Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

Empowering Saudi youth: The ISAS framework for promoting online safety and cybersecurity awareness

Nawaf Alharbi [1], Halima Samra [2, *], Alice Li [3], Ben Soh [1]

[1]*Department of Computing, Science and Information Technology, La Trobe University, Melbourne, Victoria 3086, Australia*
[2]*Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia*
[3]*La Trobe Business School, La Trobe University, Melbourne, Victoria 3086, Australia*

ARTICLE INFO

Article history:
Received 14 October 2024
Received in revised form
3 February 2025
Accepted 9 March 2025

Keywords:
Internet safety
E-safety framework
Youth awareness
Cybersecurity risks
Behavioral adoption

ABSTRACT

The increasing use of the Internet, along with the widespread access to social media, video games, and various online platforms, presents significant safety challenges, particularly for young people and teenagers. To address these concerns, this study develops and validates the Internet Security Awareness (ISAS) e-safety framework, designed to promote safe Internet usage among youth in Saudi Arabia. The framework was constructed based on a survey of 92 IT professionals and experts, ensuring its relevance and reliability. Data analysis was conducted using IBM SPSS for exploratory factor analysis (EFA) and IBM AMOS for confirmatory factor analysis (CFA). Of the 33 initial survey items, the study identified 5 items related to privacy, 4 items concerning security, 5 items addressing threats, and 3 items focusing on communication. The findings confirm that these four factors—privacy, security, threats, and communication—are strongly interrelated, demonstrating high validity and reliability. These factors were further examined to assess young people's behavioral intentions to adopt the ISAS e-safety framework in their online activities. This study offers valuable insights for IT professionals and educators while providing practical recommendations for managers aiming to enhance Internet safety awareness among young users.

1. Introduction

Information technology (IT) and Information and Communication Technology (ICT) are exciting and fast-growing fields across the globe. Increased connectivity and access to a wide array of communication devices have enabled the growth of the Internet as an essential infrastructure in the communication sector. The ability to access diverse types of information hosted on the Internet has consequently made the world a global village, especially with globalization. This has, in turn, led to a situation where basic supervision of Internet use, especially among minors, is limited. Unethical hacking is a significant threat to Internet security (Alnajim et al., 2023). In Saudi Arabia, the number of Internet users has increased exponentially in the past decade. The number of people using the Internet in the country increased by 1.3 million between 2020 and 2021. Factors that favor the nation's quick adoption of Internet use include having a majority young population, increased smartphone use, and a higher-than-average income per capita. Saudi Arabia has a majority young population, with 51% being 25 years and below. Younger people use the Internet more often, contributing to Saudi Arabia's impressive Internet penetration rates.

The Internet provides users with various activities that they find appealing, and it allows them to interact with individuals from around the world with no restrictions. Youth has become an essential objective for this promotional concern because of the Internet's open accessibility (Browne and Hamilton-Giachritsis, 2005). Youth have been drawn to the rapidly expanding activities and techniques found on the Internet, which has led to Internet addiction. A dysfunctional attitude toward the Internet is considered "Internet addiction" (Young, 2004). According to several studies, youth are the most vulnerable group to becoming addicted to the Internet because they prefer to communicate with their peers through online social networking sites rather than in person (Caplan, 2005). People

* Corresponding Author.
Email Address: hsamra@kau.edu.sa (H. Samra)

https://doi.org/10.21833/ijaas.2025.03.014
Corresponding author's ORCID profile:
https://orcid.org/0000-0002-5199-3677
2313-626X/© 2025 The Authors. Published by IASE.

worldwide believe that college students pose a particularly hazardous risk due to their excessive Internet use. Several different mental disorders, such as anxiety, stress, and depression. Another study carried out in Cairo, Egypt, among youth hired from private and public schools, discovered that the prevalence of the disease was 0.8 percent (Reda et al., 2012). On the other side, Internet usage among Saudis is significantly higher than that of people in other countries. Most Saudi Arabian students participated in an online activity, as indicated by the fact that 98.2 percent of them did so (Abdel-Salam et al., 2019).

Addiction to the Internet is a concern that is becoming more widespread among students in Saudi Arabia (Abdel-Salam et al., 2019). There are many educational benefits to be gained from using the Internet; however, excessive Internet use can result in negative results such as social exclusion and poor academic performance. When the youth intentionally or unintentionally access or post improper information online or specifically target media applications, this can pose a risk to their mental health. Cohen-Almagor (2018) provided the chances that the youth face, some of which include receiving flirty texts, online interaction with strangers, face-to-face conferences with such strangers, damaging content, misapplication of private information, cyberbullying, and murder linked to online bullying. Cohen-Almagor (2018) found that the youth face these risks. These dangers are related to the user's online activities and the possibility of being targeted by phishing scams.

Different studies identified the models and frameworks to manage cybersecurity threats and maintain privacy, security, and communication of the information (Choong et al., 2019; Kabali et al., 2015; Zou et al., 2020). For instance, Edwards et al. (2018) investigated the perspectives of the youth (ages four to five years old) on the Internet. The report argues that because the youth of this age have become able to access the Internet at home without the help of their parents (for instance, due to contact display latest technology which makes individual use easier), they are vulnerable to dangers varying from "replying accidentally to enticements for online or in-app items purchased" to "going to experience inappropriate material" or "engaging in interaction with random persons." Since youth of this age are now capable of using the Internet at home without the assistance of their parents, the researchers claim. According to Edwards et al. (2018), some people believe that the youth cannot contextualize or conceive of the dangers they face. These studies are frequently carried out to determine the youth's levels of awareness regarding these risks. Unfortunately, these models were developed and deployed in developed countries and other contexts; particularly, these are not fitted to Saudi culture. In Saudi Arabia, there are not nearly enough safety and cybersecurity operations in cybercrime education (Alqurashi et al., 2020). On the other hand, students' awareness and abilities of e-safety regarding how it affects students have received far too little focus in recent years (Hassan et al., 2020). As a result, existing frameworks and models for online safety, often developed for other regions, fail to adequately address the unique cultural and technological challenges faced by Saudi youth. This highlights an urgent need for localized efforts in e-safety education and cybersecurity awareness to better protect young Internet users in the Kingdom.

In summary, the rapid rise of information and communications technology (ICT) has revolutionized how the world stays connected, giving people unprecedented access to the Internet and its vast resources. While this connectivity has brought the world closer together, it has also exposed young users to new risks. In Saudi Arabia, with its mainly young population, high smartphone adoption, and widespread Internet access, concerns have been growing about issues such as Internet addiction, exposure to harmful content, cyberbullying, and mental health challenges.

Many existing cybersecurity and safety models have been developed with different cultural contexts in mind, making them less effective in addressing the unique challenges faced by Saudi youth online. Despite the increased risks, there remains a significant gap in cybersecurity education and cybersecurity practices tailored to this demographic. This study aims to fill this gap by developing and demonstrating a culturally relevant ISAS cybersecurity framework designed to protect Saudi youth from these growing online threats and promote safer Internet use.

This study aims to address the critical online safety challenges faced by youth in Saudi Arabia and develop a tailored solution to mitigate these risks. The study makes specific contributions to research in the following ways:

- Assess the current state of Internet use among youth in Saudi Arabia, with a focus on addiction, exposure to inappropriate content, cyberbullying, and mental health risks.
- Evaluate the limitations of existing cybersecurity frameworks and safety models in addressing the specific cultural and technological needs of Saudi youth.
- Develop a culturally appropriate ISAS e-safety framework designed to mitigate Internet-related risks among Saudi youth.
- Validate the effectiveness of the proposed ISAS e-safety framework in promoting online safety for Saudi youth.

2. Proposed ISAS framework and parameters

2.1. Youth awareness of Internet usage

Protecting and raising awareness among youth is an important consideration now that most young people are spending more time surfing the Internet with their smart devices. Control is mainly in the form of time limitations rather than the content accessed. Despite controls, it is evident that dependence on technology continues to grow with outcomes that redirect us to the issue of addiction, especially to social media (Longstreet and Brooks, 2017). Mobile devices are essential when it comes to the use of social networks. Internet addiction disorder is associated with aggression and poor educational performance (Lim and Hastie, 2015). Internet addiction is inversely related to physical activity. Sahin and Lok (2018) further found a positive correlation between low physical activity and Internet addiction. More people can stay connected to these sites for longer, owing to the ease of use associated with smartphones and tablet computers. Regulating the Internet and gaming use among teenagers is necessary to safeguard this population from the harm of inappropriate use of technology. While many fall prey unknowingly, measures such as regular observation, time limits, and safeguards such as supervision must be instituted to ensure safety.

2.2. E-safety systems and implications

When evaluating the application of e-safety systems and privacy, the IT professionals address the process and procedures required to adopt privacy and security. Several studies have been motivated by the desire to recognize students' concerns regarding implementing technologies in the classroom (Khan and Hammami, 2019). In contrast, other studies have been inspired by the desire to identify ways to manage e-safety cost-effectively. Issues about students' safety fit within a more extensive agenda concerning student e-safety, which recognizes the need to establish the skills and knowledge necessary to keep students safe in the digital world. The methodology used to investigate scholarly exercise in e-safety concerning online cooperative groups. Competencies are required to use the benefits that information and communication technologies (ICTs) might provide, including e-safety in schools. Parmaxi et al. (2017) investigated e-safety in e-learning, the advantages and risks of online interaction, and standards for preparing organizations to manage e-safety. While most students were aware of the dangers posed by the Internet, many performed poorly on e-safety tests (e.g., in practice around password security). Although parents are generally supportive of using devices for educational purposes, there are still worries about Internet security.

Researchers have a significant amount of interest in the topic of fully comprehending and analyzing the e-safety regulations that are imposed on educational institutions. In this vein, Lorenz et al. (2012) investigated the various kinds and causes of safety risks, the remedies offered, the students' responses to these occurrences, and the solutions the students recommended. The results showed that many students are unaware of what e-safety is and believe that they were not associated in any way with an e-safety incident, even though they have been the target of an online attack. The awareness training is ineffective because it is drastically dissimilar to how students think and behave when confronted with real-life scenarios (Parmaxi et al., 2017). Even though it is the primary focus of the specific awareness training currently being done, blocking unwanted content is the least efficient option for the students. Awareness in such areas is also required for the youth responsible for setting the criteria for how their students will behave and cope with the issues that may arise (Lorenz et al., 2016). In the end, it is of the greatest priority for schools to formulate policies, techniques, and remedies that address the fundamental problems that the students face. Lorenz et al. (2019) investigated 201 e-safety-related stories displayed by students (12–16 years old), parents, school IT, managers, and police officers. The narratives plotted typical behavioral patterns, opinions, regulations, and restrictions concerning using social connections in Estonian schools and were told from the student's perspective. The findings showed that only a tiny percentage of schools have a clear policy regarding issues related to online safety. However, even these few policy documents at the school level fall short when addressing the problems most frequently brought up in the accounts provided by the students. Cyberbullying and exposure to illegal content continue to be safety issues that have not been adequately addressed and, in some cases, are not even detected. Similarly, Cranmer (2013) noted the e-safety perceptions of omitting youth. He demonstrates that the techniques these youth use to manage their e-safety are rudimentary and insufficient, which points to the necessity of further developing these online youth techniques and their level of digital literacy.

2.3. Challenges and issues of Internet usage by the youth

It should be one of our primary goals to instill a sense of reasonable scepticism in our youth generation and to encourage them to take preventive measures for their e-safety measures on Internet usage. Youth require empowerment through the advancement of resilient behaviors and abilities through the accumulation of experience, the carrying of risks, and the experiencing of failure. The study contends that shielding youth from the potential risks of the Internet by filtering the data they access will prevent them from acquiring the knowledge and abilities they will need to keep themselves safe in the future (Amichai-Hamburger and Etgar, 2018). It is essential to pay attention to ensuring that every member of our society can deal with potential dangers to their Internet use and capitalize on potential opportunities. On the other hand, disparities in levels of consciousness and interest in e-safety measures have already been brought to light (Majid et al., 2016; 2020). Research conducted in Singapore found that students who did not have access to the Internet were less worried about confidentiality issues and online bullying than those who did have access. This was the case even though Internet education is a required part of the curriculum there. Interestingly, there were disparities based on gender, expressing a higher level of concern. The position of technology in education systems is frequently driven by powers outside the system (i.e., government entities, propaganda) rather than being centered on the e-safety of the learner.

Advancements such as increased surveillance, monitoring of students' personal behavior, the use of big data, and the need to learn data analysis and technology pose challenges to maintaining effective e-safety measures. It is important to address the issues arising from these socio-technical trends. Rather than focusing on a strength-based approach that supports fair skill development in areas such as empathy, self-control, awareness, and access to support systems, current efforts tend to rely heavily on rules and regulations. This approach differs from one that builds on the strengths of individuals. To ensure that all young people—regardless of their education level, access to resources, or prior experience—benefit from e-safety, programs should aim to enhance their knowledge, digital skills, and ability to adapt in online environments.

Excessive Internet use is likely to lead to poor social skills among young people. The Internet provides many opportunities and harbors many dangers to users (Krasteva, 2018). This is compounded by the fact that introversion can lead to secrecy, hence the possibility that these children can form easy targets for groups or individuals keen on social ills such as criminal indoctrination and extremist behaviors. Compulsive Internet use is the opposite of enhancing social connectedness (McIntyre et al., 2015). It often culminates in realizing outcomes that are not the express choice of teenagers but those of the people they interact with on the Internet. There is a positive correlation between Internet addiction and low physical activity (Sahin and Lok, 2018). The Internet is mainly used for social communication and entertainment as opposed to educational purposes, especially among teenagers (Amichai-Hamburger et al., 2002). It creates a sense of anonymity for the user while providing freedom in deciding what to expose to others regarding social outlook and appearance (Amichai-Hamburger and Etgar, 2018). The assumption that one is safe can create a false feeling of security that affects interactions with others in real-life situations. This is a real problem, especially among introverts, as they are likely to find solace on the Internet, where no one can tell their fundamental behavioral characteristics.

2.4. Factors related to e-safety awareness

The protection of the Kingdom's economy, as well as its digital services and infrastructure, must be a key focus. Cybersecurity and e-safety awareness measures have become increasingly important in recent years. Therefore, the study assesses the factors that are related to the e-safety awareness framework in the following sub-sections.

2.4.1. Privacy awareness

According to the findings of a survey conducted by Choong et al. (2019), the youth exhibited ambiguity between the notions of passwords, privacy, and safety. This content is expected to cover data security aspects such as managing passwords and detecting scams; however, in practice, it generally focuses on privacy (i.e., e-safety). This is related to previous research that demonstrated that users have the propensity to give up privacy and security tools once they discover they are uncomfortable (Zou et al., 2020). Prior research has demonstrated the significance of security and privacy for awareness and attitude change, with unofficial narratives from friends and relatives being the most important factor (Rader et al., 2012). The climate of the youth has a significant role to play in the process of bringing attention to concerns regarding privacy and security. It is well-established that the concept of curiosity serves as an essential component of the motivational makeup for fostering learning in youth. Some research has been done on pure interest in the sense of privacy ability to comprehend and disclose (Rader et al., 2012). However, not a lot of work has centered on interaction to learn about privacy, particularly.

2.4.2 Security awareness

Information security includes understanding the issues surrounding e-safety and security. The students learn about online safety, privacy, and security, and how much of their instructional time are teachers allowed to devote to these subjects? There is a widespread consensus among information security professionals that individuals are the primary cause of information security-related issues. According to the statistics, most security breaches are the result of actions taken by employees within an organization, and the damage they cause can be significantly more severe than anything developed by hackers operating from the outside. As well, van der Walt et al. (2008) and Kruger et al. (2010), the youth in the field of information security are comprised of the awareness measures that they are already familiar with that are associated with information security. A more comprehensive education in security must be a high priority as the youth are increasingly attempting to access their gadgets and records on a variety of services alone without the oversight of the youth (Kabali et al., 2015), even though e-safety is the greatest priority for youth. The youth know it does not recognize or follow the best practices for security, which can result in the passing on of flawed practices to youth generations even when supervision and advice are provided.

2.4.3. Communication awareness

The students, media outlets, and academic institutions have expressed fears over the risks that the youth face in e-safety measures regularly and have shown the need for targeted solutions to minimize the harm that certain online activities could cause, especially to young people. These concerns have been voiced over several years. Lorenz et al. (2012) reported that e-safety training typically addresses MSN communication and issues with strangers (with the convenient solution of obstructing the unhappy person). However, today's communication has decided to move to social networking sites, where there is also a chance to chat. This is another very interesting result. There is a growing gap between those with access to technology and those without access. Therefore, communication in e-safety systems ensures the conversation between the Internet and the youth.

2.4.4. Threat awareness

Server maintenance, data misuse or theft, and disclosure of sensitive information are the primary concerns regarding online threats to the online school system (Kabali et al., 2015). The problem of protecting one's privacy has surfaced. Although the primary focus of our research was to analyze online safety incidents, it also alerts the e-learning community to the necessity of raising awareness among students regarding potential threats to their private information. Most college students are more susceptible to cyberattacks; this demonstrates that they do not place sufficient importance on maintaining their online security, and at the exact moment, they lack the understanding of potential security risks and the preventative measures that are required to avoid those. Therefore, Kruger et al. (2010) recommended that an individual's expertise and behavior have a positive bond in the prevention of cybersecurity threats, (McDaniel, 2013) stated that this relationship does not exist.

2.5. ISAS framework

Building on Sections 2.1-2.4 and acknowledging that existing cybersecurity models are not aligned with the unique cultural and technological landscape of Saudi Arabia, this study aims to develop a culturally tailored ISAS framework specifically designed for Saudi youth. Fig. 1 illustrates the theoretical framework of the ISAS, highlighting the four identified factors for investigation, which are discussed in the previous sub-sections.

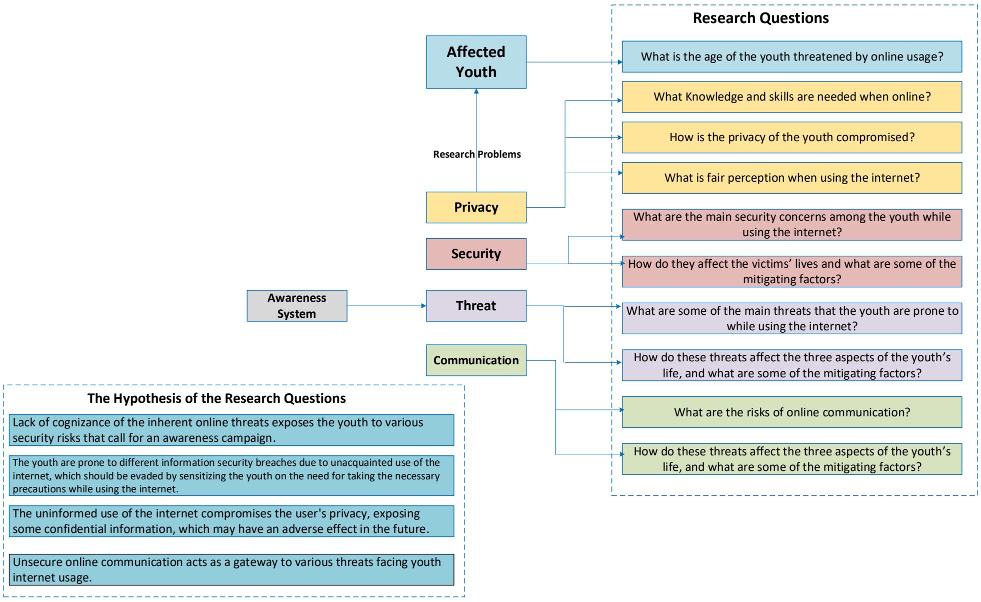
Research Questions
Affected Youth
What is the age of the youth threatened by online usage?
What Knowledge and skills are needed when online?
How is the privacy of the youth compromised?
Research Problems
What is fair perception when using the internet?
Privacy
What are the main security concerns among the youth while using the internet?
Security
How do they affect the victims' lives and what are some of the mitigating factors?
Awareness System
Threat
What are some of the main threats that the youth are prone to while using the internet?
Communication
How do these threats affect the three aspects of the youth's life, and what are some of the mitigating factors?
The Hypothesis of the Research Questions
What are the risks of online communication?
Lack of cognizance of the inherent online threats exposes the youth to various security risks that call for an awareness campaign.
How do these threats affect the three aspects of the youth's life, and what are some of the mitigating factors?
The youth are prone to different information security breaches due to unacquainted use of the internet, which should be evaded by sensitizing the youth on the need for taking the necessary precautions while using the internet.
The uninformed use of the internet compromises the user's privacy, exposing some confidential information, which may have an adverse effect in the future.
Unsecure online communication acts as a gateway to various threats facing youth internet usage.

Fig. 1: The proposed conceptual ISAS e-safety framework

3. Research methodology

This study adopted a quantitative research approach to validate the proposed ISAS framework, beginning with the proposed ISAS framework and parameters in Section 2 to develop survey items. A questionnaire was then designed, incorporating survey items adapted from prior research.

3.1. Research design

First, the questionnaire items were reviewed by an IT specialist and two IT professors for editing and revision. After making the necessary revisions and reformulating the items, the study continued with the pilot testing of the survey instrument. This pilot-testing stage uses a quantitative research design by administering a questionnaire (Östlund et al., 2011). In pilot-testing the survey, the study targeted 40 IT professionals to check whether the survey items were loaded correctly on 5-point Likert scales. The study runs the data in IBM SPSS to apply Principal Component Analysis (PCA) to check the factor loadings of the survey items. Subsequently, the study assessed the Cronbach's alpha for the four factors of the ISAS e-safety framework: Privacy (11 items), Security (12 items), Communication (4 items), and Threat (6 items). Finally, the study confirmed satisfactory factor loadings and Cronbach's alpha values.

3.2. Participants and data collection procedure

The study employed a purposive sampling method to specifically target IT professionals in Saudi Arabia, whose technical expertise was deemed crucial for the development and validation of the ISAS e-safety framework. This approach ensured that participants had the necessary knowledge and experience to provide informed feedback on the framework components and structure (Campbell et al., 2020). A survey was distributed using QuestionPro, a validated and reliable online platform recommended by La Trobe University for its data security features and user-friendly interface. Participants were informed that their participation was entirely voluntary, with clear assurances that their responses would remain confidential and anonymous, and no sensitive data would be disclosed.

Survey invitations were sent to 150 IT professionals on November 24, 2020. By January 12, 2021, a total of 92 responses had been received. To ensure the accuracy and integrity of the data, responses were carefully screened, and 58 incomplete questionnaires were excluded due to missing or inconsistent information. This resulted in 34 fully completed and valid responses, yielding a final response rate of 36.95%. Despite the challenges of securing a high response rate, the completed surveys provided valuable insights into the participants' perspectives, contributing significantly to the validation of the ISAS framework.

3.3. Measurement items

To develop the four-factor ISAS e-safety framework, the research assigned 11 survey items to the privacy factor, 12 to the security factor, 6 to the threat factor, and 4 to the communication factor, resulting in a total of 33 survey items in the second survey. Ultimately, the ISAS framework consists of four factors: privacy, security, connectivity, and threat. A five-point Likert scale was used to rate the awareness amongst participants regarding the perspectives of the ISAS e-safety framework employed in the study. The Likert scale is adopted to measure "respondents' attitudes, beliefs, emotions, feelings, perceptions, personality characteristics and other psychological constructs" (Spector, 2004, p. 3).

3.4. Data analysis

This study used a survey questionnaire to test the validity and reliability of the newly developed survey items surrounding four factors in the ISAS e-safety framework, i.e., privacy, security, threat, and communication. First, the study applied exploratory factor analysis (EFA) to get the variance extracted and valid measures. By applying EFA, the study used IBM SPSS software. Second, the study used IBM AMOS to do confirmatory factor analysis (CFA) to ensure the validity of the new measurement scales (Shek and Yu, 2014). The reliability of the survey instrument was evaluated using Cronbach's alpha coefficient in IBM SPSS.

4. ISAS framework scale development and validation

4.1. Normal distribution

The presumption of normal data is implicit in parametric testing. Descriptive statistics allow for examining a distribution's skew and kurtosis. When using EFA, values of skewness that fall between -2 and +2 are considered acceptable, whereas kurtosis that falls within the range of -7 to +7 is considered adequate. Finally, the study found that there was normal data for further statistical analysis.

4.2. Exploratory factor analysis

Exploratory factor analysis, sometimes known as EFA, is a statistical technique used in multivariate statistics (Fabrigar and Wegener, 2011). The principal component approach with oblique rotation was utilised for this analysis. Because the study anticipated that the factors would be associated with one another, the study utilised oblique rotation (Fabrigar and Wegener, 2011). During this iteration of the EFA (Kaiser–Meyer–Olkin (KMO) equals 0.828; Bartlett's test of sphericity equals 2221.147; df equals 528; p=0.000), 12 items (the communalities 0.50) were eliminated. Because of this, an additional round of EFA were performed with the 21 items that were left using the principal component approach with component rotation matrix (Kaiser–Meyer–Olkin (KMO) = 0.838; Bartlett's test of sphericity = 1330.530; df = 210; p=0.000). The results of the KMO and Bartlett's test are presented in Table 1. Finally, the data have good accuracy and relevancy.

Table 1: KMO and Bartlett's test

Kaiser-Meyer-Olkin measure of sampling adequacy		.838
Bartlett's test of sphericity	Approx. Chi-Square	1330.530
	DF	210
	Sig	.000

4.2.1. Total variance explained and common method bias (CMB)

The study also examined CMB if the responses were biased. Common method bias (CMB) occurs when variances in responses are produced by the measurement scales rather than the participants' real behavioural patterns that the instruments aim to uncover (MacKenzie et al., 2011). Therefore, the study used the Herman sing factor method by Podsakoff et al. (2012) to check CMB in the dataset. The study loaded 4 factors of the cybersecurity scale into one single factor with the component factor axis method. In this condition, the total variance of the scales should not be more than 50%. Finally, the study found that the total variance explained was 31.630%, less than 50%, so there was no biasness.

4.2.2. Factor loadings

The amount of variance that is accounted for by a variable on a given factor can be seen through factor loading. A general rule of thumb when using the methodology is to use a factor loading of 0.7 or above to indicate that the factor removes significant variance from the studied variable (Rababah et al., 2022). When a new item is being developed, it is important that every item's factor loading be more than 0.5. When dealing with established items, the factor loading for each item needs to be at least 0.6. (Awang et al., 2015). The study is developing new measurement items, so it follows the criteria of Awang et al. (2015), which recommends that the factor loadings should be higher than 0.5, which is acceptable (Table 2). After a series of PCAs, there were privacy factors with 9 items, security with 4 items, threat with 5 items, and communication with 3 items. Out of 33 items, 18 items were highly loaded on the latent factors.

The study also tested the reliability of the newly developed scales. The study applied the Cronbach's alpha technique to test the internal consistency of four measurement factors of cybersecurity. Kline suggested that the Cronbach alpha value for each factor/variable should be higher than 0.7 (Wang and Cunningham, 2005), which is the acceptance criteria for internal consistency. Finally, the study meets the criteria of factor loading and Cronbach's alpha.

4.3. Confirmatory factor analysis (CFA)

A confirmatory factor analysis (CFA) was carried out with the use of the covariance matrix to provide additional verification of the latent structure discovered by the EFA analysis. The second round of data was collected by IBM AMOS to test the validity of the measurement factors (i.e., cybersecurity). The study runs a series of confirmatory factor analyses to ensure the validity of the measures and items of the factors. The study further removed 4 items of privacy factors as PF6, PF9, PF10, and PF11, because their factor loadings were lower than 0.7 as per the suggested criteria in CFA (Zhang et al., 2012). Finally, the study found 5 items of the privacy factor, 4 items of the security factor, 5 items of threat, and 3 items of the communication factor (Table 3).

Table 2: Factor loadings and Cronbach's alpha

	Privacy factor	Security factor	Threat factor	Communication factor
PF1	.625			
PF2	.649			
PF5	.750			
PF6	.653			
PF7	.814			
PF8	.776			
PF9	.688			
PF10	.624			
PF11	.537			
SF9			.748	
SF10			.660	
SF11			.713	
SF12			.635	
Threat1		.738		
Threat2		.586		
Threat3		.581		
Threat4		.615		
Threat6		.761		
CF1				.720
CF3				.793
CF4				.619
Cronbach’s alpha				
	0.922	0.887	0.884	0.849

4.3.1. Convergent and discriminant validity

Secondly, the scores of the four factors' average variance extracted (AVE) were higher than the crucial value of 0.50, but all loadings were higher than 0.7 and meaningful at p=0.000 (Anthony et al., 2007). The findings demonstrated a significant degree of correlation between several items that were measured along the same dimension, indicating that the convergent validity of the measure was adequate. The discriminant validity of the measure was also investigated in the third step of the process. As shown in Fig. 2, There were also strong correlation coefficients among the factors of cybersecurity, i.e., privacy factors, security factors, threats and communication factors (see appendixes), which are below the 0.85 crucial value and smaller than the square roots of the AVE of the respective factor (Chen et al., 2014). Because of these findings, the discriminant validity of the scale was found to be satisfactory, given that the disparities between these dimensions were found to be substantial. In conclusion, it is possible to conclude that the evaluation of the measurement model provided support for the reliability and validity of the latent constructs.

Table 3: Factor loadings

Measurement scales	1	2	3	4
Privacy factors				
1. I am aware that the Internet is a safe environment.	.847			
2. It is hard to find a reliable source to educate us about Internet security information.	.872			
5. I share my personal information online	.844			
7. I sometimes leave my pc unattended	.773			
8. I know well how firewall important	.752			
Security factors				
9. I know how to respond to phishing attacks		.776		
10. I feel a phishing attack cannot steal my personal information without my knowledge		.839		
11. I open links that say I won prizes		.805		
12. I know how to identify fake emails, websites, or links		.832		
Threats				
I use public Wi-Fi that does not require a password			.819	
I use a VPN wherever possible			.819	
While using public Wi-Fi, I log in to sensitive websites, such as bank websites, or others that have my personal information.			.801	
I always keep my AirDrop or file sharing on			.778	
I know how to analyze information on the Internet to know if that is commercial or a threat			.715	
Communication factors				
I know well what cyberbullying is and how to deal with it				.774
I do chat with anonymously				.857
When you are online, do you pretend to say you are older than your real age				.795

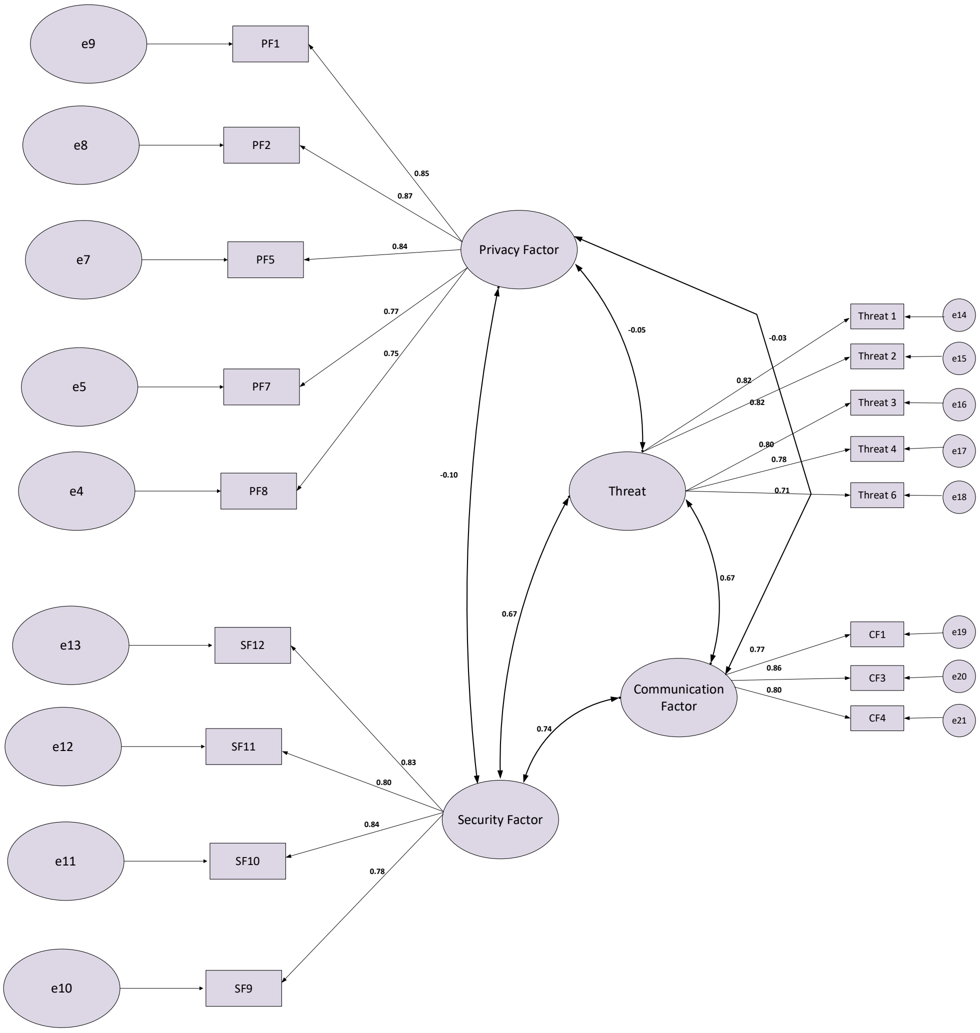

Fig. 2: Confirmatory factor analysis

4.3.2. Model fit indices

The study ensured other goodness-of-fit indicators likewise suggested that the four-factor model had an excellent overall fit to a 92-sample size (Chen et al., 2014; Zhang et al., 2012). RMSEA is an acronym for "root mean square error of approximation," whose value should fall within the range of 0.08 and 0.1 are acceptable (Kääriäinen et al., 2011). A CFI greater than 0.9 indicates an acceptable fit. If the TLI is more than 0.9, the fit is considered adequate. A value of 0.95 for the NFI implies that the model of interest enhances the fit by 95. TLI value should be greater than or equal to 0.90 (Byrne, 2001). The goodness-of-fit index was 0.806, the CFI was 0.914, and the incremental fit metrics were all greater than the 0.80 significance threshold. The parsimony comparison fit indices were also not lower than the 0.50 significance threshold, and the RMSEA value was 0.079, below the 0.08 significance threshold. Finally, the study found that all indices fitted with the conceptual model.

5. Discussion

The development of an e-safety system is crucial to support youth in safely navigating the Internet, as they require greater awareness to protect themselves from online threats such as hacking, identity theft, and exposure to harmful content (Akram and Ping, 2020). This system was necessary due to the lack of adequate Internet safety awareness programs in Saudi Arabia, particularly for young users. The study identified four key factors essential to an effective e-safety system: privacy, security, threats, and communication. The results indicated that all five privacy-related items received strong responses, highlighting how students perceive Internet safety measures to protect themselves from online threats and security vulnerabilities. Unethical hacking poses a significant risk to the integrity of the Internet, and the e-safety system enhances resilience against cyberbullying, identity theft, and other youth-related cybercrimes, which erode the moral values of Saudi culture. Given the rapid increase in Internet penetration rates in Saudi Arabia, implementing an e-safety system (ISAS) is vital to safeguarding the growing number of young Internet users.

As mentioned before, youth in Saudi Arabia are becoming increasingly addicted to the Internet, making the implementation of an e-safety system essential to protect them by promoting safe Internet usage. According to our study's findings, students from high schools, colleges, and universities will benefit from Internet safety awareness programs, and the newly developed e-safety system will help them navigate the Internet securely and without disruption. Several examples from the Saudi context illustrate the growing scale of youth Internet usage, such as a study of female university students in Dammam, where over two-thirds of participants experienced problematic online use (38%) and Internet addiction (Barayan et al., 2018). In addition, Khan and Hammami (2019) found that girls were significantly more likely than boys to be addicted to the Internet. Consequently, the proposed e-safety system is designed to help young people use the Internet cautiously, protecting them from misinformation and spam. The ISAS e-safety system operates through four key mechanisms:

1. Privacy: The system educates youth on privacy options, emphasizing the importance of privacy settings on devices to prevent unauthorized access to personal information.
2. Security: The security mechanism is particularly effective during times of crisis, when safeguarding the online environment is critical. Youth can participate in awareness programs led by experts, while school administrators are responsible for providing basic security measures. As Hope (2010) argued, youth must learn to avoid insecure online services, and this principle is integral to the data security methods included in the e-safety system.
3. Communication: This factor focuses on raising awareness about safe Internet usage among youth. The desire to achieve security, particularly during periods of vulnerability, underscores the importance of implementing an e-safety system that can detect hacking attempts and secure smartphone communications.
4. Threats: The system educates youth on the various threats to computer security, helping them recognize and avoid dangers that could compromise their systems. The study highlights that Internet-related threats in Saudi Arabia have resulted in billions of dollars in damages each year, yet research on this topic remains limited. This component of the e-safety system is designed to mitigate these risks by identifying potential threats and providing preventative measures.

5.1. Managerial implications

As mentioned before, this study aims to enhance the technical awareness of Internet security among youth in Saudi Arabia by developing the ISAS e-safety system. It explores security awareness programs and examines common modes of cyberattacks, providing youth with a deeper understanding of how to safely navigate the Internet. The study emphasizes that schools should adopt their own e-safety systems, using the proposed e-safety framework as a foundation. In addition, a national Internet policy for youth should be established to ensure uniform and safe Internet usage across all schools. Currently, Saudi Arabia lacks a dedicated e-safety system to address youth misuse of the Internet, highlighting the urgency of implementing such a framework. The study's e-safety framework identifies key threats and vulnerabilities, offering a structured approach to mitigating these risks. The absence of a clear e-safety policy has led to confusion, as the government has urged the adoption of e-safety systems without providing clear guidance or resources. A national e-safety framework should be developed and consistently updated, with sufficient resources allocated for creating teaching materials and training staff to model appropriate e-safety behaviors.

Teachers need to be empowered through workshops and training to effectively teach Internet safety. Based on the study's findings, an e-safety framework can be implemented to help youth manage Internet hazards, regardless of where they are. This system would address existing e-safety concerns in schools, providing a safer and more secure online environment for young users.

In summary, the implications of these findings are significant for both policy and practice. Policymakers should leverage the ISAS framework to develop standardized e-safety guidelines tailored to Saudi Arabia's cultural context. Schools and educational institutions, in turn, can incorporate the framework into digital literacy curricula to empower youth with practical skills for navigating online risks. Furthermore, collaboration between the government, private sectors, and educational institutions is essential to ensure sustained implementation and continuous refinement of e-safety programs.

6. Conclusion and future directions

This study underscores the urgent need to enhance Internet safety awareness among Saudi youth through the implementation of the ISAS e-Safety Framework. As Internet use among youth continues to rise, so do the risks associated with it, making it imperative to adopt a comprehensive approach to e-safety that effectively addresses the unique challenges they face. Although there is some awareness of online risks among young users, a significant gap still exists in their understanding of effective strategies to protect themselves online and their ability to apply this knowledge in practical scenarios. Therefore, the ISAS Framework focuses on four key factors: privacy, security, connectivity, and threat awareness, each designed to equip youth with the tools and knowledge to safely navigate the digital world.

The study focused on employing a rigorous methodology to develop and validate the ISAS framework. First, it proposed a framework and parameters to identify relevant survey items. These items were refined through pilot testing, where the questionnaire was administered to 40 IT professionals to ensure the clarity and functionality of the questions. Principal Component Analysis (PCA) was applied using IBM SPSS to assess the factor loadings of the survey items. The study also examined reliability using Cronbach's alpha for the four ISAS factors: privacy, security, connectivity, and threat. Additionally, the study ensured the framework's robustness by conducting exploratory factor analysis (EFA) using IBM SPSS, followed by confirmatory factor analysis (CFA) with IBM AMOS. This comprehensive and systematic approach validated the ISAS framework, confirming its reliability as an effective tool for improving youth cybersecurity awareness. It also provides a strong foundation for future research and practical applications.

While the study provides valuable insights, it is important to recognize its limitations to guide future research. The small sample size, which primarily consisted of IT professionals, may limit the generalizability of the findings. To gain a more comprehensive understanding of youth experiences and the challenges they face in adopting e-safety measures, future research should include a more diverse population, particularly involving youth themselves. Furthermore, although the ISAS framework is designed for the Saudi context, its principles can be adapted for use in other global settings facing similar e-safety challenges.

Future work will also involve conducting comparative analysis of e-safety frameworks across different cultural contexts to evaluate their effectiveness and adaptability. This would help highlight the unique cultural and technological considerations addressed by the ISAS framework and assess its applicability in diverse global settings.

The proposed ISAS e-safety framework aims to reduce the risks associated with cyberbullying, identity theft, and other online threats. This initiative not only addresses immediate concerns but also fosters a culture of responsible Internet use. The successful implementation of the ISAS framework has the potential to significantly contribute to a safer online environment for the next generation, laying the groundwork for a more informed, resilient, and secure digital future. Finally, we recommend that:

- Educational institutions should adopt the ISAS framework as part of mandatory curricula focused on digital literacy and cybersecurity awareness. Key components, such as privacy, security, threat awareness, and safe online communication, can be taught through interactive workshops, online modules, and practical exercises.
- Government and education policymakers should establish comprehensive e-safety policies based on the ISAS framework to ensure a consistent approach to cybersecurity across all schools and institutions.

List of abbreviations

ISAS	Internet security awareness and safety
IT	Information technology
ICT	Information and communication technology
EFA	Exploratory factor analysis
CFA	Confirmatory factor analysis
SPSS	Statistical Package for the Social Sciences
AMOS	Analysis of moment structures
PCA	Principal component analysis
AVE	Average variance extracted
CMB	Common method bias
DF	Degrees of freedom
Sig	Significance
KMO	Kaiser–Meyer–Olkin
RMSEA	Root mean square error of approximation
CFI	Comparative fit index
TLI	Tucker–Lewis index
NFI	Normed fit index
VPN	Virtual private network
MSN	Microsoft Network
CF	Communication factor
PF	Privacy factor
SF	Security factor

Compliance with ethical standards

Ethical considerations

This study was conducted in accordance with the ethical standards of La Trobe University and the 1964 Helsinki Declaration and its later amendments. Ethics approval for this research was obtained from the La Trobe University Human Ethics Committee

(Reference number HEC21080). Participation was voluntary, and informed consent was obtained from all participants. All responses were collected anonymously, and participant confidentiality was strictly maintained.

Conflict of interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

Abdel-Salam DM, Alrowaili HI, Albedaiwi HK, Alessa AI, and Alfayyadh HA (2019). Prevalence of Internet addiction and its associated factors among female students at Jouf University, Saudi Arabia. Journal of the Egyptian Public Health Association, 94(1): 12. https://doi.org/10.1186/s42506-019-0009-6 **PMid:32813134 PMCid:PMC7366308**

Akram J and Ping L (2020). How to build a vulnerability benchmark to overcome cyber security attacks. IET Information Security, 14(1): 60-71. https://doi.org/10.1049/iet-ifs.2018.5647

Alnajim AM, Habib S, Islam M, AlRawashdeh HS, and Wasim M (2023). Exploring cybersecurity education and training techniques: A comprehensive review of traditional, virtual reality, and augmented reality approaches. Symmetry, 15(12): 2175. https://doi.org/10.3390/sym15122175

Alqurashi RK, AlZain MA, Soh B, Masud M, and Al-Amri J (2020). Cyber-attacks and impacts: A case study in Saudi Arabia. International Journal, 9(1): 217-224. https://doi.org/10.30534/ijatcse/2020/33912020

Amichai-Hamburger Y and Etgar S (2018). Personality and Internet use: The case of introversion and extroversion. In: Attrill-Smith A, Fullwood C, Keep M, and Kuss DJ (Eds.), The Oxford handbook of cyberpsychology. Oxford University Press, Oxford, UK. https://doi.org/10.1093/oxfordhb/9780198812746.013.4

Amichai-Hamburger Y, Wainapel G, and Fox S (2002). On the Internet no one knows I'm an introvert": Extroversion, neuroticism, and Internet interaction. Cyberpsychology and Behavior: The Impact of The Internet, Multimedia and Virtual Reality on Behavior and Society, 5(2): 125–128. https://doi.org/10.1089/109493102753770507 **PMid:12025878**

Anthony JL, Assel MA, and Williams JM (2007). Exploratory and confirmatory factor analyses of the DIAL-3: What does this "developmental screener" really measure? Journal of School Psychology, 45(4): 423-438. https://doi.org/10.1016/j.jsp.2007.02.003

Awang Z, Afthanorhan A, Mohamad M, and Asri MAM (2015). An evaluation of measurement model for medical tourism research: The confirmatory factor analysis approach. International Journal of Tourism Policy, 6(1): 29-45. https://doi.org/10.1504/IJTP.2015.075141

Barayan SS, Al Dabal BK, Abdelwahab MM, Shafey MM, and Al Omar RS (2018). Health-related quality of life among female university students in Dammam district: Is Internet use related? Journal of Family and Community Medicine, 25(1): 20-28. https://doi.org/10.4103/jfcm.JFCM_66_17 **PMid:29386958 PMCid:PMC5774039**

Browne KD and Hamilton-Giachritsis C (2005). The influence of violent media on children and adolescents: A public-health approach. The Lancet, 365(9460): 702-710. https://doi.org/10.1016/S0140-6736(05)17952-5 **PMid:15721477**

Byrne BM (2001). Structural equation modeling with AMOS, EQS, and LISREL: Comparative approaches to testing for the factorial validity of a measuring instrument. International Journal of Testing, 1(1): 55-86. https://doi.org/10.1207/S15327574IJT0101_4

Campbell S, Greenwood M, Prior S, Shearer T, Walkem K, Young S, Bywaters D, and Walker K (2020). Purposive sampling: Complex or simple? Research case examples. Journal of Research in Nursing, 25(8): 652-661. https://doi.org/10.1177/1744987120927206 **PMid:34394687 PMCid:PMC7932468**

Caplan SE (2005). A social skill account of problematic Internet use. Journal of Communication, 55(4): 721-736. https://doi.org/10.1111/j.1460-2466.2005.tb03019.x

Chen W, Gao Y, Xie W, Gong L, Lu K, Wang W, Li Y, Liu X, Zhang H, Dong H, and Zhang W (2014). Genome-wide association analyses provide genetic and biochemical insights into natural variation in rice metabolism. Nature Genetics, 46(7): 714-721. https://doi.org/10.1038/ng.3007 **PMid:24908251**

Choong YY, Theofanos M, Renaud K, and Prior S (2019). Case study: Exploring children's password knowledge and practices. In the Proceedings 2019 Workshop on Usable Security (USEC), The Internet Society, San Diego, USA. https://doi.org/10.14722/usec.2019.23027

Cohen-Almagor R (2018). Social responsibility on the Internet: Addressing the challenge of cyberbullying. Aggression and Violent Behavior, 39: 42-52. https://doi.org/10.1016/j.avb.2018.01.001

Cranmer S (2013). Listening to excluded young people's experiences of e-safety and risk. Learning, Media and Technology, 38(1): 72-85. https://doi.org/10.1080/17439884.2012.658405

Edwards S, Nolan A, Henderson M, Mantilla A, Plowman L, and Skouteris H (2018). Young children's everyday concepts of the Internet: A platform for cyber-safety education in the early years. British Journal of Educational Technology, 49(1): 45-55. https://doi.org/10.1111/bjet.12529

Fabrigar LR and Wegener DT (2011). Exploratory factor analysis. Oxford University Press, Oxford, UK. https://doi.org/10.1093/acprof:osobl/9780199734177.001.0001

Hassan T, Alam MM, Wahab A, and Hawlader MD (2020). Prevalence and associated factors of Internet addiction among young adults in Bangladesh. Journal of the Egyptian Public Health Association, 95(1): 3. https://doi.org/10.1186/s42506-019-0032-7 **PMid:32813097 PMCid:PMC7364753**

Hope A (2010). Seductions of risk, social control and resistance to school surveillance. In: Monahan T and Torres RD (Eds.), Schools under Surveillance: Cultures of control in public education: 230-245. Rutgers University Press, New Brunswick and London, UK. https://doi.org/10.36019/9780813548265-014

Kääriäinen M, Kanste O, Elo S, Pölkki T, Miettunen J, and Kyngäs H (2011). Testing and verifying nursing theory by confirmatory factor analysis. Journal of Advanced Nursing, 67(5): 1163-1172. https://doi.org/10.1111/j.1365-2648.2010.05561.x **PMid:21226874**

Kabali HK, Irigoyen MM, Nunez-Davis R, Budacki JG, Mohanty SH, Leister KP, and Bonner RL (2015). Exposure and use of mobile media devices by young children. Pediatrics, 136(6): 1044-1050. https://doi.org/10.1542/peds.2015-2151 **PMid:26527548**

Khan HU and Hammami H (2019). Measuring Internet addiction in Europe-based knowledge societies: A case study of France. International Journal of Business Information Systems, 32(2): 199-218. https://doi.org/10.1504/IJBIS.2019.103075

Krasteva N (2018). Existing dangers for the child on the internet. International Conference Knowledge-Based Organization, 24(2): 206-211. https://doi.org/10.1515/kbo-2018-0091

Kruger H, Drevin L, and Steyn T (2010). A vocabulary test to assess information security awareness. Information Management and Computer Security, 18(5): 316–327. https://doi.org/10.1108/09685221011095236

Lim M and Hastie T (2015). Learning interactions via hierarchical group-lasso regularization. Journal of Computational and Graphical Statistics, 24(3): 627-654. https://doi.org/10.1080/10618600.2014.938812 **PMid:26759522 PMCid:PMC4706754**

Longstreet P and Brooks S (2017). Life satisfaction: A key to managing Internet and social media addiction. Technology in Society, 50: 73-77. https://doi.org/10.1016/j.techsoc.2017.05.003

Lorenz B, Kikkas K, and Laanpere M (2012). Comparing children's e-safety strategies with guidelines offered by adults. Electronic Journal of e-Learning, 10(3): 326-338.

Lorenz B, Kikkas K, Laanpere M, and Laugasson E (2016). A model to evaluate digital safety concerns in school environment. In the Learning and Collaboration Technologies: 3rd International Conference, LCT 2016, Held as Part of HCI International 2016, Springer International Publishing. Toronto, Canada: 707-721. https://doi.org/10.1007/978-3-319-39483-1_64

Lorenz B, Kikkas K, Sõmer T, and Laugasson E (2019). Cybersecurity within the curricula of informatics: the Estonian perspective. In the 12th International Conference on Informatics in Schools: Situation, Evolution, and Perspectives, Springer International Publishing, Larnaca, Cyprus: 159-171. https://doi.org/10.1007/978-3-030-33759-9_13

MacKenzie SB, Podsakoff PM, and Podsakoff NP (2011). Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. MIS Quarterly, 35(2): 293-334. https://doi.org/10.2307/23044045

Majid S, Chang YK, and Foo S (2016). Auditing information literacy skills of secondary school students in Singapore. Journal of Information Literacy, 10(1): 44-66. https://doi.org/10.11645/10.1.2068

Majid S, Foo S, and Chang YK (2020). Appraising information literacy skills of students' in Singapore. Aslib Journal of Information Management, 72(3): 379-394. https://doi.org/10.1108/AJIM-01-2020-0006

McDaniel AE (2013). Securing the information and communications technology global supply chain from exploitation: Developing a strategy for education, training, and awareness. In the Proceedings of the Informing Science and Information Technology Education Conference, Informing Science Institute, Porto, Portugal: 313–324. https://doi.org/10.28945/1813

McIntyre E, Wiener KK, and Saliba AJ (2015). Compulsive Internet use and relations between social connectedness, and introversion. Computers in Human Behavior, 48: 569-574. https://doi.org/10.1016/j.chb.2015.02.021

Östlund U, Kidd L, Wengström Y, and Rowa-Dewar N (2011). Combining qualitative and quantitative research within mixed method research designs: A methodological review. International Journal of Nursing Studies, 48(3): 369-383. https://doi.org/10.1016/j.ijnurstu.2010.10.005 **PMid:21084086 PMCid:PMC7094322**

Parmaxi A, Papadamou K, Sirivianos M, and Stamatelatos M (2017). E-safety in Web 2.0 learning environments: A research synthesis and implications for researchers and practitioners. In the Learning and Collaboration Technologies. Novel Learning Ecosystems: 4th International Conference, Springer International Publishing, Vancouver, Canada, 249-261. https://doi.org/10.1007/978-3-319-58509-3_20

Podsakoff PM, MacKenzie SB, and Podsakoff NP (2012). Sources of method bias in social science research and recommendations on how to control it. Annual Review of Psychology, 63(1): 539-569. https://doi.org/10.1146/annurev-psych-120710-100452 **PMid:21838546**

Rababah JA, Al-Hammouri MM, and Aldalaykeh M (2022). Validation and measurement invariance of the Arabic health literacy questionnaire. Heliyon, 8(4): e09301. https://doi.org/10.1016/j.heliyon.2022.e09301 **PMid:35497048 PMCid:PMC9043993**

Rader E, Wash R, and Brooks B (2012). Stories as informal lessons about security. In the Proceedings of the Eighth Symposium on Usable Privacy and Security, ACM, Washington D.C., USA: 1-17. https://doi.org/10.1145/2335356.2335364 **PMid:22465494 PMCid:PMC3358468**

Reda M, Rabie M, Mohsen N, and Hassan A (2012). Problematic Internet users and psychiatric morbidity in a sample of Egyptian adolescents. Psychology, 3(8): 626-631. https://doi.org/10.4236/psych.2012.38096

Sahin M and Lok S (2018). Relationship between physical activity levels and Internet addiction of adults. Journal of Depression and Anxiety, 7(2): 1-4. https://doi.org/10.4172/2167-1044.1000310

Shek DT and Yu L (2014). Confirmatory factor analysis using AMOS: A demonstration. International Journal on Disability and Human Development, 13(2): 191-204. https://doi.org/10.1515/ijdhd-2014-0305

van der Walt M, Maree K, and Ellis S (2008). A mathematics vocabulary questionnaire for use in the intermediate phase. South African Journal of Education, 28(4): 489-504. https://doi.org/10.15700/saje.v28n4a210

Wang WC and Cunningham EG (2005). Comparison of alternative estimation methods in confirmatory factor analyses of the general health questionnaire. Psychological Reports, 97(1): 3-10. https://doi.org/10.2466/pr0.97.1.3-10 **PMid:16279297**

Young KS (2004). Internet addiction: A new clinical phenomenon and its consequences. American Behavioral Scientist, 48(4): 402-415. https://doi.org/10.1177/0002764204270278

Zhang H, Zhang J, Cheng S, Lu S, and Shi C (2012). Role of constraints in Chinese calligraphic landscape experience: An extension of a leisure constraints model. Tourism Management, 33(6): 1398-1407. https://doi.org/10.1016/j.tourman.2012.01.001

Zou Y, Roundy K, Tamersoy A, Shintre S, Roturier J, and Schaub F (2020). Examining the adoption and abandonment of security, privacy, and identity theft protection practices. In the Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, ACM, Honolulu, USA: 1-15. https://doi.org/10.1145/3313831.3376570