

Quantitative analysis on awareness and perception of the Online Safety Act 2025 (ONSA): A case study of law students at UiTM Sarawak

Juliza Salleh^{1*}, Ikhwan Naguib Jusoh², W Fatimah Hanun Wan Mohamad
Saferdin³, Nurul Aqmal Roslan⁴, Siti Mahanisayu Marhaban⁵

¹*Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA, Cawangan Sarawak, 94300 Kota Samarahan, Sarawak, Malaysia*

^{2,3,4,5}*Faculty of Law, Universiti Teknologi MARA, Cawangan Sarawak, 94300 Kota Samarahan, Sarawak, Malaysia*

ARTICLE INFO

Article history:

Received 5 May 2026
Revised 16 July 2026
Accepted 16 July 2026
Online first
Published 31 July 2026

Keywords:

Legal awareness
Online Safety Act
Perception

DOI:

10.24191/ji.v21i2.11584

ABSTRACT

This study examines the awareness and perception of the Online Safety Act (ONSA) among 315 law students from Universiti Teknologi MARA, Sarawak Branch. Using a quantitative survey analysed with descriptive statistics and independent t-test, the research reveals a moderate level of legal awareness and a high level of positive perception toward the Act. Data analysis indicates that female students have significantly higher awareness than male students, though awareness remains consistent across educational levels. Conversely, while perception do not vary by gender, degree students hold significantly stronger perception than diploma students. A key finding identifies educators as the primary source of information, emphasising their vital role in legal literacy. Despite widespread exposure to harmful experiences, a gap persists between students' supportive attitudes and their substantive legal understanding. These results offer valuable insights for policymakers and academic institutions to refine online safety initiatives through targeted curriculum integration and demographic-specific outreach.

1. INTRODUCTION

The existing legislation governing telecommunications, namely the Communications and Multimedia Act 1998 (Act 589), was enacted over two decades ago in a technological landscape that differs significantly from today's highly digitised environment. To respond to the rapid evolution of digital technologies and

^{1*}Corresponding author. *E-mail address:* juliza3379@uitm.edu.my

online platforms, the Online Safety Act 2025 (ONSA) (Act 866) was introduced to complement this legal framework. Coming into force on 1 January 2026 and enforced by the Malaysian Communications and Multimedia Commission (MCMC), ONSA seeks to strengthen and advance online safety in Malaysia by regulating harmful online content and delineating the duties and responsibilities of application service providers, content application service providers, and network service providers, as illustrated in its Preamble. By addressing emerging forms of online harm, the Act ensures that Malaysia's regulatory regime remains relevant, responsive, and aligned with contemporary technological developments.

The term "online safety" is often interchangeably used with concepts related to internet safety, cyber safety, internet security, online security, and cyber security (Jang and Ko, 2023). Meanwhile, the term "online harm" generally refers to the adverse effects associated with internet use, which frequently stem from problematic online behaviour as well as biases embedded within technological design and digital platforms (Zhang et al., 2026). According to Section 4 of ONSA, the term "harmful content" refers to the categories of content enumerated in the First Schedule. This includes material relating to child sexual abuse financial fraud, obscene material, indecent content, as well as any content that may cause harassment, distress, fear, or alarm through threatening, abusive, or insulting words, communications, or conduct. Collectively, these categories reflect the legislative intent to address a broad spectrum of online harm that may adversely affect individuals and the wider community.

The enforcement of ONSA as a legal response is to prevent harmful incidents such as the case of Rajeswary Appahu, known online as Esha, a 30-year-old Malaysian social media influencer and activist who tragically took her own life in July 2024 following sustained cyberbullying and online harassment (Azma Mohd Lazim, 2024). According to MCMC (Internet Users Survey 2024, n.d.), although affecting a smaller share of users than fraud or technical threats, cyberbullying has emerged as a significant issue in Malaysia, with 7.9% of users reporting incidents in 2024, up from 1.1% in 2022. ONSA, therefore, seeks to enhance individual protections and establish clear accountability for both perpetrators and digital platforms within Malaysia's contemporary online environment. In addition, the ONSA provides for extraterritorial application, extending its scope to individuals or entities located outside Malaysia who are licensed as Application Service Providers (ASPs), Content Application Service Providers (CASPs), or Network Service Providers (NSPs) under the Communications and Multimedia Act (CMA), insofar as they provide application services, content application services, or network services within Malaysia (Section 3(2) ONSA).

As undergraduates represent one of the most digitally active groups in Malaysia, their awareness and perception of such legislation are critical for fostering responsible online behaviour. However, empirical evidence on how students understand and respond to ONSA remains limited. Therefore, this study addresses this gap by investigating the awareness and perception of ONSA among Malaysian undergraduates as a way to contribute to ongoing efforts to enhance legal literacy and inform targeted educational interventions.

1.1 Research objectives

The primary objective of this study is to examine students' awareness and perception of the ONSA. Specifically, the study seeks:

- (i) To assess the overall level of students' awareness of ONSA
- (ii) To evaluate the level of students' perception towards ONSA
- (iii) To determine whether students' awareness and perception toward ONSA differ significantly across gender and education level

1.2 Limitations

This study employed a convenience sample restricted to students from a single branch only, with participation limited to students enrolled in law courses during the period of data collection. As such, the findings of this study cannot be generalized to all Malaysian undergraduates or to students from other faculties, institutions, or regions. The sample reflects the perspectives of a specific cohort (law-course students) and may not capture the diversity of awareness and perception across disciplines. Apart from this, the sample exhibited a gender imbalance, as male students are relatively few in this campus. This imbalance may have influenced the overall results and reduced the representativeness of the findings. Law students may possess a higher baseline of legislative awareness, which could skew the results compared to non-law undergraduates. Future research should implement stratified random sampling across multiple faculties and nationwide campuses to achieve a more representative evaluation of the ONSA.

2. LITERATURE REVIEW

2.1 Internet risks

The rapid expansion of digital technologies has reshaped the academic and social environment of university students, exposing them to both opportunities and risks. Internet use among young adults, particularly law students, is often associated with challenges such as cybersecurity threats, online addiction, privacy concerns, and exposure to harmful content. These risks are critical in the context of the Online Safety Act 2025 (ONSA), which emphasizes safeguarding digital engagement. Studies consistently highlight the link between excessive internet use and psychological distress, with internet addiction being associated with depression, anxiety, and loneliness among Malaysian university students (Muhamad et al., 2026; Xu, 2026). Similarly, deficits in self-control have been shown to exacerbate vulnerability to addictive online behaviours. University students often lack awareness of data privacy and online safety practices, making them susceptible to phishing, identity theft, and cyberbullying. Research underscores the importance of digital literacy in mitigating these risks, as students frequently underestimate the consequences of unsafe online practices. Excessive screen exposure has also been linked to declines in academic performance, sleep quality, and mental health (Zeng et al., 2025). Moreover, the pervasive use of social media platforms can foster cyberbullying and misinformation, which directly affect students' perceptions of online safety regulations. University students are increasingly vulnerable to internet-related risks, ranging from problematic usage behaviours to cybersecurity threats.

Sánchez-Fernández and Borda-Mas (2022) found that problematic smartphone and internet use among students is driven by psychological factors such as negative affectivity and fear of missing out, underscoring the need for consistent diagnostic criteria. Salam et al. (2026) highlighted phishing and malware as persistent cybersecurity challenges in higher education, exacerbated by low awareness and inadequate training among students. Ulven and Wangen (2021) further emphasized that universities are attractive

targets for espionage and organized cybercrime, identifying nine strategic risks including data breaches and intellectual property theft. Collectively, these studies illustrate that internet risks among university students are multidimensional, encompassing psychological, behavioural, and institutional domains. Addressing these risks requires both individual-level interventions, such as digital literacy and well-being programs, and systemic measures like integrated cybersecurity frameworks.

The internet provides many benefits for children and young people, such as access to educational resources, opportunities for creative expression, and the ability to communicate with people around the world. However, these opportunities also come with significant risks. According to Alsehaima and Alanazi (2018), young users may encounter harmful online material, including violent or explicit content, which can negatively affect their psychological and emotional development. Similarly, Daskalaki et al. (2020) found that although digital platforms improve learning and social interaction, they can also expose children to cyberbullying, privacy threats, and inappropriate communication. Their large-scale survey of adolescents showed that increased internet use is linked to greater exposure to online risks, highlighting the importance of continuous monitoring and education about safe internet practices. Overall, these studies suggest that while the internet supports learning and creativity, proper safety measures are necessary to reduce potential harm.

Research also shows that many children do not have enough knowledge about online threats, which makes them vulnerable to scams, cyberbullying, and privacy breaches. Sağlam et al. (2023), who conducted a systematic literature review involving 44 research papers on cybersecurity education for children around the world, found that cybersecurity education programs differ greatly across countries, with many gaps in curriculum design and implementation. Their findings highlight the need to integrate digital safety training into school education systems so that children can develop better awareness and resilience against cyber threats. Another study on cybersecurity awareness also identified several common strategies for improving online safety, such as interactive learning tools, digital citizenship programs, and parental involvement. These initiatives can help children understand responsible internet behaviour and recognise potential online risks.

Cyberbullying is one of the most widely studied online safety issues affecting children and adolescents around the world. Unlike traditional bullying, cyberbullying can occur continuously and anonymously through digital platforms such as social media, messaging applications, and online gaming environments. According to Hinduja and Patchin (2015), cyberbullying refers to the wilful and repeated harm inflicted through electronic devices. Their research shows that victims of cyberbullying often experience emotional distress, depression, anxiety, and lower academic performance. Similarly, Livingstone and Haddon (2009) studied children's internet use across Europe and found that although digital technologies expand opportunities for communication, they also increase the risk of online harassment, bullying, and unwanted contact. Their findings suggest that online safety education and effective reporting mechanisms are essential for reducing incidents of cyberbullying.

Further research indicates the prevalence of cyberbullying varies between countries due to cultural, technological, and regulatory differences. Its psychological impacts also remain consistently serious, highlighting the need for international cooperation to address the problem. As a result, international regulations, such as data protection laws, have been introduced in many countries to address these concerns. These frameworks aim to limit the collection and misuse of personal information and encourage organizations to implement stronger cybersecurity measures.

Privacy and data protection are major components of online safety in the digital era. Many internet users, especially young people, share personal information online without fully understanding the potential risks. Research by Boyd (2014) highlights that adolescents often struggle to balance online self-expression with privacy protection. As social media platforms encourage users to share personal content, this can lead to privacy breaches, identity theft, or misuse of personal data. Furthermore, Acquisti et al. (2015) argue that individuals frequently underestimate privacy risks due to a limited understanding of how digital platforms collect and process personal data. Their study suggests that stronger privacy regulations and better user education are necessary to improve online safety.

Online grooming is another serious international online safety concern. It occurs when adults use digital platforms to build relationships with minors for sexual exploitation. According to Davidson and Gottschalk (2011), online grooming often involves a gradual process in which offenders gain a child's trust before manipulating or coercing them into harmful activities. This is made easier by digital communication tools such as chat rooms, gaming platforms, and social media that enable offenders to contact and interact with potential victims. Research also suggests that children who lack digital literacy or parental supervision are more vulnerable to grooming attempts. Therefore, studies emphasise the need for improved detection technologies, parental awareness programs, and stronger law enforcement collaboration to combat online exploitation. International organisations and governments have begun implementing strategies to address these risks, including specialised cybercrime units, reporting platforms, and awareness campaigns.

Ensuring online safety requires collaboration among multiple stakeholders, including parents, educators, governments, and technology companies. Parents play a crucial role in monitoring children's online activities and guiding responsible digital behaviour. As such, parental awareness and supervision can reduce children's exposure to online risks such as cyberbullying, pornography, and online scams. Governments and international organisations also contribute by developing policies and regulatory frameworks. For example, international collaborations and policy frameworks often aim to improve cybersecurity, protect personal data, and promote safe digital environments for young users. Such initiatives emphasise the need for stronger regulations and cooperation between technology platforms and regulatory bodies.

2.2 Digital literacy

As digital technologies continue to evolve, digital literacy among youth and students is important for developing responsible online behaviour by promoting empathy, the ethical dimension of digital use, and moral development (Quamhlo et al., 2024). According to Rao et al. (2024), when comparing the behaviour of youth and students from four countries, they found that the youth spend more time online chatting, gaming, and entertainment compared to utilising it for their studies. This trend is often influenced by peer pressure, where they try to emulate the standards set by their peers, and due to the pervasive 'Fear of Missing Out' (FOMO). In this situation, youth and students tend to be exposed to ethical dilemmas and academic integrity, such as plagiarism and other academic misconduct. At the same time, the use of online platforms may expose them to various risks if they fail to practice responsible online behaviour, especially when sharing their personal data and information. This might trigger some ethical issues such as privacy protection, identity theft, and other issues. Other forms of online misconduct among youth and students include the dissemination of hoaxes, cyberbullying, and limited critical thinking skills in evaluating information on the internet, which may lead to misinformation and fake news. Besides, irresponsible online

behaviour might lead them to anxiety and feelings of inadequacy, which affect their mental health and physical wellness. Therefore, it is crucial to encourage more positive and educational practices among youth and students when using digital platforms (Quamhlo et al., 2024; Nasrullah, 2026; Lin et al., 2024; Shete & Shetty, 2023).

To develop responsible online behaviour among youth and students, Lewin et al. (2021) introduced the cyber wellness concept to build awareness, judgment, and self-protection skills in digital spaces. They emphasise that cyber wellness supports youth and students in becoming more aware of how to behave appropriately, protect themselves, manage online identity, and maintain safe and responsible relationships in cyberspace. Cyber wellness can help strengthen information and media literacy, where it helps them develop critical thinking skills to judge whether online information is reliable to avoid fake news, echo chambers or manipulations. Cyber wellness also increases students' awareness of online risks such as misuse of personal data, cyberbullying, contact with strangers, phishing, scams, and exposure to harmful content. This awareness helps them regulate their behaviour, protect their privacy, and respond appropriately when problems arise.

The concept or framework of cyber wellness can be taught not only through restriction, but also through education, guidance, and balanced practice in the form of explicit training, opportunities to practice, and support from the teacher, parents, and school. For instance, in Vietnam, experimental research conducted found that structured online safety programs can significantly reduce risky online behaviours among students. The program led to a noticeable decrease in unsafe digital practices, demonstrating the effectiveness of educational interventions in promoting safer online habits. Rashidov (2024) and Hughes et al. (2024) also agreed that young people need more than technical digital skills and move beyond basic safety, where they need to learn how to behave safely, engage ethically and respectfully, think critically, participate responsibly, and act democratically online. This awareness can be fostered through formal education, simulations, and school-wide programs.

2.3 Legal awareness and legal literacy

Legal awareness or legal literacy is a crucial foundation for every individual to understand their constitutional and legal rights, duties, and responsibilities in ensuring the stability and sustainability of a country. Legal illiteracy or deficient legal awareness may contribute to an increase in criminal behaviour, including serious offences such as murder, robbery, and corruption, as well as online crimes, including fraud, scams, and other forms of cybercrime (Andyastuti et al., 2025; Damayanti et al., 2024). It also refers to a system of individual knowledge and understanding of law and the proper order of legal regulation, as well as their belief in, recognition of, and acceptance of the values embodied in law.

Legal awareness is an important part of society's legal life and a key element of legal culture. Law and legal awareness are closely connected and cannot be separated from one another. As a counterpart to law, legal awareness represents how people understand and perceive legal realities, serving as a kind of measure for the legitimacy of the law (Horák et al., 2021). According to Haitao (2022), legal awareness can be understood as a system of knowledge about the law and how legal regulation should function. It also reflects how people perceive legal phenomena and their ideas about what a fair and proper legal order should be. In this sense, it represents a psychological reflection of state and legal realities.

Legal awareness can be seen as people's belief in the values embodied in the law. Nelken (2004) argued that it also refers to a person's attitude toward the existing law, the behaviour of others, and their own rights

and responsibilities. This reflects the multi-level nature of how legal awareness operates, involving both legal knowledge and legal evaluation. Within the theoretical framework of the legal awareness, legal values, legal behaviour triangle, legal awareness represents the intellectual, emotional, and value-based understanding of information related to legal reality.

Legal awareness theory has emerged through contributions from scholars in the sociology of law and legal culture rather than from a single originator. These researchers explored how individuals perceive, interpret, and engage with law in everyday contexts. A key figure in this field is Lawrence M. Friedman, who introduced the concept of legal culture. He emphasised that the effectiveness of law depends not only on institutions and formal rules but also on the attitudes, values, and expectations people hold toward it (Friedman, 1975). His work emphasises that public awareness and beliefs about the law play an important role in shaping how legal systems operate.

Ewick and Silbey (1998) also made a significant contribution. In their book *The Common Place of Law*, they examined how ordinary people experience and interpret the law in their everyday lives. They introduced the concept of legal consciousness, suggesting that people relate to the law in different ways, such as by viewing themselves as “before the law”, “with the law”, or “against the law”. It refers to the way individuals and groups perceive, understand, and respond to the law. Although law exists as an objective social reality, its effectiveness largely depends on people’s attitudes and actions toward it.

Legal awareness combines knowledge, emotions, and moral values, which influence whether behaviour is lawful, socially beneficial, or harmful. It includes both rational and emotional components. The rational aspect involves legal knowledge and reasoning, while the emotional aspect relates to people’s attitudes and feelings toward the law. Legal education, both general and professional, plays an important role in shaping this awareness. Legal awareness can exist at three levels. Professional legal awareness develops through legal education and legal practice. Scientific legal awareness is typical of researchers who study law and legal philosophy. Legal awareness can also be individual or collective. Collective legal awareness may exist within specific groups or larger communities and can extend to the broader public sense of justice within society (Kozhukhova & Zhiyenbayey, 2018).

3. METHODOLOGY

3.1 Respondents and sampling

This study focused on a population of 867 students from the Accounting, Administrative Science, and Business Studies faculties at the Samarahan, Samarahan 2, and Mukah campuses who were enrolled in various law-related courses during the October 2025 to February 2026 semester. To ensure the sample size was sufficient for statistical analysis, the guidelines proposed by Krejcie and Morgan (1970) were utilised. Based on their sample size determination table for the given population, a minimum sample size of 265 respondents was required to represent the population at 95% confidence. While the sample size was determined statistically, the selection of respondents was conducted using convenience sampling. This non-probability sampling method was chosen due to the accessibility of the students and logistical constraints. The data collection phase resulted in 315 valid responses, exceeding the minimum requirement. All 315 valid responses were retained for the final analysis to enhance statistical power and improve the robustness of the findings.

3.2 Research instrument

The data for this study were collected using a structured questionnaire designed to assess students' awareness and perception of ONSA. Questionnaires are widely used in awareness and perception studies because they enable efficient collection of standardised data from a large number of respondents and allow for quantitative analysis (Creswell, 2014; Sekaran & Bougie, 2016). The questionnaire was developed with AI assistance and subsequently refined to ensure clarity and relevance to the study constructs. Although a formal pilot test was not conducted due to practical constraints, the validity of the instrument was established through expert review. Three subject matter experts (law lecturers) examined the items for content validity, confirming their alignment with the intended constructs of awareness and perception.

The questionnaire consisted of three sections. Section A collected respondents' demographic and academic background information. This information was important for describing the respondents' characteristics and provides context for understanding differences in awareness and perception. Section B measured respondents' awareness of ONSA using five items that assessed their familiarity, knowledge, and exposure to the act, including whether they had heard about ONSA, understood its purpose, and were aware of its implementation and relevance to online safety. Section C utilised five items to gauge perception regarding the relevance, fairness, and effectiveness of ONSA in enhancing online safety and user protection. Understanding their perception was important as it reflected respondents' acceptance and evaluation of the Act's role in enhancing digital safety. The responses for Sections B and C were measured using a 5-point Likert scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree), which allowed respondents to indicate their level of agreement with each statement and provide a reliable measure of awareness and perception constructs.

Construct validity of the questionnaire was examined using factor analysis to verify whether the items aligned with the intended theoretical constructs of awareness and perception. Prior to extraction, the Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy was calculated and yielded a value of 0.877, exceeding the recommended threshold of 0.60 (Kaiser, 1974). In addition, Bartlett's Test of Sphericity was significant ($\chi^2=1906.042$, $p\text{-value} < .001$), confirming that the correlation matrix was suitable for factor analysis. The analysis also showed two clear factors with eigenvalues greater than 1, which matched the expected constructs. Each item for both constructs also had a strong loading (above 0.40), showing that they fit well with their intended construct (Kaiser, 1960). Overall, the two factors explained 70.26% of the total variance, which is considered satisfactory. This result means the questionnaire items worked as expected and provided good evidence of construct validity.

3.3 Statistical analysis

To ensure credible results, several statistical checks were applied. Reliability was confirmed using Cronbach's alpha, with all constructs exceeding the accepted threshold. Construct validity was examined through factor analysis to confirm the dimensionality of the questionnaire. Descriptive statistics summarised student responses, while mean scores were calculated to treat Likert-scale data as continuous. An independent t-test explored differences by education level and gender, following normality checks through visual plots and skewness values. Together, these steps ensured that the findings on students' awareness and perception of ONSA were both reliable and interpretable.

4. RESULTS AND DISCUSSIONS

4.1 Demographic analysis

Table 1 summarises the demographic characteristics of the 315 respondents who participated in this study, categorised by gender, educational level, and campus. The sample was predominantly female, accounting for 76.5% (n=241), while male respondents accounted for 23.5% (n=74). In terms of educational level, the distribution was nearly balanced with Diploma students comprising 50.5% (n=159), and Degree students making up the remaining 49.5% (n=156). The majority of the respondents were from the Samarahan campus (n=152, 48.3%). This was followed by the Samarahan 2 campus with 39% (n=123) and the Mukah campus with 12.7% (n=40).

Table 1. Demographic profile of respondents

Demographic		Frequency	Percentage
Gender	Male	74	23.5%
	Female	241	76.5%
Education Level:	Diploma	159	50.5%
	Degree	156	49.5%
Campus	Mukah	40	12.7%
	Samarahan	152	48.3%
	Samarahan 2	123	39%
Total		315	100%

Figure 1 details the sources of awareness regarding ONSA among the 315 respondents. Most of the students (58.4%, n=184) indicated that they first heard about the Act from their lecturers. Social media was the second most common source of information (27.9%, n=88), followed by online and offline news (10.5%, n=33). Interpersonal communication played a minimal role, with only 1.9% (n=6) hearing about the act from friends. The ‘Others’ category included respondents who had not heard of the Act before participating in this survey. This finding highlights the pivotal role of educators in disseminating knowledge on online safety. Prior studies have emphasised that lecturers and teachers serve as critical agents in shaping students’ awareness of cybersecurity and digital safety. For instance, Raju et al. (2022) found that structured guidance from academic staff significantly enhances students’ understanding of safe practices when using digital platforms in higher education settings. Similarly, Arishi et al. (2024), in their systematic review of cybersecurity awareness in schools, concluded that educators are among the most effective channels for instilling digital safety knowledge, given their authority and direct engagement with students.

Figure 2 reveals that harmful online experiences are widespread among students. A total of 81.9% (n=258) of respondents reported encountering harmful online situations at least occasionally, comprising those who experienced them rarely (27%), sometimes (43.2%), often (8.3%), and very often (3.5%). Only 18.1% (n=57) of the students reported never encountering harmful online situations. The predominance of ‘Sometimes’ responses suggests that harmful content or interactions were part of the typical online environment for students, rather than isolated incidents. This finding underscores the importance of digital safety education and awareness initiatives. Since lecturers were identified earlier as the primary source of awareness about ONSA, their role has become even more critical in equipping students with strategies to recognise, avoid, and respond to harmful online situations.

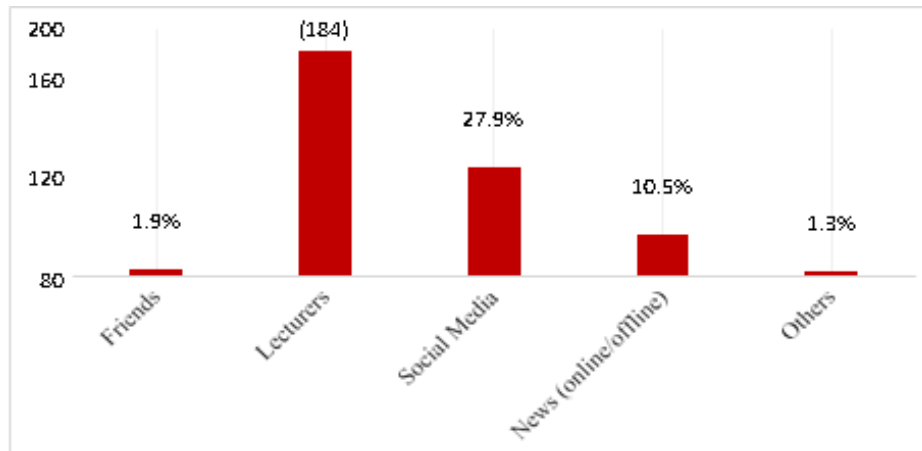


Fig. 1. Sources of awareness regarding the ONSA

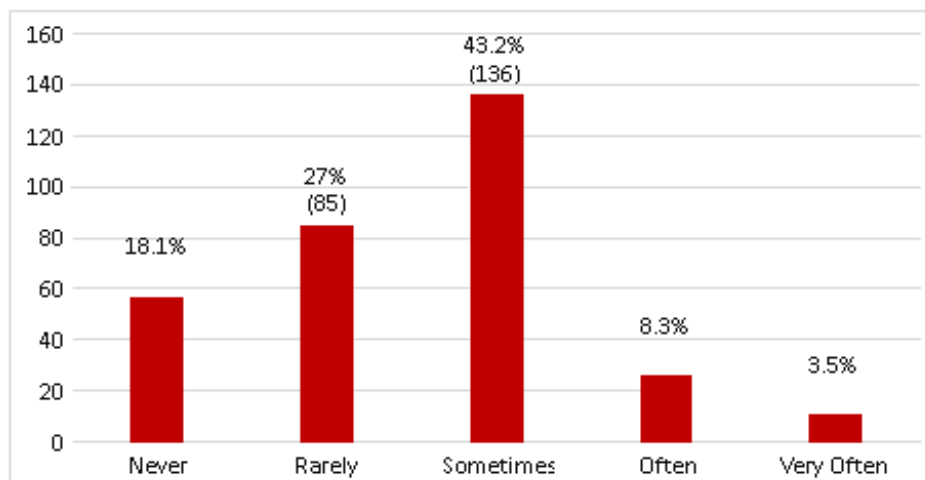


Fig. 2. Exposure to harmful situations while using the internet

4.2 Reliability analysis

Reliability analysis was conducted to assess the internal consistency of the items in measuring the awareness and perception constructs. Cronbach's Alpha was used as the reliability coefficient, with values above 0.70 generally considered acceptable for social science research (Nunnally, 1978). Values between

0.70 and 0.95 are typically regarded as the ideal range, indicating that items are sufficiently correlated without being redundant. Overall, both constructs exceeded the minimum threshold of 0.70, with values ranging from 0.84 to 0.927 as presented in Table 2. These results confirm that the measurement instrument is highly reliable for assessing students' awareness and perception of ONSA.

Table 2. Reliability test result

Construct	Number of Items	Cronbach's Alpha
Awareness	5	0.840
Perception	5	0.927

4.3 Normality and descriptive analysis

Before conducting inferential analyses, the normality of the data was assessed through boxplots and skewness values as presented in Table 3. The skewness values for both constructs fell within the acceptable range of -1 to $+1$, indicating that the distributions were approximately normal. Both constructs exhibited slight negative skewness, suggesting a tendency for responses to cluster toward higher agreement levels on the Likert scale. Visual inspection of boxplots, as shown in Figure 3, further indicated that both constructs are approximately normally distributed, with medians centred and only minor skewness toward higher agreement levels. Although some outliers were present, the overall spread supports the assumption of normality, justifying the use of parametric tests. For the interpretation of mean scores in Table 3, the descriptive framework of Best and Kahn (2006), was adopted as presented in Table 4. This framework categorises mean values into five levels, ranging from very low to very high, and was used to guide the analysis of students' responses, providing a structured understanding of their perception and awareness of the ONSA.

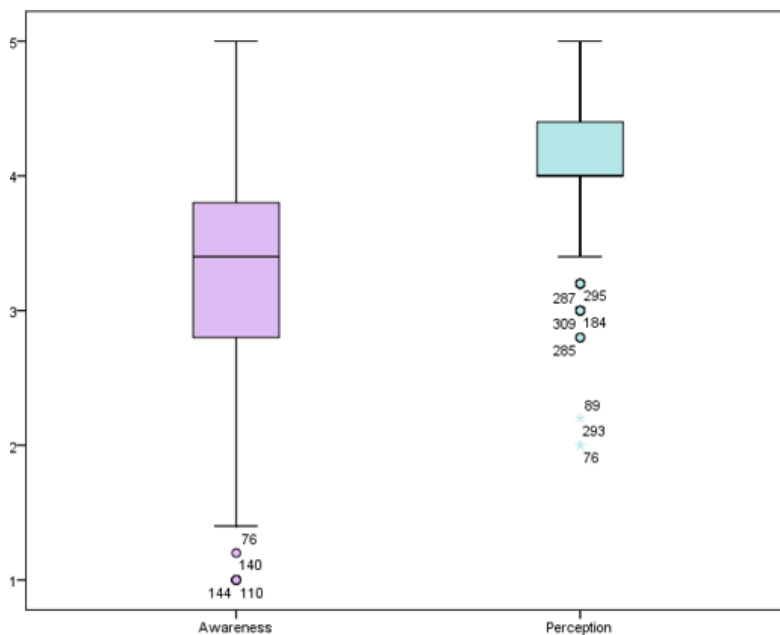


Fig. 3. Boxplots of both constructs

Table 3. Descriptive statistics for both constructs

Construct	Mean (M)	Standard Deviation (SD)	Skewness	Level of Agreement
Awareness	3.25	0.75	-0.552	Moderate
Perception	4.08	0.56	-0.326	High

Table 4. Interpretation of mean score

Mean score	Level of agreement
1.00-1.80	Very low
1.81-2.60	Low
2.61-3.40	Moderate
3.41-4.20	High
4.21-5.00	Very high

Source: Best and Kahn (2006)

The construct of awareness yielded a mean score of 3.25 (SD=0.75). According to Table 4, this score falls within the 2.61–3.40 range, indicating a moderate level of agreement. In contrast, the perception construct received a higher level of endorsement from the students, with a mean score of 4.08 (SD=0.56). This value falls within the 3.41–4.20 range, signifying a high level of agreement. The lower standard deviation compared to awareness suggests greater consensus among students regarding their perception. Despite a high level of positive perception (M=4.08), the students' awareness (M=3.25) is only moderate, indicating an imbalance between sentiment and information. This highlights a need for further educational outreach to ensure that students' awareness levels eventually match their perception.

4.4 Analysis of awareness and perception towards (ONSA)

An independent samples t-test was performed to assess differences in awareness and perception of ONSA across gender and education level. Levene's test in Table 5 indicated that the assumption of homogeneity of variances was satisfied for both gender ($F=2.338$, $p\text{-value} > .05$) and education level ($F=0.282$, $p\text{-value} > .05$) for the awareness construct. Due to the unequal sample sizes between male and female students, Welch's t-test was employed which does not assume equal variances. The results showed that female students (M=3.32, SD=0.71) reported higher awareness mean scores than male students (M=3.04, SD=0.83), and this difference was statistically significant ($t=-2.589$, $p\text{-value} < .05$). The magnitude of this difference was small, with Cohen's $d = -0.37$ and the 95% confidence interval of -0.64 and -0.11 also signify that the result is statistically significant as it does not include zero. In contrast, although degree students (M=3.32, SD=0.73) obtained slightly higher mean scores than diploma students (M=3.19, SD=0.77), the difference was not statistically significant ($t=1.551$, $p\text{-value} > .05$, Cohen's $d = -0.18$, $CI = [-0.40, 0.05]$). These results suggest that gender is associated with differences in students' awareness of ONSA, while education level does not exert a significant effect.

For gender analysis, Levene's test indicated no violation of variance equality ($F=0.754$, $p\text{-value} > .05$). Likewise, Welch's t-test also was used for gender analysis to account for unequal sample sizes and variances between male and female students. The t-test revealed that although female students (M=4.11, SD=0.54) reported slightly higher mean scores than male students (M=3.99, SD=0.63), this difference was not statistically significant ($t=-1.40$, $p\text{-value} > .05$). The effect size was small, Cohen's $d = -0.20$, 95%

confidence interval between -0.46 to 0.06 , with the confidence interval crossing zero, confirming the lack of statistical significance.

In contrast, degree students ($M=4.15$, $SD=0.56$) scored higher than diploma students ($M=4.01$, $SD=0.55$). Levene's test in Table 6 showed unequal variances ($F=4.122$, $p\text{-value} < .05$), and the independent t-test revealed a significant difference ($t=2.125$, $p\text{-value} < .05$), indicating that education level influenced perception of ONSA. The magnitude of this difference was small, Cohen's $d=-0.24$, 95% confidence interval between -0.46 to -0.02 . Because the confidence interval excludes zero, the effect is statistically reliable. These findings align with prior research suggesting that education level enhances online safety knowledge and attitudes (Qin et al., 2023), while gender differences in online safety perception often appear less consistent across contexts (Savoia et al., 2021). Together, the results suggest that educational attainment plays a more decisive role than gender in shaping students' perception of online safety.

Table 5. Independent t-test results for the awareness construct

Construct Awareness	n	Mean	SD	Levene's F-test	Independent t-test	Effect size (Cohen's d)	95% CI
Gender:							
Male	74	3.04	0.83	2.338	-2.589	-0.37	(-0.64, -0.11)*
Female	241	3.32	0.71	(0.127)	(0.001)*		
Education level:							
Degree	156	3.32	0.73	0.282	1.551	-0.18	(-0.40, 0.05)
Diploma	159	3.19	0.77	(0.596)	(0.122)		

Note: * indicates significance at 5% level.

Table 6. Independent t-test results for the perception construct

Construct Awareness	n	Mean	SD	Levene's F-test	Independent t-test	Effect size (Cohen's d)	95% CI
Gender							
Male	74	3.99	0.63	0.754	-1.400 (0.164)	-0.20	(-0.46, 0.06)
Female	241	4.11	0.54	(0.386)			
Education level							
Degree	156	4.15	0.56	4.122	2.125 (0.034)*	-0.24	(-0.46, -0.02)
Diploma	159	4.01	0.55	(0.043)*			

5. CONCLUSION

This study examined the awareness and perception of the ONSA among undergraduates at Universiti Teknologi MARA, Sarawak Branch. The findings revealed moderate awareness and a high level of perception of the Act. Although students expressed strong support for the relevance and importance of ONSA, their depth of knowledge and familiarity with its specific provisions remained only moderate. This disparity indicates that positive attitudes toward digital safety legislation do not necessarily equate to a comprehensive grasp of its legal dimensions. The analysis also points to meaningful demographic patterns. Gender differences were observed in awareness, with female students reporting higher levels than their male counterparts, though perception of ONSA did not vary significantly by gender. Conversely, education level reported no significant effect on awareness, but degree students showed stronger perception compared to diploma students. These results suggest that demographic factors shape awareness and evaluative

attitudes in distinct ways. Lecturers play a critical role in transforming general online vulnerability into a more coherent legal understanding. Overall, this research contributes empirical evidence to ongoing discussions on digital governance and legal literacy in higher education, offering practical insights for policymakers and academic institutions seeking to enhance online safety awareness among young people.

6. RECOMMENDATIONS

The findings indicate that although students demonstrate strong evaluative support for ONSA, their level of legal awareness remains moderate. This imbalance highlights the need for structured curriculum-based interventions within higher education institutions. Universities should systematically integrate ONSA-related content into relevant programmes or students' activities, particularly those involving digital literacy, law, and communication studies. Beyond general discussions of online safety, instructional strategies should incorporate applied case analyses, legislative interpretation exercises, and scenario-based learning to strengthen students' cognitive understanding of the act. Given that lecturers were identified as the primary source of awareness, institutional mediation mechanisms should be reinforced through professional development initiatives, standardised teaching materials, and coordinated digital safety modules. Strengthening the role of educators as legal knowledge translators is essential to bridging the gap between favourable perception and substantive awareness.

The observed gender and education-level differences suggest that legal literacy initiatives must be responsive to demographic variations rather than uniformly implemented. Universities and policymakers should leverage both formal instruction and digital communication platforms, including social media campaigns, interactive workshops, and student-led advocacy programmes, to broaden engagement. Experiential learning activities such as mock legal proceedings or online risk simulations may further enhance the internalisation of legal norms. Future research should extend this study across multiple institutions and employ advanced analytical techniques, such as Structural Equation Modelling (SEM) and examine the mediating role of institutional influence in shaping legal consciousness.

7. ACKNOWLEDGEMENTS/FUNDING

All authors express their gratitude to the students of Universiti Teknologi MARA, Sarawak Branch (Mukah, Samarahan, and Samarahan 2 campuses) who took law courses during the October 2025 to February 2026 semester, for their voluntary participation and valuable contributions to this study. This study did not receive any financial support from governmental or any institutional authorities.

8. CONFLICT OF INTEREST STATEMENT

This research was carried out independently, without any financial, commercial, or personal interests that could be perceived as potential conflicts.

9. AUTHORS' CONTRIBUTIONS

Juliza Salleh: Methodology, data collection; formal data analysis, writing-original draft; writing-review and editing. **Ikhwan Naguib Jusoh, W Fatimah Hanun Wan Mohamad Saferdin, Nurul Aqmal Roslan, Siti Mahanisayu Marhaban:** Validation; literature review; project adminstation; writing-original draft; writing-review and editing.

10. DECLARATION OF GENERATIVE AI IN THE WRITING PROCESS

During the preparation of this work, the authors used Microsoft Copilot and Google Gemini for the purpose of rephrasing text. After using these tools, the authors reviewed the content as needed to ensure the accuracy and integrity of the publication. This article has also been proofread by subject-matter experts to further ensure its quality. In addition, the manuscript underwent professional proofreading by Life Linguist Enterprise to guarantee clarity, consistency, and adherence to academic standards.

11. DATA AVAILABILITY/SUPPLEMENTARY MATERIALS

All supporting materials from this study, including datasets and related resources are available upon request. Authors may contact the first author directly to obtain the files, which will be provided in accessible formats to support further research.

12. ETHICS STATEMENT

The authors declare that this study was conducted with voluntary respondents who provided informed consent. Participant anonymity and confidentiality were safeguarded at all stages of the research process.

13. REFERENCES

- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509–514. <https://doi.org/10.1126/science.aaa1465>
- Alsehaima, A. O., & Alanazi, A. A. (2018). Psychological and social risks to children of using the internet: Literature review. *Journal of Child and Adolescent Behaviour*, 6(380), 2. <https://doi.org/10.4172/2375-4494.1000380>
- Arishi, A. A., Kamarudin, N. H., Abu Bakar, K. A., Shukur, Z. B., & Hasan, M. K. (2024). Cybersecurity awareness in schools: A systematic review of practices, challenges, and target audiences. *International Journal of Advanced Computer Science and Applications*, 15(12), 124–134. <https://doi.org/10.14569/IJACSA.2024.0151249>
- Andyastuti, E., Sasmita, W., Nursalim, Widodo, A., Suratman, Pristiani, Y. D., Wiranata, I. H., Fauziah, H. U., & Boo, I. K. (2025). A theoretical review of urban community legal literacy in the context of citizenship rights and obligations. *International Journal of Research and Review*, 12(7), 561–567. <https://doi.org/10.52403/ijrr.20250758>
- Best, J. W., & Kahn, J. V. (2006). *Research in education* (10th ed.). Pearson Education Inc.
- Boyd, D. (2014). *It's complicated: The social lives of networked teens*. Yale University Press. <https://doi.org/10.12987/9780300166439>

- Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). SAGE Publications.
- Damayanti, S., Khairunisa, W., & Fajriani, N. (2024). Building legal awareness of citizens through civic participation competence in civic education. *ABJAD: Journal of Humanities & Education*, 2(2), 91–99. <https://doi.org/10.62079/abjad.v2i2.34>
- Daskalaki, E., Psaroudaki, K., Karkanaki, M., & Fragopoulou, P. (2020). *Understanding the online behavior and risks of children: Results of a large-scale national survey on 10-18 year olds*. <https://doi.org/10.48550/arXiv.2008.10274>
- Davidson, J., & Gottschalk, P. (2011). Characteristics of the internet for criminal child sexual abuse by online groomers. *Criminal Justice Studies*, 24(1), 23-36. <https://doi.org/10.1080/1478601X.2011.544188>
- Ewick, P., & Silbey, S. S. (1998). *The common place of law: Stories from everyday life*. University of Chicago Press. <https://doi.org/10.2307/2655592>
- Friedman, L. M. (1975). *The legal system: A social science perspective*. Russell Sage Foundation.
- Haitao, N. (2022). Determination of behavior, principles and law abiding on business ethics. *Journal of Law Politic and Humanities*, 2(2), 76-84. <https://doi.org/10.38035/jlph.v2i2.87>
- Hinduja, S., & Patchin, J. W. (2015). *Bullying beyond the schoolyard: Preventing and responding to cyberbullying*. Corwin press.
- Horák, F., Lacko, D., & Kloczek, A. (2021). Legal consciousness: A systematic review of its conceptualization and measurement methods. *Anuario de Psicología Jurídica*, 31(1), 9–34. <https://psycnet.apa.org/doi/10.5093/apj2021a2>
- Jang, Y., & Ko, B. (2023). Online safety for children and youth under the 4cs framework. *A focus on digital policies in Australia, Canada, and the UK. Children*, 10(8), 1415. <https://doi.org/10.3390/children10081415>
- Kaiser, H. F. (1960). The application of electronic computers to factor analysis. *Educational and Psychological Measurement*, 20(1), 141–151. <https://doi.org/10.1177/001316446002000116>
- Kaiser, H. F. (1974). An index of factorial simplicity. *Psychometrika*, 39(1), 31–36. <https://doi.org/10.1007/BF02291575>
- Kozhukhova, M., & Zhiyenbayev, M. (2018, January). *Conceptualizing legal culture and legal awareness: Meaning and structural components*. SHS Web of Conferences (Vol. 55, pp. 02009). <https://doi.org/10.1051/shsconf/20185502009>
- Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and Psychological Measurement*, 30(3), 607–610. <https://doi.org/10.1177/001316447003000308>
- Lewin, C., Niederhauser, D., Johnson, Q., Saito, T., Sakamoto, A., & Sherman, R. (2021). Safe and responsible internet use in a connected world: Promoting cyber-wellness. *Canadian Journal of Learning and Technology*, 47(4). <https://doi.org/10.21432/cjlt28069>
- Lazim, A. M. (2024, July 9). Buat laporan polis, tak sempat beri keterangan tamat riwayat sendiri, berikut kronologi buli siber pempengaruh Rajeswary Appahu | *SinarPlus*. SinarPlus. <https://sinarplus.sinarharian.com.my/lifestyle/kisah-masyarakat/buat-laporan-polis-tak-sempt-beri-keterangan-tamat-riwayat-sendiri-berikut-kronologi-buli-siber-pempengaruh-rajeswary-appahu>
- Livingstone, S., & Haddon, L. (2009). EU kids online: Final report 2009. *The London School of Economics and Political Science*. <https://researchonline.lse.ac.uk/id/eprint/24372>

- Lin, L.-C., Chang, F.-C., Huang, T.-F., Chen, T.-Y., Chiu, C.-H., Chen, P.-H., Miao, N.-F., Chuang, H.-Y., & Chen, H.-C. (2024). Effects of media literacy intervention on weight-control products digital marketing targeting adolescents. *Behavioral Sciences*, 14(11), 1023. <https://doi.org/10.3390/bs14111023>
- Muhamad, N.A., Maamor, N. H., Tengku Baharudin Shah, T. P. N., Jamalluddin, N. H., Leman, F. N., Rosli, I. A., Nik Azhan, N. A. F., Chemi, N., Muhamad Rasat, M. A., Abdullah, N., Abdul Jabbar, N., Ibrahim, N., & Mohamad Isa, M. F. (2026). Association between depression, anxiety and loneliness with internet addictions among public university students in Malaysia. *BMJ Open* 2026, 16(e108315). <https://doi.org/10.1136/bmjopen-2025-108315>
- Nasrullah, A., Marlina, M., Caesarani, S., Dwiyantri, W., & Aminah, M. (2026). Pemanfaatan media sosial sebagai sarana edukasi literasi bagi siswa sekolah dasar negeri 1 Serang. *Jurnal Pengabdian Masyarakat dan Riset Pendidikan*, 4(3), 17598–17603. <https://doi.org/10.31004/jerkin.v4i3.4740>
- Nelken, D. (2004). Using the concept of legal culture. *Australian Journal of Legal Philosophy*, 29(2004), 1–26. <https://classic.austlii.edu.au/au/journals/AUJLegPhil/2004/11.pdf>
- Nunnally, J. C. (1978). *Psychometric theory* (2nd ed.). McGraw-Hill.
- Qin, A., Cheong, H. H. W., Xu, X., Zhang, Y., & Kolletar-Zhu, K. (2023). How education level influences internet security knowledge, behaviour, and attitude: A comparison among undergraduates, postgraduates and working graduates. *International Journal of Information Security*, 22(3), 305–317. <https://doi.org/10.21203/rs.3.rs-1977578/v1>
- Quamhlo, H., Yasin, M., & Ghazali, N. (2024). *Moral behaviour practice among students in the digital era: A conceptual exploration*. In International Graduate Research in Education Seminar 2024 (i-GREduc 2024) Proceedings (pp. 121–128). Faculty of Educational Studies, Universiti Putra Malaysia. https://spel3.upm.edu.my/max/dokumen/GREDUC_GREduc_2024_Proceedings_Final2-compressed.pdf
- Raju, R., Abd Rahman, N. H., & Ahmad, A. (2022). Cyber security awareness in using digital platforms among students in a higher learning institution. *Asian Journal of University Education*, 18(3), 756–766. <https://doi.org/10.24191/ajue.v18i3.18967>
- Rao, D., Lee, C., Fdilati, Y., Bouziane, A., & Dressman, M. (2024). Across four nations: Comparing the discourses of adolescents' digital literacy. *Journal of Adolescent & Adult Literacy*, 68(2), 94–104. <https://doi.org/10.1002/jaal.1338>
- Rashidov, A. (2024). Integrating cybersecurity education in schools: A strategic approach to fostering digital resilience and ethical digital citizenship among youth. *Uzbek Journal of Educational Research*, 4(6), 72–78. <https://doi.org/10.5281/zenodo.14007299>
- Sağlam, R. B., Miller, V., & Franqueira, V. N. (2023). A systematic literature review on cyber security education for children. *IEEE transactions on education*, 66(3), 274–286. <https://doi.org/10.1109/TE.2022.3231019>
- Salam, M., Abu Bakar, K. A., Abdul Ghani, A. T., & Mohd Aman, A. H. (2026). Cybersecurity in higher education institutions digitalisation: Addressing threats and vulnerabilities. *SAGE Open*, 16(1), 1–14. <https://doi.org/10.1177/21582440251413473>
- Sánchez-Fernández, M., & Borda-Mas, M. (2022). Problematic smartphone use and specific problematic internet uses among university students and associated predictive factors: A systematic review. *Education and Information Technologies*, 28(6), 7111–7204. <https://doi.org/10.1007/s10639-022-11437-2>

- Savoia, E., Harriman, N. W., Su, M., Cote, T., & Shortland, N. (2021). Adolescents' exposure to online risks: Gender disparities and vulnerabilities related to online behaviors. *International Journal of Environmental Research and Public Health*, 18(11), 5786. <https://doi.org/10.3390/ijerph18115786>
- Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill-building approach* (7th ed.). John Wiley & Sons.
- Shete, D. R., & Shetty, P. H. (2023). Social media's effect on today's teenagers' mental and physical health. *Journal of Advanced Zoology*, 44(S8), 213–219. <https://doi.org/10.53555/jaz.v44iS8.3539>
- Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet*, 13(2), 39. <https://doi.org/10.3390/fi13020039>
- Xu, J., Lan, W., Xie, Z., Fu, C., Guan, J., & Ren, Y. (2026). Association between self-control and internet addiction in university students: A simulation-based network analysis. *International Journal of Mental Health and Addiction* 2026. <https://doi.org/10.1007/s11469-026-01678-4>
- Zeng, Z., Shi, Z., Hou, S., Yan, J., Yang, R., & Li, X. (2025). Comprehensive effects and dose–response relationship of screen exposure on university students' physical and mental health and academic performance in the digital age: A systematic review and meta-analysis. *BMC Public Health*, 26, 1363. <https://doi.org/10.1186/s12889-026-27025-9>
- Zhang, M., Wang, F., & Zhang, J. (2026). Educational disparities in digital inequality: Relationships between online activities and online harms. *Acta Psychologica*, 264, 106545. <https://doi.org/10.1016/j.actpsy.2026.106545>



© 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY-NC-ND) license (<http://creativecommons.org/licenses/by/4.0/>).