https://doi.org/10.2352/EI.2025.37.3.MOBMU-312

Cybersecurity Awareness Among Young Adults: An Analytical Study

Mahipal Mahipal, Navaneeth Shivananjappa [1]***, Reiner Creutzburg*** [1,2]

[1] ***SRH University, School of Technology and Architecture, Sonnenallee 221, D-12509 Berlin, Germany***
[2] ***Technische Hochschule Brandenburg, Department of Informatics and Media, Magdeburger Str. 50, D-14770 Brandenburg, Germany***

Email: mukuljangra5@gmail.com, navaneeth.shivananjappa@srh.de, reiner.creutzburg@srh.de, creutzburg@th-brandenburg.de

Keywords: Cybersecurity Awareness, Young Adults, Phishing, Two-Factor Authentication, Data Backup, Encryption, Online Privacy

Abstract

This research investigates the cybersecurity awareness of young adults aged 18 to 27 through a structured survey. It evaluates key areas such as phishing recognition, two-factor authentication usage, data backup practices, and knowledge of encryption. The findings indicate that while many participants actively use two-factor authentication, there are notable gaps in understanding encryption and managing privacy settings. Differences in awareness were observed between age groups, with younger individuals displaying lower confidence in technical skills. The results highlight the importance of targeted educational programs to address these knowledge gaps and enhance online safety practices. These initiatives are essential to help young adults strengthen their cybersecurity defenses and protect their personal information in an increasingly digital world. The study underscores the continuous need for education to stay ahead of evolving cyber threats.

Glossary

Encryption: It is a process that transforms data or information into a code to block unauthorized access.

Blockchain: It is a technology that securely records transactions across numerous computers in a decentralized manner.

Phishing: It is a type of cyberattack that involves attackers pretending to be legitimate entities to trick people into disclosing sensitive information.

Malware: It is software created to cause harm, exploit, or compromise computer systems.

Two-Factor Authentication (2FA): It is an additional security measure that goes beyond just a password and username to include something unique to the user, such as information or a physical token.

Identity Theft: Identity theft is when someone dishonestly obtains and uses another individual's identification details, typically to make money.

Cyberbullying: It is the act of using electronic means to intimidate, bully, or harass a person, often through intimidating or threatening messages.

Social Engineering: Social Engineering involves cyber attackers manipulating individuals to reveal personal or confidential information for fraudulent use.

Digital Literacy: It is the skill to efficiently and thoughtfully use various digital technologies to navigate, assess, and produce information.

Privacy Settings: Privacy Settings are configurations that control the visibility of your personal information to others on the internet.

Public Wi-Fi Networks: Public Wi-Fi networks are open to everyone and usually do not have the same level of security as private networks, which can leave them susceptible to cyberattacks.

Cybersecurity: It safeguards systems, networks, and programs to prevent digital attacks that seek to gain unauthorized access, manipulate, or compromise sensitive data.

Introduction

Cybersecurity has become a key priority for individuals and organizations in recent decades due to the increasing use of Information Technologies. Young adults, a population that is particularly susceptible to cyber threats due to the heavy use of digital technologies, are especially vulnerable. The consequences of cyber threats like phishing, malware, and identity theft can be far-reaching, so young adults must be informed of these risks, thereby creating awareness and improving their security posture. This study assesses the perception of 18-27-year-old young adults from SRH Berlin University of Applied Sciences, Berlin, Germany; BML Munjal University, Gurugram, India; and CMR University, Bangalore, India regarding their level of knowledge and adherence to some of the fundamental practices of cybersecurity. Through this survey, it is possible to determine their existing knowledge, uncover their weak spots, and create specific programs for enhancing their cybersecurity preparedness.

This research aims to assess the level of cybersecurity knowledge among young people between the ages of 18 and 27, including their attitudes and behavior concerning proven cybersecurity paradigms. From their existing level of awareness, potential training strategies to strengthen their cybersecurity defenses can be determined.

Objectives

The main objective of this research is to determine the Cybersecurity awareness levels of young adults aged 18-27. Ideally, the research would like to know their awareness of high-priority areas like phishing emails, two-factor authentications, data backups, password management, and concepts like encryption. Thus, the researchers would like to know what they may lack regarding Cybersecurity awareness levels, which will help establish its modern state.

Literature Review

The growing dependence on digital technologies among young adults, particularly university students, has made cybersecurity awareness a crucial concern. Despite being proficient with technology, many young adults lack sufficient knowledge of cyber threats such as phishing, identity theft, and malware, which puts them at significant risk [1]. Research has shown that despite cybersecurity awareness, many young adults still engage in risky behaviors like using weak passwords or failing to recognize phishing attempts [2][3].

The role of education in enhancing cybersecurity awareness is crucial. Various studies emphasize the need for targeted educational interventions to address specific gaps in knowledge. For instance, many young adults are unfamiliar with key concepts like encryption and data backup, essential for protecting personal information online[1][4]. Game-based learning platforms and educational campaigns have been proposed as effective methods to improve understanding and retention of cybersecurity practices[5][6].

Furthermore, the literature suggests that attitudes toward cybersecurity perceived behavioral control, and social influences play significant roles in shaping cybersecurity behaviors [4]. Even when students have basic knowledge, these factors can lead to complacency or risky online behaviors [1].

Information sharing is another critical aspect of cybersecurity awareness. Reference [7] highlights the importance of establishing robust information-sharing mechanisms, such as Information Sharing and Analysis Centers (ISACs), to enhance cybersecurity resilience. These platforms can help disseminate crucial information across various sectors, improving cybersecurity preparedness.

In conclusion, while efforts have been made to increase cybersecurity awareness among young adults, significant gaps remain, particularly in technical areas like encryption and data protection. Continuous education and the development of tailored interventions are necessary to close these gaps and promote safer online practices among this vulnerable demographic[1]

Methodology

This study employed a quantitative research approach to evaluate the cybersecurity awareness of young adults aged 18-27. The survey was conducted online using the platform CyberSurvey, targeting a sample of 100 participants selected based on their age to ensure representation of this demographic.

The survey consisted of 15 questions, carefully designed to cover critical aspects of cybersecurity that are particularly relevant to young adults. These questions were chosen to assess critical areas of cybersecurity behavior [1][2][5] and awareness without following a specific predefined framework. The questions addressed several important topics, including Phishing Scam Identification and Two-Factor Authentication. These areas are critical for understanding how young adults manage common vulnerabilities.

Additionally, the survey explored other significant aspects of cybersecurity, such as Data Backups, Encryption, and Social Media Privacy Settings, to evaluate how respondents protect their data and online presence[2]. Questions were also included on using Public Wi-Fi Networks, recognizing Social Engineering Attempts, and verifying Website Authenticity, which is crucial for assessing the ability to navigate risky situations and prevent fraud[6]. Other topics such as Reading Terms and Conditions, Familiarity with Blockchain Technology, Sharing Location Data Online, and Managing Cookie Settings were also examined to understand privacy practices and awareness of emerging technologies.

The data collected from the survey was analyzed with the Likert scale[8] to measure responses to identify patterns and trends in cybersecurity awareness and practices among the participants. This analysis helped highlight areas where young adults demonstrate strong cybersecurity practices and areas that require improvement. The findings from this study aim to inform the development of targeted educational interventions to enhance cybersecurity readiness and resilience among young adults[9][10].

Results

The survey had 68 respondents, with 57 participants falling within the desired age range of 18-27 years. The age distribution of the respondents is presented in Table 1 below.

Age	Number of Participants
18	7
19	7
20	10
21	3
22	5
23	9
24	2
25	6
26	4
27	4

Table 1: Age distribution of participants

Gender	Number of Participants
Male	52
Female	5

Table 2: Gender distribution among participants aged 18-27

The gender distribution of the respondents is presented in Table 2 below. This distribution provides a well-rounded representation of young adults in their early twenties, mainly focusing on those in their early twenties. Meanwhile, the gender distribution showed that many respondents were male. The balanced spread of ages within this group ensures that the survey results are relevant and provide a comprehensive insight into this key demographic's cybersecurity practices and awareness levels.

The survey results provide a comprehensive overview of cybersecurity awareness among the respondents:

How often do you update your passwords?

45% of the respondents change their passwords frequently or very frequently. However, 40% said they infrequently or never change their passwords. This indicates that more awareness about password standards and the frequency of changes among young adults is required.

How comfortable are you with identifying phishing emails?

60% of the surveyed individuals were very or moderately comfortable identifying phishing emails. However, 35% are uncomfortable or not at all comfortable with identifying phishing emails, with lower confidence in the 18-21 age group.

How frequently do you use two-factor authentication?

75% of respondents use two-factor authentication frequently, showcasing strong adoption of this security measure, especially in the 22-24 age group. However, 25% use it rarely or never, indicating possible vulnerability, particularly in the 18-21 age group.

How confident are you in your ability to protect your data online?

60% of respondents are very or moderately confident in protecting their data online. However, 40% are slightly or not at all confident, suggesting a need for enhanced education, especially in the 25-27 age group with the lowest confidence levels.

How often do you check app permissions before installing?

65% of the respondents frequently check app permissions, indicating good awareness. However, 15% rarely or never do, emphasizing the importance of increasing awareness, particularly in the 18-21 age group.

How familiar are you with encryption concepts?

Only 15% of respondents are very familiar with encryption concepts, while 50% are slightly or not at all familiar, indicating a significant knowledge gap, most pronounced in the 18-21 age group.

How often do you back up your data?

55% of respondents back up their data often or always, showing a basic understanding of the importance of data backup. However, 20% rarely or never do, pointing to a need for improvement.

How comfortable are you configuring social media privacy settings?

55% of respondents feel very or moderately comfortable configuring privacy settings, whereas 45% are only slightly or not at all comfortable. This indicates a need for better education on privacy controls, especially among the 18-21 age group.

How frequently do you use public Wi-Fi networks?

55% of respondents use public Wi-Fi sometimes or often, posing potential security risks. Only 15% never use public Wi-Fi, suggesting the need for increased awareness about its dangers, particularly among the 22-24 age group.

How confident are you in recognizing social engineering attempts?

65% of respondents are very or moderately confident in recognizing social engineering attempts, while 35% are slightly or not at all confident. This highlights the need for practical training, especially among the 18-21 age group.

How often do you read terms and conditions before accepting?

Only 35% of respondents often or always read terms and conditions, indicating a general neglect of understanding service agreements. 40% rarely or never read them, suggesting a need for increased attention to this area, particularly in the 25-27 age group.

How familiar are you with blockchain technology?

Awareness of blockchain technology is low, with only 12% very familiar. 62% are slightly or not familiar, highlighting the need for better education, particularly among the 18-21 age group.

How frequently do you share your location data online?

A majority (65%) of respondents rarely or never share their location data, which is a positive trend for privacy. However, 35% share their location data sometimes or often, suggesting some privacy concerns, especially in the 22-24 age group.

How comfortable are you with managing cookie settings in your browser?

Only 42% of respondents feel very or moderately comfortable managing cookie settings, indicating a need for better education. 58% are slightly or not at all comfortable, showing significant room for improvement, particularly in the 18-21 age group.

How often do you verify the authenticity of websites before entering sensitive information?

62% of respondents frequently verify website authenticity, a positive security practice. However, 18% rarely or never do, indicating a need for increased awareness and caution, especially in the 18-21 age group.

Fig.1 visually represents the cybersecurity awareness survey results. It shows the percentage of positive and negative responses for each key finding (A., B., C., etc.). The chart highlights areas where respondents are generally well-versed, such as using two-factor authentication, and areas needing improvement, like familiarity with encryption concepts.

Fig.2 illustrates the comparative cybersecurity awareness across three age groups: 18-21, 22-24, and 25-27. Each age group shows varying positive responses to the survey questions (A., B., C., etc.), highlighting differences in cybersecurity practices and confidence among the different age cohorts. This helps identify which age groups may need more targeted cybersecurity education and awareness programs.

Findings

This study examined cybersecurity awareness among individuals aged 18-27, shedding light on the subtle differences in cybersecurity behavior within this group. The 22-24 age group was found to have the highest levels of cybersecurity awareness

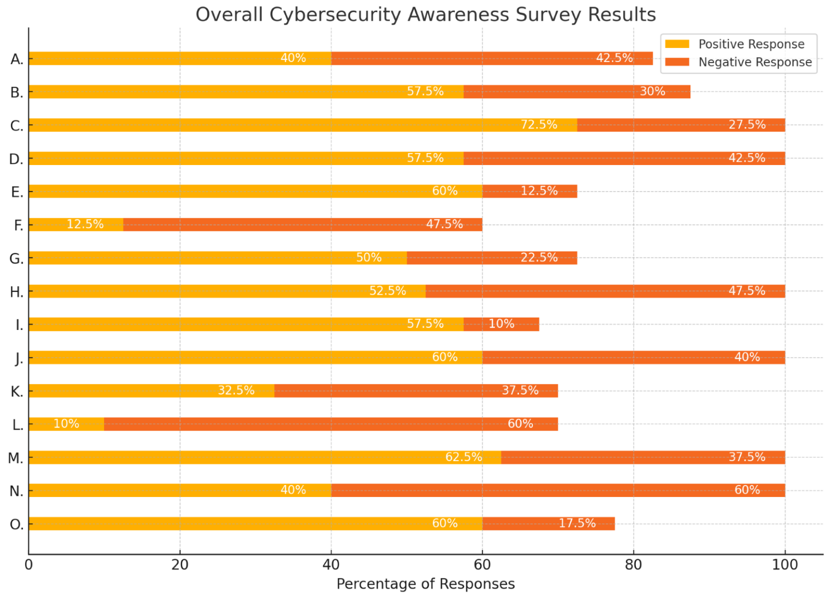

Figure 1: Survey Results

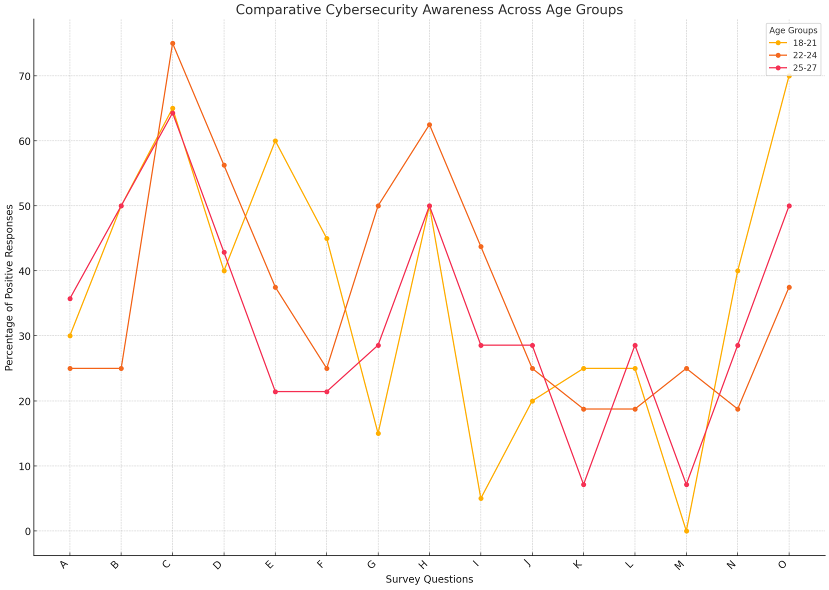

Figure 2: Comparative Cybersecurity Awareness

based on the positive responses to each of the questions in the survey, closely followed by the 18-21 age group. Awareness tends to decrease slightly, particularly in the 25-27 age range 2.

The study found that the 22-24 age group had the highest levels of cybersecurity awareness, showing strong engagement with practices like two-factor authentication and phishing identification. In contrast, while also aware, the 18-21 age group exhibited less familiarity with technical concepts such as encryption. The 25-27 age group showed a slight decline in awareness, suggesting a possible shift in focus or priorities as individuals move further into adulthood[11]. These differences highlight the varying levels of cybersecurity awareness and the need for targeted educational efforts across different age groups.

Calculation of Average Awareness per Age Group

In Fig. 3 each respondent's answer to the survey questions was converted into a numeric value based on a 5-point Likert scale, as follows:

Never = 1 Rarely = 2 Sometimes = 3 Often = 4 Always = 5
Not at all = 1 Slightly = 2 Moderately = 3 Very = 4 Extremely = 5

For each respondent, the Likert scale scores for all questions were averaged to create a single "Average Awareness per Age Group." This average calculates how vigilant and aware each individual is based on their survey responses.

25-27 Age Group had the highest average score. 22-24 Age Group followed closely behind, showing strong but slightly lower awareness. 18-21 Age Group had the lowest average score, although they still demonstrated good awareness, particularly in basic cybersecurity practices.

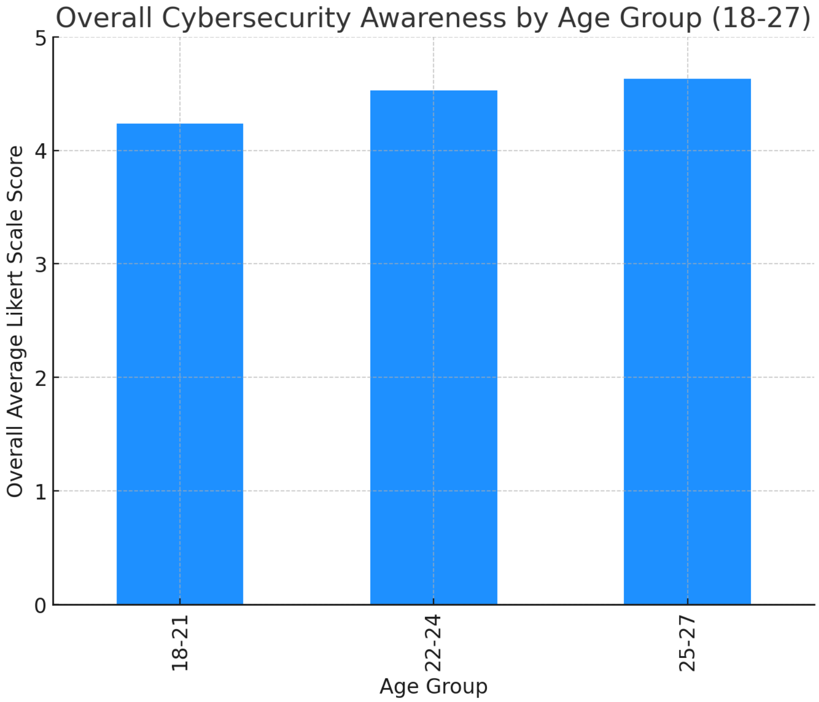

Figure 3: Calculation of Average Awareness per Age Group

Correlation Between Age and Cybersecurity Awareness

The Fig. 4 with a trend line illustrates the relationship between age and cybersecurity awareness for individuals aged 18-27. Each point represents a participant, showing their age on the x-axis and the number of positive cybersecurity practices on the y-axis. The upward-sloping trend line indicates a general increase in awareness as age rises.

However, there's noticeable variability, with some younger participants showing high awareness and some older participants showing less. Overall, the plot suggests that while age correlates with better cybersecurity practices, individual differences also play a significant role.

Influence of Specific Factors on Cybersecurity Behavior

Fig.5 shows how different age groups score across various cybersecurity practices, highlighting each group's strengths and weaknesses.

The average scores for each cybersecurity practice are plotted on the axes of the radar chart. Each age group is represented by a different line, allowing for comparison across different cybersecurity behaviors. The area enclosed by the line represents the overall strength or weakness of the group's cybersecurity practices.

The radar chart shows that older participants (25-27) have a more advanced understanding of cybersecurity practices than younger groups. The 18-21 age group consistently scores lower across several categories, particularly in technical areas such as encryption and privacy settings. Educational interventions targeting the younger groups could help bridge these gaps and enhance cybersecurity awareness.

Regression Analysis of Influential Factors

Fig. 6 The plot visualizes the coefficients from the regression analysis. Each bar represents the strength of the influence of a specific factor on overall cybersecurity awareness. The longer the bar, the more significant the impact of that factor.

The R-squared value of 0.46 means these factors explain about 46% of the overall cybersecurity awareness variance. This suggests that while these factors are significant, other variables not included in the model could also influence cybersecurity awareness.

The coefficient plot reveals that confidence in protecting personal data is the most influential factor impacting cybersecurity awareness. Additionally, familiarity with blockchain technology and comfort with configuring privacy settings are significant contributors. This suggests that improving users' confidence in data protection and boosting their technical knowledge of emerging technologies can enhance their overall cybersecurity behavior. Conversely, while checking app permissions has a lesser impact, it still raises awareness.

Recommendations

These findings emphasize the need for cybersecurity education programs to focus on increasing user confidence and technical expertise, which could lead to better cybersecurity habits and more robust protection against threats.

Adaptive training programs for Cybersecurity Awareness:

Adaptive training programs that utilize engaging methods, such as gamification, can be employed to reinforce learning. The

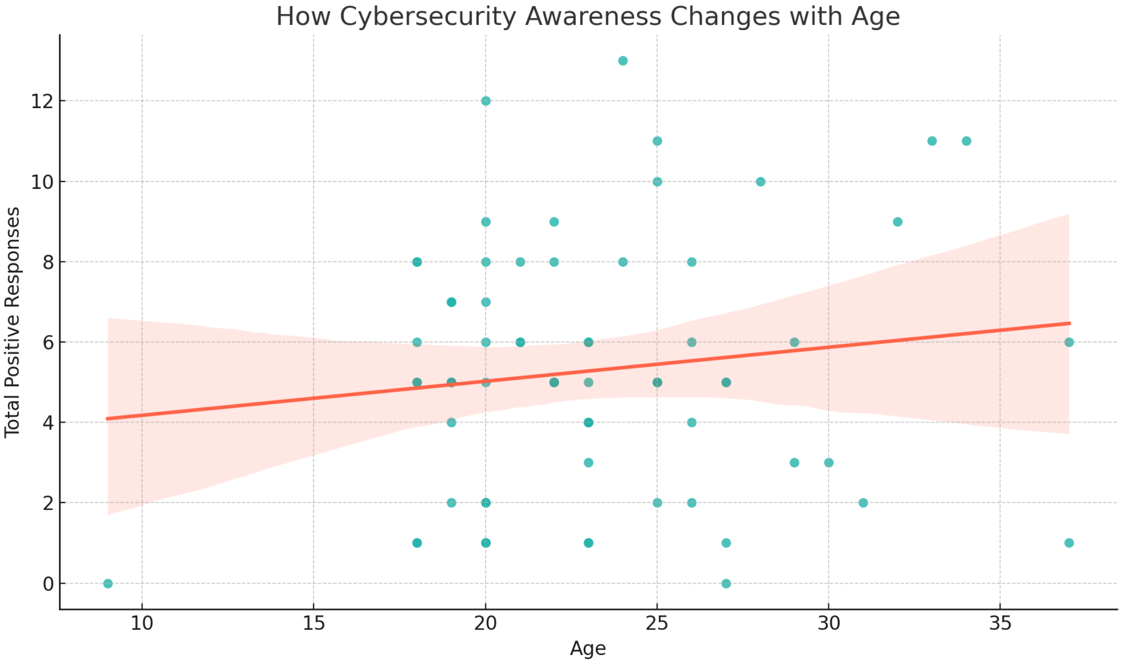

Figure 4: Correlation Between Age and Cybersecurity Awareness

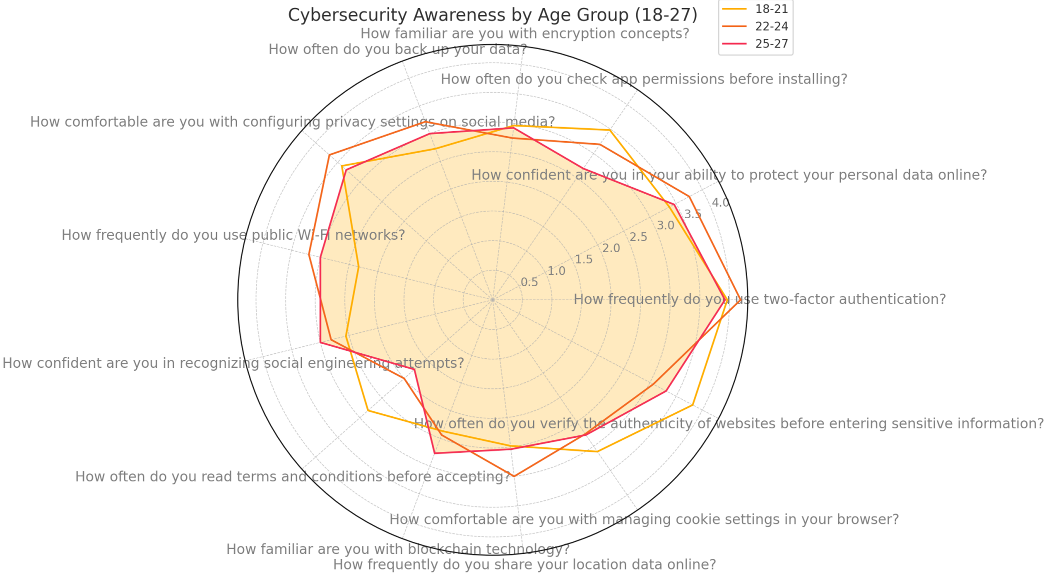

Figure 5: Awareness by Specific Factors

essential components are continuous evaluation and integration of psychological principles to encourage positive behavior change. This strategy can lead to significant improvements in cybersecurity practices and reduce vulnerabilities within this demographic [9].

Gamification-Based Cybersecurity Awareness Course for Self-regulated Learning:

It encourages self-regulated learning by integrating game elements to enhance user engagement and motivation. The course presents interactive content, quizzes, and challenges through platforms like Moodle to promote active learning. Game elements like points, badges, and leaderboards drive engagement, while practical exercises help learners identify and prevent cybersecurity threats. This approach aims to build cybersecurity knowledge and learners' ability to manage their learning independently[10].

Future Work

For future work, the research aims to conduct a detailed survey on cybersecurity awareness among young adults aged 18-27 in technical and non-technical domains. This will help uncover areas where these young adults may lack essential cybersecurity knowledge. The same knowledge base will be enhanced with a Gamification-Based Cybersecurity Awareness Course for Self-

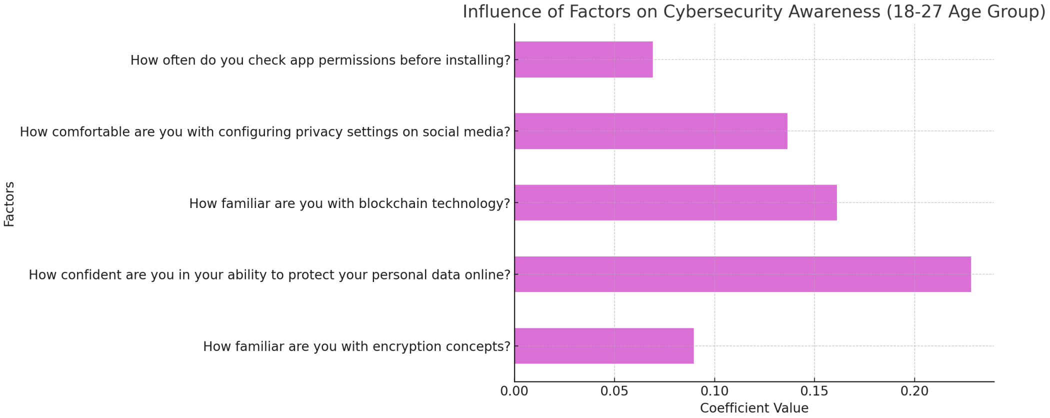

Figure 6: Awareness by Influential Factors

regulated Learning [10]. Finally, the improvement among the nontechnical groups will be measured with the same survey.

Conclusion

This study offers valuable insights into the cybersecurity awareness of young adults aged 18-27. The findings show that while many participants have adopted basic security practices, such as using two-factor authentication, significant gaps exist in more complex areas like encryption, social media privacy settings, and phishing recognition. The 22-24 age group demonstrated the highest levels of cybersecurity awareness, while the youngest (18-21) and oldest (25-27) age groups showed lower familiarity with key cybersecurity concepts.

These results highlight the need for targeted educational interventions, mainly focusing on technical areas lacking awareness. Educational strategies such as gamified learning and personalized training can help address these gaps. By improving knowledge and promoting secure online behaviors, young adults can enhance their ability to protect their data and digital privacy.

Overall, this research emphasizes the importance of continuous education to strengthen cybersecurity preparedness among young adults and reduce vulnerabilities in their online practices.

Acknowledgments

This work was supported partially by the European Union in the framework of ERASMUS MUNDUS, Project CyberMACS (Project #101082683) (`https://cybermacs.eu`). We want to extend our warm regards to Sam Soney Chemparathy for his support with peer review.

References

[1] G. Muhammad, A. R. Pratama, C. Shaloom, and C. Cassandra, ”Cybersecurity awareness literature review: A bibliometric analysis,” in *2023 International Conference on Informatics, Multimedia, Cyber and Information Systems (ICIMCIS)*, Jakarta Selatan, Indonesia, 2023, pp. 195-199.

[2] Z. B. Abdullah, N. B. M. Dahlan, A. B. Dahlan, A. F. I. Bin, and A. S. Arifin, ”Cybersecurity awareness on personal data protection using game-based learning,” *Information Management and Business Review*, vol. 15, no. 3(I), pp. 497-503, Oct. 2023.

[3] B. Ahamed, A. Rahman, S. Ghosh, and T. K. Roy, ”Empowering students for cybersecurity awareness management in the emerging digital era: The role of cybersecurity attitude in the 4.0 industrial revolution era,” *SAGE Open*, vol. 14, no. 1, Jan. 2024.

[4] M. Alanazi, M. Freeman, and H. Tootell, ”Exploring the factors that influence the cybersecurity behaviors of young adults,” *Computers in Human Behavior*, vol. 136, p. 107376, Nov. 2022.

[5] N. A. Badela, ”Fostering cybersecurity consciousness: Assessing awareness among students and staff in a technical institution,” *International Journal of Modern Trends in Social Sciences*, vol. 7, no. 27, pp. 26-39, Jun. 2024.

[6] S. Back and R. T. Guerette, ”Cyber place management and crime prevention: The effectiveness of cybersecurity awareness training against phishing attacks,” *Journal of Contemporary Criminal Justice*, vol. 37, no. 3, pp. 427-451, Mar. 2021.

[7] S. Ghernaouti, L. Cellier, and B. Wanner, ”Information sharing in cybersecurity: Enhancing security, trust and privacy by capacity building,” in *2019 3rd Cyber Security in Networking Conference (CSNet)*, Quito, Ecuador, 2019, pp. 58-62.

[8] J. Robinson, ”Likert scale,” in *Springer eBooks*, 2014, pp. 3620-3621.

[9] A. A. Maqousi, ”A proposed framework for user cybersecurity awareness,” in *2023 24th International Arab Conference on Information Technology (ACIT)*, Ajman, United Arab Emirates, 2023, pp. 1-6.

[10] T. M. Tran, R. Beuran, and S. Hasegawa, ”Gamification-based cybersecurity awareness course for self-regulated learning,” *International Journal of Information and Education Technology*, vol. 13, no. 4, pp. 724-730, Jan. 2023.

[11] J. L. Tanner and J. J. Arnett, ”Presenting ’emerging adulthood’: What makes it developmentally distinctive?,” in *Oxford University Press eBooks*, 2011, pp. 13-30.

Author Biography

Mahipal completed his Master’s in Computer Science with a focus on Cybersecurity at SRH Berlin University of Applied Sciences, Berlin School of Technology. He specializes in AI-driven phishing detection, Business Logic Exploitation Vulnerabilities, Penetration Testing, Web Application Security, and Cybersecurity

Awareness.

Navaneeth Shivananjappa is a Lecturer at SRH University of Applied Sciences, Berlin School of Technology and Architecture, specializing in the field of Web Application Pentesting and Cyber Security. His research interests include Cybersecurity, Cybersecurity tools, Penetration Testing, Web Application Security, Kubernetes Security, Cloud Security, and Cybersecurity Awareness.

Reiner Creutzburg is a Retired Professor for Applied Computer Science at the Technische Hochschule Brandenburg in Brandenburg, Germany. Since 2019, he has been a Professor of IT Security at the SRH Berlin University of Applied Sciences, Berlin School of Technology. He is a member of the IEEE and SPIE and chairman of the Multimedia on Mobile Device (MOBMU) Conference at the Electronic Imaging conferences since 2005. In 2019, he was elected a member of the Leibniz Society of Sciences to Berlin e.V. His research interests include Cybersecurity, Digital Forensics, Open Source Intelligence (OSINT), Multimedia Signal Processing, eLearning, Parallel Memory architecture, and Modern Digital Media and Imaging Applications.

JOIN US AT THE NEXT EI!

electronic IMAGING

Imaging across applications . . . Where industry and academia meet!

• SHORT COURSES • EXHIBITS • DEMONSTRATION SESSION • PLENARY TALKS •
• INTERACTIVE PAPER SESSION • SPECIAL EVENTS • TECHNICAL SESSIONS •

www.electronicimaging.org