International Journal Of
Digital Trends And
Youth Development
VOL 01 | No. 1 | 2026
P-I-SSN: XXXXXXXXXX | E-I-SSN: XXXXXXXXXX

CYBERSECURITY AWARENESS AND DIGITAL PRIVACY CHALLENGES AMONG YOUNG PEOPLE

Kinza Abdul Star
BS, Department of English, The Cosmic Degree College (For Women) ,University of Okara

ABSTRACT

The rapid expansion of digital technologies, social media platforms, online gaming, mobile applications, and artificial intelligence has transformed how young people communicate, learn, socialize, and access information. However, increased digital participation has also exposed young people to cybersecurity threats and digital privacy challenges, including phishing, identity theft, account hacking, cyberbullying, online scams, unauthorized data collection, and misuse of personal information. This study examines cybersecurity awareness and digital privacy challenges among young people, focusing on their knowledge of online threats, privacy management practices, digital behaviors, and access to cybersecurity education. Recent research indicates that young people may understand basic online safety principles while experiencing difficulties applying this knowledge consistently in everyday digital environments. The study adopts a proposed mixed-methods research design combining a structured questionnaire with semi-structured interviews to explore the relationship between cybersecurity knowledge, privacy concerns, and protective online behavior. The research also considers the roles of educational institutions, parents, social media platforms, and government policies in promoting safer digital practices. Because no original survey or interview data have been provided, the findings section presents an evidence-informed synthesis of existing research and anticipated themes rather than claiming results from completed fieldwork. The study is expected to contribute to a better understanding of the awareness–behavior gap and to support practical recommendations for strengthening cybersecurity education, improving privacy literacy, and encouraging responsible digital citizenship among young people.

KEYWORDS: *Cybersecurity awareness, digital privacy, young people, adolescents, online safety, cyber threats, social media, phishing, privacy literacy, digital citizenship, data protection, cybersecurity education, online behavior, personal information security.*

INTRODUCTION

Digital technology has become an essential part of young people's everyday lives. Smartphones, social networking platforms, online learning environments, digital payment services, gaming applications, and artificial intelligence tools provide opportunities for education, entertainment, communication, and personal development. Young people increasingly depend on digital platforms to maintain relationships, obtain information, participate in social activities, and develop professional skills. Nevertheless, frequent internet use does not automatically guarantee that individuals possess the knowledge and practical skills required to protect themselves online. Al-Saggaf, Y., & Maclean, J. (2024, December). found that The United Nations Children's Fund (UNICEF, 2024) emphasizes that expanding digital access creates important opportunities for children while also increasing exposure to privacy risks, harmful content, and exploitation. Consequently, cybersecurity awareness and digital privacy have become important concerns for educational institutions, families, technology providers, and policymakers.Young people encounter a range of cybersecurity threats that may affect their personal information, financial security, online relationships, and psychological well-being. Common threats include phishing messages, fraudulent websites, malicious applications, stolen passwords, compromised social media accounts, impersonation, and online scams. Cybercriminals may exploit curiosity, trust, urgency, peer pressure, or the desire to obtain rewards to persuade users to disclose sensitive information or

International Journal Of
Digital Trends And Youth Development
VOL 01 | No. 1 | 2026
P-I-SSN: XXXXXXXXXX | E-I-SSN: XXXXXXXXXX

click unsafe links. The growing use of artificial intelligence also creates additional challenges because fabricated messages, manipulated images, and convincing impersonation attempts may become harder to recognize. Although these threats affect internet users of different ages, young people may face distinctive risks because digital participation is closely connected to social acceptance, identity development, education, and entertainment. Understanding these threats is therefore essential for developing effective and age-appropriate cybersecurity education.

Digital privacy refers to an individual's ability to understand, manage, and exercise appropriate control over the collection, use, sharing, and retention of personal information. Young people routinely share photographs, videos, location information, personal opinions, educational details, and relationship updates through digital platforms. Information shared for immediate social purposes may remain accessible, be copied by other users, or be processed by platforms for advertising, recommendation systems, and other commercial purposes. Privacy challenges also arise from default account settings, extensive application permissions, third-party tracking, and limited understanding of privacy notices. Research on adolescents' perceptions of digital privacy indicates that young people's understanding of privacy can involve several dimensions, including control over information, personal boundaries, and the consequences of data disclosure (Vespoli et al., 2024/2025). Therefore, digital privacy should be understood as both an individual responsibility and a matter of platform design and institutional accountability.An important problem in cybersecurity research is the difference between knowing about online risks and consistently adopting protective behavior. Explained that A young person may recognize that passwords should remain confidential but still reuse the same password across several accounts. Similarly, an individual may understand the importance of privacy settings while maintaining a public profile to increase visibility or social engagement. These inconsistencies may result from convenience, limited technical knowledge, social pressure, insufficient time, confusing platform interfaces, or the belief that serious threats are unlikely to occur personally. Research by Williams, Choong, and Buchanan (2023) found that young participants could describe basic online privacy and security concepts, while also identifying the importance of how parents communicate with them about digital risks. These findings suggest that cybersecurity awareness should not be measured only through factual knowledge; it should also consider practical decision-making and the conditions that support secure behavior.

Cybersecurity education can help young people recognize suspicious communications, protect personal information, configure privacy settings, create stronger passwords, enable multifactor authentication, and report harmful online activity. However, effective education should extend beyond occasional lectures or general warnings. Young people need practical opportunities to identify phishing attempts, evaluate application permissions, respond to account compromise, understand digital footprints, and assess the reliability of online information. Al-Saggaf and Maclean (2024), in their research on a targeted cybersecurity intervention in secondary schools, reported improvements in students' knowledge of smartphone privacy settings and greater awareness of potential information leakage. This supports the value of practical and context-specific educational interventions. Schools, universities, families, youth organizations, and technology providers can contribute by offering consistent guidance and creating environments in which young people feel comfortable asking questions and reporting incidents.Despite increasing attention to online safety, questions remain about how young people understand cybersecurity risks, which

International Journal Of
Digital Trends And Youth Development
VOL 01 | No. 1 | 2026
P-I-SSN: XXXXXXXXXX | E-I-SSN: XXXXXXXXXX

privacy-protection practices they actually use, and what prevents them from applying their knowledge consistently. These issues are especially important in contexts where digital literacy education, access to trusted guidance, and institutional support may differ substantially among communities. The present study therefore examines cybersecurity awareness and digital privacy challenges among young people, with particular attention to knowledge, attitudes, protective behaviors, educational experiences, and perceived barriers. It aims to provide an integrated framework for understanding the relationship between cybersecurity awareness and responsible digital participation. The study may help educators develop relevant learning materials, assist parents in supporting safer digital habits, and inform policymakers and digital service providers about the importance of accessible privacy controls and youth-centered protection measures.

RESEARCH QUESTION

1. What is the relationship between cybersecurity awareness and digital privacy-protection practices among young people, and what factors influence their ability to recognize and respond to online security and privacy threats?

RESEARCH OBJECTIVES

1. To assess young people's awareness and understanding of common cybersecurity threats and digital privacy risks.

LITERATURE REVIEW

Cybersecurity awareness refers to an individual's knowledge of digital threats, understanding of protective measures, and ability to make informed decisions when using digital technologies. It includes recognizing suspicious links, understanding malware and phishing, securing online accounts, protecting devices, identifying fraudulent communications, and responding appropriately to security incidents. Among young people, cybersecurity awareness is particularly important because digital technologies are integrated into educational, social, and recreational activities. However, awareness is not a single skill; it includes knowledge, attitudes, risk perception, confidence, and the practical ability to apply security principles. Botturi, L., Fioroni, T., Beretta, C., Andreoletti, D., Ferrari, A., Cardoso, F., ... & Giordano, S. (2024). Explains that Williams et al. (2023) investigated how young people understand online privacy and security through interviews with 40 youth–parent pairs in the United States. Their findings indicated that participants could explain basic privacy and security concepts, but the depth of their understanding varied. The study also highlighted the importance of communication between parents and children in developing nuanced understandings of online risks. These findings suggest that cybersecurity awareness should be treated as a developmental and educational process rather than an ability acquired automatically through frequent internet use. Research published in 2025 also demonstrates the need to assess cybersecurity awareness in relation to actual student experiences. Azad (2025) examined online privacy and cybersecurity awareness among 353 college students in Bangladesh. The study reported limited knowledge of fundamental cybersecurity concepts despite frequent social media use and personal information sharing. It also identified

International Journal Of
Digital Trends And Youth Development
VOL 01 | No. 1 | 2026
P-I-SSN: XXXXXXXXXX | E-I-SSN: XXXXXXXXXX

relationships between information-sharing behavior, experiences of cyberattacks, and students' ability to respond to incidents. These findings are relevant to understanding young people in environments where digital participation is expanding faster than formal cybersecurity education. They suggest that awareness programs should address specific online situations instead of relying exclusively on general explanations of digital safety. Students should be taught how to evaluate messages, identify suspicious requests, protect account recovery information, and respond when their accounts are compromised.

Cybersecurity awareness should also be evaluated in relation to the context in which young people use digital services. For example, a student using an educational platform may face different risks from someone participating in online gaming or sharing content on social media. Educational platforms may expose users to fraudulent links, insecure file-sharing practices, and account misuse, whereas social media can increase exposure to impersonation, privacy violations, and social engineering. Awareness programs should therefore consider the digital environments young people actually use. Effective cybersecurity education should combine foundational concepts with realistic examples and practical exercises, enabling students to transfer knowledge across different applications and circumstances.Digital privacy literacy concerns the ability to understand how personal information is collected, processed, stored, shared, and potentially reused by digital platforms. Corcoran, E., Clement, A., & Gabrielli, J. (2024). revealed that It includes understanding privacy settings, evaluating application permissions, recognizing data-sharing practices, and making informed choices about the information disclosed online. Privacy literacy differs from general internet familiarity because a user may navigate applications confidently without understanding how personal data are used. Young people frequently encounter lengthy privacy policies, complicated consent notices, default sharing settings, and personalized recommendations that make data practices difficult to understand. Consequently, effective privacy education should explain both immediate risks, such as public disclosure of a telephone number, and less visible risks, such as the aggregation of browsing activity and behavioral information.Vespoli et al. (2024; issue publication 2025) explored how teenagers conceptualize online privacy and understand the implications of their data being available digitally. Their research contributes to the argument that privacy is not merely a technical matter; it also involves personal boundaries, control, expectations, and interpretations of information sharing. Teenagers may understand privacy in relation to who can view their photographs or messages while having less developed knowledge of the broader systems through which platforms collect and use information. Such differences can create a gap between perceived privacy and the actual exposure of personal information.

Corcoran, Clement, and Gabrielli (2024) examined a measurement model of online privacy cognitions among adolescents in the United States. Their work is important because it treats privacy-related thinking as a multidimensional construct that can be studied systematically. Measuring privacy cognition can help researchers distinguish between concern about data collection, beliefs about control, knowledge of privacy risks, and the decisions individuals make online. For the present research, this distinction is useful because young people may express strong privacy concerns without possessing the skills needed to change account settings or reduce unnecessary data disclosure. Privacy education should therefore be evaluated using both knowledge-based questions and behavior-oriented measures.Digital privacy literacy also requires an understanding of the permanence and circulation of online

International Journal Of
Digital Trends And Youth Development
VOL 01 | No. 1 | 2026
P-I-SSN: XXXXXXXXXX | E-I-SSN: XXXXXXXXXX

information. Photographs, comments, location details, and personal disclosures can be copied, redistributed, or preserved beyond their original context. Information intended for a small group of friends may reach strangers, future employers, educational institutions, or malicious actors. De Wolf, R., Martens, M., Vanden Abeele, M., & De Marez, L. (2023). Elaborated on Young users should consequently learn to consider the audience, purpose, sensitivity, and potential future consequences of online disclosures. These skills can be strengthened through practical exercises that examine real-world privacy scenarios without collecting students' actual passwords, private messages, or sensitive personal information.A central issue in the literature is that cybersecurity knowledge does not necessarily produce consistent protective behavior. Users may recognize the importance of strong passwords but reuse credentials because remembering multiple passwords is inconvenient. They may know that unfamiliar links are dangerous but click them when a message appears to come from a trusted friend or offers an attractive reward. Likewise, users may understand the importance of account privacy but choose public settings to increase visibility or social engagement. These behaviors demonstrate that cybersecurity decisions are influenced by convenience, social expectations, perceived risk, confidence, and the design of digital services.

RESEARCH DESIGN

The proposed study will employ a mixed-methods research design to investigate cybersecurity awareness and digital privacy challenges among young people. A mixed-methods approach is appropriate because the research problem includes measurable factors, such as cybersecurity knowledge and privacy-protection practices, as well as personal experiences, attitudes, and explanations that require qualitative interpretation. The quantitative component will assess participants' understanding of phishing, password security, multifactor authentication, suspicious links, account privacy, application permissions, personal information sharing, and incident reporting. The qualitative component will explore how young people interpret online risks, why they make particular privacy decisions, and how family guidance, educational experiences, social expectations, and platform features influence their behavior. The study will target young people aged 15–24, with participants recruited from secondary schools, colleges, and universities. A proposed sample of approximately 300 questionnaire respondents and 15–20 interview participants will provide a practical starting point, subject to institutional approval, available resources, and a preliminary power or feasibility assessment. The quantitative sample will be recruited using stratified sampling where reliable sampling frames are available; otherwise, a clearly documented multistage or convenience-based recruitment procedure may be used, with limitations acknowledged. Interview participants will be selected purposively to represent different levels of cybersecurity knowledge, educational backgrounds, and online experiences. The study will follow an explanatory sequence in which questionnaire results guide the selection of interview topics and participants, allowing qualitative evidence to help explain quantitative patterns. The research design will be cross-sectional because information will be collected during a defined period rather than through repeated observations over several years. Although this design can identify associations and differences among groups, it cannot independently establish causal relationships or determine whether observed behaviors remain stable over time. To improve the quality of the research, the questionnaire will be reviewed by cybersecurity and research-methodology specialists and piloted with a small group before full administration.

International Journal Of
Digital Trends And Youth Development
VOL 01 | No. 1 | 2026
P-I-SSN: XXXXXXXXXX | E-I-SSN: XXXXXXXXXX

METHODOLOGY

The study will use a structured and systematic methodology to examine the relationship between cybersecurity awareness and digital privacy-protection practices among young people. The target population will consist of internet-using individuals aged 15–24 who regularly use smartphones, social networking services, online learning platforms, gaming applications, or other internet-based services. Data collection will involve a structured questionnaire and semi-structured interviews. The questionnaire will contain sections on demographic characteristics, internet-use patterns, knowledge of cybersecurity threats, privacy literacy, security attitudes, protective behaviors, previous experiences of online threats, and access to cybersecurity education. Knowledge questions will assess participants' ability to identify phishing messages, recognize suspicious links, understand the purpose of multifactor authentication, and select appropriate responses to possible account compromise. Behavioral questions will examine password uniqueness, privacy-setting reviews, application permissions, software updates, use of account-recovery mechanisms, and willingness to report suspicious activity. Attitudinal questions will measure perceived threat severity, perceived personal vulnerability, confidence in performing protective actions, and trust in digital platforms. Where appropriate, established measurement items will be adapted with permission or according to their licensing requirements, and their suitability for the intended age group will be assessed before use. The questionnaire may use a five-point Likert scale for attitudinal and self-reported behavioral items, together with multiple-choice knowledge questions. A pilot study of approximately 20–30 participants may be conducted to identify unclear wording, excessive questionnaire length, and technical problems. Quantitative data will be collected using an accessible online questionnaire or paper-based instrument, depending on participants' access and institutional requirements. Semi-structured interviews will explore participants' understanding of privacy, experiences with suspicious communications, reasons for sharing personal information, responses to cyber incidents, and opinions about school-based cybersecurity education.

DATA ANALYSIS

Quantitative data will be analyzed using appropriate statistical software, such as SPSS, R, or an equivalent package. Before analysis, the researcher will examine the dataset for duplicate submissions, invalid responses, inconsistent entries, missing values, and potentially careless completion. Data-cleaning rules will be established before examining the principal research relationships to reduce the risk of selective decisions. Descriptive statistics, including frequencies, percentages, means, standard deviations, and appropriate distribution summaries, will be used to describe participants' characteristics, digital habits, cybersecurity knowledge, privacy concerns, and reported protective behaviors. Knowledge questions will be scored using predefined correct-answer criteria, while Likert-scale items will be coded consistently, with negatively worded items reverse-coded where necessary. If multiple items are intended to measure the same construct, internal consistency will be assessed using a suitable reliability coefficient, such as Cronbach's alpha or McDonald's omega, where assumptions permit. The research team will also examine whether the proposed measures adequately represent the constructs being investigated. To address the research question, correlations will be calculated to examine associations between cybersecurity awareness, privacy literacy, risk perception, self-efficacy, and protective behavior. Depending on the measurement level and distribution of the variables, Pearson or Spearman correlation coefficients may be

International Journal Of
Digital Trends And Youth Development
VOL 01 | No. 1 | 2026
P-I-SSN: XXXXXXXXXX | E-I-SSN: XXXXXXXXXX

appropriate. Group comparisons may be conducted to investigate whether awareness and reported practices differ by age group, educational level, prior cybersecurity training, or frequency of internet use. Appropriate tests may include independent-samples t-tests, analysis of variance, or their nonparametric alternatives, depending on assumptions and sample characteristics. Multiple regression may be used to examine whether cybersecurity knowledge, privacy literacy, perceived risk, self-efficacy, and educational exposure are associated with protective behavior while accounting for relevant demographic and usage variables. Results will be reported with effect sizes, confidence intervals, and p-values where appropriate, rather than relying exclusively on statistical significance. The researcher will avoid interpreting cross-sectional associations as proof of causation.

FINDINGS

The following section is an evidence-informed synthesis of the literature reviewed above, not a report of original fieldwork. It should be replaced or updated with actual statistical results, interview themes, and participant quotations after the proposed research has been completed. The literature suggests that young people possess varying levels of cybersecurity awareness and can often identify basic online safety principles, but their understanding of more complex privacy and security issues may be uneven. Williams et al. (2023) found that young participants could describe fundamental privacy and security concepts, while Azad (2025) reported limited knowledge of basic cybersecurity concepts among the college students in the Bangladesh sample. Taken together, these studies indicate that awareness is influenced by educational opportunities, previous experiences, and the nature of the digital services being used. A second anticipated theme is the possible gap between privacy concerns and actual protective behavior. Young people may understand that public sharing, weak passwords, and suspicious links create risks while continuing to engage in these practices because of convenience, social expectations, or confidence that serious incidents will not occur. Research on teenage privacy management and digital literacy supports the importance of examining knowledge, concerns, and perceived control together rather than treating them as interchangeable measures (De Wolf et al., 2023; Saritepeci et al., 2024). A third theme concerns personal information sharing and limited understanding of platform data practices. Young users may focus on who can see their posts while paying less attention to the collection, retention, and algorithmic use of behavioral data. Research on teenagers' privacy concepts and young people's experiences of algorithmically mediated services indicates that transparency and control are important concerns (Vespoli et al., 2024/2025; A call to action, 2024).

CONCLUSION

Cybersecurity awareness and digital privacy have become essential components of young people's safe and responsible participation in contemporary digital society. The expansion of social media, online education, gaming, mobile applications, and AI-supported services has created substantial opportunities for communication, learning, creativity, and social engagement. At the same time, these environments expose young people to phishing, account compromise, identity theft, fraudulent messages, cyberbullying, unauthorized data collection, and other security and privacy risks. The literature reviewed in this paper indicates that understanding online risks and applying protective measures are related but distinct

International Journal Of
Digital Trends And Youth Development
VOL 01 | No. 1 | 2026
P-I-SSN: XXXXXXXXXX | E-I-SSN: XXXXXXXXXX

capabilities. Young people may recognize common cybersecurity threats without consistently using strong and unique passwords, reviewing privacy settings, limiting unnecessary information sharing, or responding effectively to suspicious activity. Digital privacy literacy, perceived risk, confidence in protective actions, educational experiences, family communication, and platform design may all influence these decisions. Recent research also emphasizes that young people's privacy concerns extend beyond public posts to questions about algorithmic recommendations, personal-data collection, transparency, and control. These challenges cannot be addressed effectively by placing responsibility exclusively on individual users. Educational institutions should provide practical and continuous cybersecurity instruction, families should encourage informed discussion, and digital service providers should develop accessible privacy controls and safer default settings. Policymakers and regulators should support age-appropriate safeguards, clear information practices, and effective mechanisms for reporting and addressing online harms.

REFERENCES

Al-Saggaf, Y., & Maclean, J. (2024, December). Raising children's awareness of smartphone privacy risks through a targeted cybersecurity intervention. In Australasian Conference on Information Systems 2024: ACIS 202 (p. 14). ACIS.

Azad, R. U., Tasmim, S., & Atikuzzaman, M. (2026). Investigating students' awareness of online privacy and cybersecurity: an empirical study with effective cybersecurity training framework. Global Knowledge, Memory and Communication, 75(7-8), 4050-4071.

Botturi, L., Fioroni, T., Beretta, C., Andreoletti, D., Ferrari, A., Cardoso, F., ... & Giordano, S. (2024). The iBuddy experience: A digital simulation-based approach to enhance secondary school students' privacy awareness. Educational technology research and development, 72(2), 973-996.

Corcoran, E., Clement, A., & Gabrielli, J. (2024). A measurement model of online privacy cognitions in a sample of US adolescents. Behaviour & Information Technology, 43(16), 4150-4171.

De Wolf, R., Martens, M., Vanden Abeele, M., & De Marez, L. (2023). Predicting teens' privacy management and attitude toward data protection on social media. Cyberpsychology, Behavior, and Social Networking, 26(3), 153-160.

Laird, R. D., & Hawk, S. T. (2024). Adolescents' perceptions of privacy violations by parents, siblings, and friends. Journal of Research on Adolescence, 34(4), 1378-1390.