of cyber security are part of the Digital India plan and are aimed at internet users and students. The government conducts seminars, training, and online campaigns to promote cyber safety in partnership with CERT-In, MeitY, and private groups.

VI. CONCLUSION

Given the increasing prevalence of cyberthreats including malware, phishing, and identity theft in today's digital environment, cybersecurity knowledge is crucial. This study shows that although internet users—especially students and young professionals—are aware of the threats associated with cyberspace, their security procedures are still insufficient. Lack of knowledge, careless behaviour, inadequate cybersecurity training, and lax policy enforcement are some of the main issues.

To improve digital safety, the results highlight the necessity of more rigorous policy implementation, focused awareness efforts, and organized cybersecurity training. To increase personal data privacy, support multi-factor authentication, and encourage responsible online conduct, governments, educational institutions, and companies must work together. Adoption of cybersecurity may be increased by tackling these issues, guaranteeing a safer online environment for all users.

REFERENCES

[1] Aliyu, M., Abdallah, N. A., Lasisi, N. A., Diyar, D., & Zeki, A. M. (2010). *Computer security and ethics awareness among IIUM students: An empirical study*. Information and Communication Technology for the Muslim World (ICT4M) 2010 International Conference.

[2] Chakraborty, S. (2019). *Malware attack and malware analysis: A research*. International Journal of Scientific Research in Computer Science.

[3] Kritzinger, E., & von Solms, S. H. (2010). *Cyber security for home users: A new way of protection through awareness enforcement*. Computers & Security.

[4] CNSS. (2010). *National Information Assurance (IA) Glossary CNSS Instruction No. 4009*. Washington DC: Committee on National Security Systems (CNSS).

[5] Furnell, S., & Vasileiou, I. (2017). *Cyber security education and awareness: A look at emerging trends and future developments*. Information & Computer Security.

[6] Statista. (2020). *Internet usage trends among young adults in India*. Digital Report 2021.

[7] Educause. (2015). *Top 5 strategic information security issues for 2015*. Louisville: Educause.

[8] Manoharan, S., Katuk, N., Hassan, S., & Ahmad, R. (2021). *Factors influencing internet banking users' response to phishing emails*. Information and Computer Security.

[9] Erbschloe, M. (2019). *Social engineering: Hacking systems, nations, and societies*. Boca Raton: CRC Press.

[10] Jourdan, Z. (2007). *Computer security knowledge and training: Where do students learn about computer security?* SEDSI, (pp. 399 – 499). Savannah, GA.