sustainability

MDPI

Article

Investigating the Effect of Students' Knowledge, Beliefs, and Digital Citizenship Skills on the Prevention of Cybercrime

Hosam A. Althibyani * and Abdulrahman M. Al-Zahrani

Department of Educational Technology, College of Education, University of Jeddah, Jeddah 21959, Saudi Arabia; ammzahrani@uj.edu.sa

* Correspondence: halthibyani@uj.edu.sa; Tel.:+966-555585010

Abstract: The growing prevalence of cybercrime, particularly among young adults, necessitates the promotion of digital citizenship to educate students about responsible online behavior and to equip them with the skills to mitigate cyber risks. The specific objective of this study was to investigate the effect of digital citizenship skills on the prevention of cybercrime among higher education students. A mixed-method approach, including surveys and interviews, was employed to collect data from 652 students in Saudi Arabia. This study found that digital citizenship generally has a significant impact on students' awareness and prevention of cybercrime through the development of responsible online behavior. Knowledge of digital law came first, followed by beliefs about digital manners. Digital communication skills came third, followed by digital rights, knowledge, and duties in fourth place. Then, digital commerce skills and digital health beliefs came fifth and sixth, respectively. This was followed by digital access skills, then digital security, and finally digital culture. The results also revealed a negative statistical relationship between digital citizenship and cybercrimes' various forms including national, financial, banking, social, immoral, insulting, slanderous, defaming, threatening, and harassment in virtual learning environments. These findings have significant implications for the understanding of how higher education institutions can promote digital citizenship and prevent cybercrime by integrating digital citizenship education into their curriculum, providing training for educators, and establishing clear policies and guidelines for responsible online behavior.

Keywords: cybercrime; digital citizenship; online learning; higher education; digital security; sustainability

Citation: Althibyani, H.A.; Al-Zahrani, A.M. Investigating the Effect of Students' Knowledge, Beliefs, and Digital Citizenship Skills on the Prevention of Cybercrime. *Sustainability* **2023**, *15*, 11512. https://doi.org/10.3390/su151511512

Academic Editor: Harris Wu

Received: 25 May 2023
Revised: 18 June 2023
Accepted: 17 July 2023
Published: 25 July 2023

1. Introduction

The 21st century is indeed characterized as the century of technological and informatics advancements [1]. The rapid development of digital technology and the internet has led to significant changes in the way we live, work, and communicate [2]. This has brought numerous opportunities and benefits, but it has also created new challenges and risks. One of the key features of the 21st century is the proliferation of digital devices and platforms. Smartphones, tablets, laptops, and other digital devices have become ubiquitous, allowing people to stay connected and access information from anywhere at any time [3]. The internet has also become an integral part of our daily lives, providing access to vast amounts of information, communication tools, and online services [1,2].

However, the rapid pace of technological advancements has also raised concerns about privacy, security, and the impact of technology on society [4]. The widespread use of social media and online platforms has led to concerns about the spread of misinformation, cyberbullying, and the potential misuse of personal data [5]. Moreover, effects include obliterating national cultures, eliminating privacy and causing many psychosocial problems that threaten students' psychological stability, such as feeling isolated, depressed, and anxious, as well as feelings of frustration and jealousy [6]. Furthermore, the prevalence of cybercrime that is often practiced against students constitutes abuses of technology among

individuals, such as extortion, exploitation, seduction, pornography, and cyberbullying in all its forms of insulting, evasion, deception, and immoral tweets that pose a threat to citizenship and cultural identity [7].

In the Arab world in general—and Saudi Arabia in particular—the issues are no more than misuse because they are centered on poor choice, excessive use of technology, and encroachment on others for self-validation and skills, which is a result of lack of knowledge of digital citizenship ethics and the harms of cybercrime [8]. This highlights the responsibility of educational institutions such as universities to protect young people from the risks of cybercrime [9]. This interest in citizens and students of higher education in Saudi Arabia was reflected in the establishment of the National Cyber Security Authority on 31 October 2007, and the authority has launched several important initiatives and projects that have contributed to enhancing cybersecurity in Saudi Arabia [10].

Digital citizenship and cybercrime are linked with several of the Sustainable Development Goals (SDGs), including SDG 4—Quality Education. Digital citizenship education can help to promote digital literacy and responsible use of digital technology among students, which is essential for achieving SDG 4. Moreover, they affect SDG 5—Gender Equality. Cybercrime and online harassment often affect women and girls disproportionately. Promoting digital citizenship and cyber-safety can help to create a safer and more inclusive online environment for all individuals, regardless of gender. In addition, digital technology has the potential to improve urban planning and resource management, but cybercrime can pose a significant threat to the safety and security of communities. Effective digital security measures are essential for achieving SDG 11 [11].

As discussed above, the widespread use of digital technology and the internet has brought about numerous opportunities and benefits, but it has also led to an increase in cybercrime. Cybercrime refers to any criminal activity that is carried out using digital technology, such as hacking, identity theft, and online fraud. Higher education students are particularly vulnerable to cybercrime, as they often use digital technology extensively for academic and social purposes. Therefore, it is important to investigate the role of digital citizenship in the prevention of cybercrime among higher education students.

Research Questions

1. How does digital citizenship education affect students' awareness and prevention of cybercrime?
2. What is the effect of digital citizenship skills in the prevention of cybercrime among higher education students in Saudi Arabia?
3. What strategies can be employed by higher education institutions in Saudi Arabia to promote digital citizenship and prevent cybercrime?

2. Literature Review

2.1. Digital Citizenship

Digital citizenship refers to the competence to navigate digital environments in a responsible and safe manner, and to engage actively and respectfully in these spaces. It involves understanding how to use digital technology effectively and ethically, while also respecting the rights and privacy of others. The nine dimensions of digital citizenship are essential for promoting safe, respectful, and responsible use of digital technology. These dimensions include digital law, digital manners, digital communication, digital rights and duties, digital trade, digital health, digital access, digital security, and digital culture. Digital citizenship requires a range of skills and behaviors, such as digital literacy, digital security, digital rights and responsibilities, digital communication, digital etiquette, and digital access [12]. The importance of digital citizenship has recently emerged in light of the widespread of information technology and the accompanying demands for policymaking that ensures citizen are protected from the dangers of digital technology while helping them make use of their advantages and deal with rights, obligations, and duties at the same time, in order to ultimately contribute to the advancement of the nation and its components,

providing citizens with rights and duties in the digital society [12]. Digital citizenship is no more than a new dimension of traditional citizenship, since traditional citizenship requires belonging to society and achieving its goals and adherence to its social, economic, political, and other laws. The same goes for the term "digital citizenship education", which means the preparation of an effective digital citizen through an education that contributes to the student's acquisition of the skills needed to use technology positively, in addition to acquiring critical thinking skills in relation to digital content and ethical social skills to interact with others by fortifying him with a solid ethical fabric that protects him from technical dangers [13].

The characteristics of a digital citizen are summarized in respect of societies' cultures in the digital environment and understanding of the human, cultural, and social issues related to technology [14]. Based on the foregoing, it is clear that digital citizenship has several aspects, including the knowledge aspect that reflects knowledge regarding the digital world [15]. It also includes the skills aspect that demonstrates the skills that enable the individual to interact with the digital community [16]. Finally, it includes the behavioral aspect, which urges the individual to establish values and ethics and abide by the necessary laws and rules; the digital citizen must possess those skills so that he can use the internet correctly and securely [14,16].

Digital citizenship plays a crucial role in the prevention of cybercrime among higher education students. By promoting responsible and ethical use of digital technology, digital citizenship can help to reduce the risk of cybercrime. Digital citizenship education can help students to develop the skills and knowledge they need to protect themselves and others from cybercrime [17].

2.2. Cybercrime

Cybercrime refers to criminal activities that are carried out using digital technology, such as computers, smartphones, and the internet. Cybercrime can take many forms, including hacking, identity theft, online fraud, cyberbullying, and cyberstalking [18]. Hacking involves gaining unauthorized access to computer systems or networks to steal information, install malware, or disrupt operations [19]. Identity theft is the fraudulent acquisition and use of someone's personal information, such as their name, address, and social security number, to commit crimes such as credit card fraud and tax fraud. Online fraud includes a range of scams and schemes that use the internet to deceive victims and steal their money or personal information [20]. These can include phishing scams, where criminals send fraudulent emails or messages that appear to be from a reputable source, in order to trick people into sharing their personal information, such as their passwords or credit card numbers [21].

As outlined by the Council of the European Union, certain groups can be at an increased risk of experiencing cybercrime and cyberviolence, including girls and women, ethnic minorities, people with disabilities, and those who are economically disadvantaged. There are many factors that can contribute to this increased risk, including social and cultural norms, lack of access to resources and education, and systemic inequalities. For example, girls and women may be targeted for cyber harassment or cyberstalking, which can have a significant impact on their mental health and wellbeing. Ethnic minorities may also be targeted by hate speech or discrimination online, which can contribute to feelings of isolation and exclusion. People with disabilities may be at an increased risk of online fraud or scams, as they may be more vulnerable to manipulation and exploitation [22].

Cyberstalking is a pattern of digital harassment that involves repeated unwanted contact or threats made online. Cyberstalking can have serious consequences for children and adolescents, including negative effects on their mental health, academic performance, and social relationships. Studies have shown that victims of cyberstalking are at an increased risk of depression, anxiety, and even suicidal ideation [23]. Moreover, cybercrime can have serious consequences for individuals and organizations, including financial losses, reputational damage, and legal repercussions. To prevent cybercrime, individuals and

organizations should take steps to protect their digital devices and networks, including using strong passwords, installing antivirus software, and being cautious when sharing personal information online [24]. Cybersecurity education and awareness-raising efforts can also help in preventing cybercrime.

2.3. Digital Citizenship in the Prevention of Cybercrime

There is a large volume of published studies describing the prevention of cybercrime among higher education students [25]. Several studies have highlighted the importance of promoting responsible and ethical use of digital technology in reducing the risk of cybercrime [26]. The prior work of Sarwatay et al. [27] found that higher education institutions that emphasized digital citizenship education experienced lower rates of cybercrime incidents among their students. The study also found that students who received digital citizenship training were more likely to adopt safe and responsible digital practices, such as using strong passwords and being cautious when sharing personal information online.

Recent evidence reported by Zhong et al. [28] suggests that digital citizenship education could help to reduce cyberbullying and other forms of online harassment among higher education students. Their study suggested that digital citizenship education could help to create a culture of respect and responsibility around the use of digital technology, which could in turn lead to a reduction in cybercrime incidents. In addition, a study conducted by Ragnedda and Muschert [29] suggested that digital citizenship education could help to reduce the spread of fake news and misinformation online. The study found that students who received digital citizenship training were more likely to be able to identify and critically evaluate online information, which could help to prevent the spread of false or misleading information.

One study conducted by Adorjan and Ricciardelli [30] investigated the impact of a digital citizenship education program on the cyber-safety knowledge and behavior of college students. The study found that after participating in the program, students had significantly increased their knowledge of cyber-safety and were more likely to engage in safe digital practices, such as using strong passwords and avoiding clicking on suspicious links. Moreover, students who received the curriculum were more likely to adopt privacy-protective behaviors, such as adjusting their social media privacy settings and being cautious when sharing personal information online [31].

Furthermore, a study by Akcil and Bastas [32] investigated the impact of a digital citizenship program on college students' attitudes towards online safety and security. The study found that the program was effective in promoting safe and responsible digital practices, and that students who participated in the program had higher levels of digital citizenship. In the Saudi context, Al-Zahrani [33] conducted a study entitled "The role of Saudi Arabia's Islamic Universities in Sensitizing their Students about the Seriousness of Cybercrime and Ways to Prevent it". It aimed to identify the most prominent images of cybercrime in Saudi Arabia and the role of universities in sensitizing their students about the seriousness of cybercrime. The study showed that universities in Saudi Arabia moderately fulfil their role in the face of cybercrime, the most important of which were national crimes, followed by social crimes, and finally economic crimes.

It is clear from the presentation of the literature review that digital citizenship studies have not been limited to a single age group. On the contrary, they have been diversified to cover different age groups and stages, from children to young people, parents, teachers, and experts. All these age groups are vulnerable to cybersecurity crimes and cyberattacks, causing hate, fraud, economic, financial, and national crimes among these age groups. Studies have shown that public and higher education students need to be better prepared to deal with cybersecurity issues and crimes, given the prevalence of such crimes in their virtual educational environments, so digital citizenship requires an effort in all educational situations, for teachers and curriculum makers to give students the values, skills, and behaviors to be followed to control their interactions with the digital community.

The existing research seeks to explore the relationship between digital citizenship and cybercrime in virtual learning environments from the perspective of higher education students in Saudi Arabia, something critical due to its contribution towards the development of strategies, plans, and root remedies for cybercrime and the enactment of legislation that will allow universities to combat crime in virtual educational environments. Overall, these studies suggest that digital citizenship education can play an important role in the prevention of cybercrime among higher education students. By promoting responsible and ethical use of digital technology, digital citizenship education can help to reduce the risk of cybercrime and create a safer digital environment for everyone.

3. Materials and Methods

The current section contains an explanation of the method used in this study, and a description of the instruments applied in the compilation of the study's data.

3.1. Research Design

A mixed-method approach was utilized for this study, combining quantitative and qualitative data collection methods. The research involved the use of surveys and open online interviews as in Figure 1.

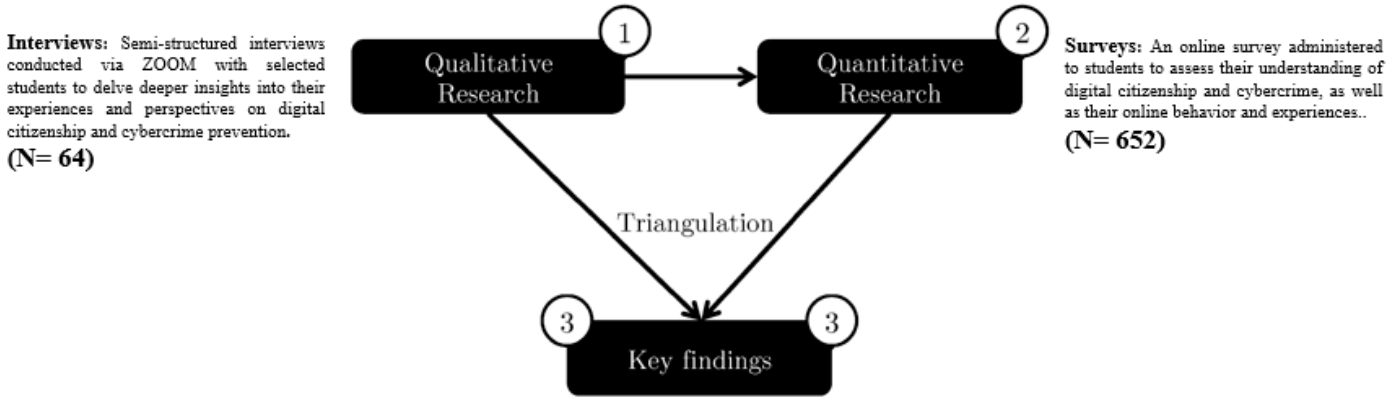

Figure 1. Convergent parallel mixed-methods design adapted from [34].

3.2. Characteristics of the Sample

The study's target population includes higher education students from various Saudi Arabian universities for the academic year 2021–2022. The sample was representative with respect to gender and diversity. A random sampling technique was employed to recruit participants, i.e., different study levels—postgraduate diploma, bachelor's degree, master's degree, and doctorate—as a study case representative of various Saudi universities. Of the initial cohort of 652 students, 336 were female and 316 male, and the surveys were distributed online in the second semester of the 2021–2022 academic year. The survey included an option to conduct an online interview via Zoom instead of meeting them face-to-face, due to the COVID-19 pandemic's imposition on researchers which required the need to adhere to social distancing, along with changes in educational systems, the inability to communicate directly with students and apply field studies, and the necessity to avoid close physical encounter to prevent the spread of the virus and avoid overwhelming healthcare systems.

3.2.1. Study Population Age

It can be seen from the data in Table 1 that the study sample was distributed according to an age variable, students aged 18–23 years old constituted 63.7%, students aged 24–29 years old constituted 14.3%, students aged 30–35 years old constituted 8.9%, students aged 36–41 years old constituted 10.1%, students aged 42–47 years old constituted 2.8%, and students aged 48–53 years old constituted the lowest rate of 0.3%. This shows that the

research sample was comprehensive and considered the diversity of students' different age groups. The interview process involved a total of 62 students from the study population, with 90% of these individuals being in their final year at university. The average age of the interviewees was 24 years old.

Table 1. Describing Study Sample's Characteristics in Terms of Age Variable.

Variable	Groups	N	Percentage
Age	18–23 Years Old	415	63.7%
	24–29 Years Old	93	14.3%
	30–35 Years Old	58	8.9%
	36–41 Years Old	66	10.1%
	42–47 Years Old	18	2.8%
	48–53 Years Old	2	0.3%
	Total	652	100%

3.2.2. Population Diversity

This study included college students from 29 different universities in Saudi Arabia from various disciplines and levels of education, as illustrated in Table 2.

Table 2. Describing Study Population diversity in terms of disciplines and levels of education.

Variable	Groups	N	Percentage
Disciplines	Human science	372	57.1%
	Natural science	280	42.9%
	Total	652	100%
Levels of education	Postgraduate diploma	43	6.6%
	Bachelor's degree	433	66.4%
	Master's degree	109	16.7%
	Doctorate	67	10.3%
	Total	652	100%

3.3. Instrument

In order to investigate the role of digital citizenship in the prevention of cybercrime among higher education students, the authors established an online survey consisting of 106 items to be given to higher education students at Saudi Arabia's universities. The survey's items were divided into two main sections:

- The first section elicited information on the study sample's demographic data, which involved gender, age, university, faculty, degree, major, and academic level.
- The second section was designed to measure the following constructs:
  - The first part contained 56 items that contributed towards the evaluation of the independent variable of higher education students at Saudi universities' amount of knowledge and possession of digital citizenship with its various dimensions, which was derived from the digital citizenship measurement survey. The items were derived from the digital citizenship measurement survey and were used to assess the students' level of digital literacy, digital rights and responsibilities, digital communication, digital security, digital etiquette, and digital access. By analyzing the results of this evaluation, the study aims to gain insights into the level of digital citizenship among higher education students at Saudi universities and identify areas for improvement; see tables (6:12) [35].

- The second part contained 50 items to measure the dependent variable regarding the role of digital citizenship in combating forms of cybercrime prevalent in virtual learning environments, which was derived from both the measurement of cybercrime survey [35], and the cybercrime survey [8].

3.3.1. Instruments Reliability and Consistency

To ensure the reliability of the online survey's items, it was presented in its preliminary form to a group of technical, educational, and cybersecurity professionals to make their observations on the survey phrases. They expressed their views on the correctness of the language and wording of the survey items and the appropriateness of the survey language level for the study sample. The ratio of agreement between the arbitrators on all terms in the survey varied between 80% and 100%. The researchers took the arbitrators' opinions and guidance, deleting and adding some items, making some modifications in accordance with their observations, and finalizing the survey. Table 3 shows Cronbach's alpha constant factors of the survey dimensions.

Table 3. Cronbach's alpha reliability and constant factors of the survey dimensions.

Digital Citizenship Scale Dimensions	Cronbach's Alpha	Items
Digital Access	0.822	5
Digital Trade	0.803	8
Digital Communication	0.815	7
Digital Culture	0.887	5
Digital Manners	0.815	5
Digital Law	0.835	4
Digital Rights and Duties	0.806	4
Digital Health	0.868	5
Digital Security	0.947	13
Total Digital Citizenship Scale	0.971	56
Digital Cybercrime Scale Dimensions	**Cronbach's Alpha**	**Items**
Digital citizenship's role in combating cybercrime that threatens national security in virtual learning environments	0.787	6
Digital citizenship's role in combating financial cybercrime in virtual learning environments	0.899	15
Digital citizenship's role in combating social cybercrime in virtual learning environments	0.893	9
Digital citizenship's role in combating insult, slander, and defamation cybercrime in virtual learning environments	0.814	8
Digital citizenship's role in combating threatening and harassing cybercrime in virtual learning environments	0.861	12
Total Digital Cybercrime Scale	0.964	50
Survey as a whole	0.980	106

The Pearson correlation coefficient was also calculated for each item in the survey and for the axis it belongs to, as well as the correlation coefficient for each axis in the overall survey in order to ascertain the constructive authenticity of the survey axis. Items' correlation factors—within the scale of digital citizenship as a whole—ranged between 0.219–0.616, with the axis between 0.524–0.909. Items' correlation factors—within the scale of cybercrime as a whole—ranged between 0.0.389–0.716, with the axis between 0.867–0.951. This indicates a strong correlation coefficient of axes and items within the survey, as they are all acceptable correlations and functional at the indicative level ($\alpha = 0.05$) for the purposes

of applying this study. As for the survey's constancy, it was calculated for each dimension of the survey and for the whole survey using Cronbach's alpha constant factor after being measured on an extranet survey sample consisting of 30 students at Jeddah University.

As can be seen from Table 3, the Cronbach's alpha coefficients for the survey demotions are high and acceptable, reaching 0.882 for the first axis that includes digital access, 0.803 for the second axis that contains digital trade, 0.815 for the third axis that contains digital communication, 0.887 for the fourth axis that contains digital culture, 0.815 for the fifth axis that contains digital manners, 0.835 for the sixth axis that contains digital law, 0.806 for the seventh axis that contains digital rights and duties, 0.868 for the eighth axis that contains digital health, and 0.947 for the ninth axis that contains digital security. Cronbach's alpha for the digital citizenship scale as a whole was 0.971, indicating that there was high stability in the study sample's responses to the survey questions. This shows the respondents' understanding of the survey terms and their ability to handle them with a high amount of confidence. So, there is a high and acceptable possibility of applying the digital citizenship survey.

3.3.2. Relative Weight and Survey's Correction

Participants were asked to respond using a 5-point Likert scale ranging from (1) strongly disagree, (2) disagree, (3) neutral, (4) agree, and (5) strongly agree. To interpret the means of the sample's estimates on each item of the survey, the following breakdown was used, as shown in Table 4.

Table 4. Measuring Means and Breakdown.

Very Low	Low	Average	High	Very High
1–1.80	1.81–2.6	2.61–3.40	3.41–4.20	4.21–5

3.4. Interviews

Semi-structured interviews were conducted with selected students to delve deeper into their experiences and perspectives on digital citizenship and cybercrime prevention. The data were recorded on a digital audio recorder and transcribed into text in Word. Qualitative data from the interviews were subjected to thematic analysis using NVivo 14 software to identify common themes and patterns [36]. In an attempt to make each interviewee feel as comfortable as possible, the interview began by introducing the purpose of the study. Then, the interviewee was asked some background questions to get to know the interviewee better and establish a rapport and they were asked about their experiences with digital citizenship. Finally, the interviewee was thanked for their time and insights, and we let them know that their responses will be kept confidential and may be used for research purposes.

4. Results and Discussion

Statistical analysis was performed using SPSS software (version 26). The first set of analyses examined the current level of understanding and practice of digital citizenship among higher education students in Saudi Arabia. Quantitative data from the surveys analyzed used descriptive and inferential statistics to establish patterns and relationships between variables. The authors used the means scale set out in Table 5 to explain these averages and their indications. Table 6 illustrates means (M) and standard deviations (SD) of digital citizenship dimensions.

Table 5. Means and Standard Deviations of digital citizenship dimensions (N = 652).

Dimension	M	SD	Rank	Sig.
Digital Access	3.13	0.92	7	Average
Digital Trade	3.29	0.78	5	Average

Table 5. *Cont.*

Dimension	M	SD	Rank	Sig.
Digital Communication	3.69	0.78	3	High
Digital Culture	2.89	1.12	9	Average
Digital Manners	3.70	0.79	2	High
Digital Law	4.07	0.88	1	High
Digital Rights and Duties	3.58	0.88	4	High
Digital Health	3.17	1.09	6	Average
Digital Security	2.93	1.04	8	Average
Total Digital Citizenship Dimension	3.31	0.76	-	Average

Table 6. Means and Standard Deviations of digital access dimensions.

N	Item	M	SD	Rank	Sig.
1	I can connect to the internet easily from home.	3.64	1.13	1	High
2	I can connect to the internet via my smart phone.	3.36	1.15	2	Average
3	I can obtain the necessary support when an internet issue occurs.	3.29	1.12	3	Average
4	Internet speed is suitable and fulfills my personal needs.	2.78	1.24	4	Average
5	I have no problem with internet connection fees.	2.60	1.35	5	Average
	Total Digital Access Dimension	3.13	0.92	-	Average

Higher education students may have an average understanding and practice of digital citizenship, exposing them to increased risks of cybercrime. This result is because digital citizenship with its different dimensions occurs at an average to high level for higher education students at Saudi universities in terms of their possession of digital citizenship skills, as well as students' adherence to the rules, regulations, and optimal use of digital technology. Digital citizenship can also help to create a culture of safety and responsibility around the use of digital technology. By promoting digital ethics and respect, students are more likely to behave in a responsible and ethical manner online, which can help to prevent cybercrime. Students' knowledge of digital citizenship skills in their different dimensions can be due to several factors, including the role of faculty, family, and university in providing guidance. Digital citizenship education can help students to develop the skills and knowledge they need to protect themselves and others from cybercrime by promoting responsible and ethical use of digital technology, and digital citizenship can help to reduce the risk of cybercrime and create a culture of safety and responsibility online [37]. The most important result was that higher education institutions should prioritize digital citizenship education and cybersecurity measures to protect their students and their networks from cybercrime. Each of these factors may contribute towards providing students with knowledge needed to use technology well. These results reflect those of Hollandsworth et al. [38] who also found that students gain the necessary awareness for digital citizenship with the help of their teachers. The details of each dimension are discussed separately, and the interpretation of the results consider the objectives and questions of the study.

4.1. Digital Access

Digital access among students refers to the availability and use of digital technology and the internet by students in higher education institutions, as confirmed in Table 7. The most obvious finding to emerge from Table 6 is that digital access is an important issue, as it can impact students' academic performance, social connections, and access to information and resources. The findings reported here suggest that to ensure all students have equal access to digital technology and the internet, institutions may need to provide resources

such as laptops, wifi hotspots, and digital literacy training. This also accords with our earlier observations, which showed that institutions may need to work with policymakers and community organizations to address broader issues related to digital infrastructure and access in underserved communities [33,35].

Table 7. Means and standard deviations of digital trade dimension.

N	Items	M	SD	Rank	Sig.
1	I prefer shopping via the internet over the traditional way.	3.19	1.16	1	Average
2	Shopping via the internet provides more choices.	3.35	1.16	2	Average
3	Shopping via the internet provides reasonable prices.	3.42	1.14	3	High
4	Electronic trade does not cause any conflict with my society's values.	3.39	1.15	4	Average
5	I only purchase allowed goods.	3.52	1.12	5	High
6	I purchase my basic and non-basic needs via the internet.	2.93	1.43	-	Average
7	Before I purchase goods via the internet, I look up their prices and specifications.	3.14	1.21		Average
8	I only purchase from trusted online stores.	3.37	1.26		Average
	Total Digital Trade Dimension	3.29	0.78		Average

4.2. Digital Trade

Shopping via the internet, also known as online shopping or e-commerce, has become increasingly popular in recent years as a part of digital citizenship [39]. Online shopping allows higher education students to purchase goods and services using the internet, without having to physically visit a store or interact with a salesperson. The most striking result from Table 7 was the that online shopping is often more convenient than traditional shopping, as students can shop from the comfort of their own home and at any time of day, as item 1 obtained a high mean score (3.64), with an acceptable standard deviation of 1.13. Moreover, online shopping allows higher education students to compare prices and products across multiple retailers, which can help them to make more informed purchasing decisions, as shown in items 2 and 7. Additionally, online shopping may offer a wider range of options and availability of products which may not be available in physical stores, as item 5 indicates.

4.3. Digital Communication

Digital communication has become an increasingly important aspect of higher education. The results in Table 8 indicate that digital communication is an important aspect of higher education that can facilitate student learning, engagement, and collaboration. By using digital communication tools effectively and responsibly, students can enhance their academic experience and succeed in their studies. This finding is consistent with that of Vlachopoulos and Makri [40] who found that the use of social media platforms for academic purposes was positively associated with academic performance among college students. The study suggested that social media can be an effective tool for sharing information and resources, and for connecting with peers and instructors [39].

Overall, these results suggest that digital communication can be an effective tool for enhancing student engagement, participation, and academic performance in higher education. However, it is important for students to use digital communication tools responsibly and in accordance with appropriate digital etiquette and professionalism.

Table 8. Means and standard deviations of digital communication dimension.

N	Items	M	SD	Rank	Sig.
1	I communicate with my peers via e-mails.	3.31	1.21	6	Average
2	I use chat apps, such as WhatsApp messenger.	4.18	1.09	1	High
3	I communicate with others using social media platforms.	3.92	1.03	3	High
4	I use online communication tools to learn and share opinions.	3.38	1.21	5	Average
5	Online communication allows me to contact with my peers and friends easily.	3.85	1.01	4	High
6	Online communication allows me to make new friendships around the world.	3.21	1.22	7	Average
7	In online dialogue, I respect others' rights, and cultures.	4.02	1.11	2	High
	Total Digital Communication	3.69	0.78	-	High

4.4. Digital Culture

The rise of digital culture has created new opportunities for cybercriminals to target individuals and organizations. For example, social media platforms can be used to spread fake news or phishing links, while e-commerce websites can be used to steal credit card information [41]. Looking at Table 9, it is clear that the means measuring digital culture among higher education students at Saudi universities ranged from 2.62 to 3.15 with an average degree. The overall mean of digital culture among higher education students at Saudi universities was 2.89 with a standard deviation of 1.12, indicating that all members of the study sample agreed on higher education students at Saudi universities' amount of digital culture. This study recommends that it is important for students to be aware of the risks and take steps to protect themselves. This may include training on how to incorporate social media platform technologies in their work environment in the future [42].

Table 9. Means and standard deviations of digital culture dimension.

N	Items	M	SD	Rank	Sig.
1	I was trained in how to use 21st century skills, such as using search engines on the internet.	2.98	1.52	2	Average
2	I was trained to optimally use some modern technical tools when learning.	2.94	1.22	3	Average
3	I always receive the necessary help when having a problem with using modern technologies in learning.	3.15	1.11	1	Average
4	I was educated on how to deal with potential dangers when using modern technologies.	2.74	1.44	4	Average
5	I was trained how to incorporate modern technologies in my work environment in the future.	2.62	1.41	5	Average
	Total Digital Culture Dimension	2.89	1.12	-	Average

4.5. Digital Manners

Cyberbullying is a serious issue that can have a negative impact on the mental health and wellbeing of those targeted. Therefore, it is important to respect the feelings of others and practice good digital etiquette [43]. Table 10 provides the summary statistics for digital manners among higher education students at Saudi universities, and these range from 3.25 to 3.87 with an average or high degree. The overall mean of digital manners among higher education students at Saudi universities was 3.70 with a standard deviation of 0.79 and a highly significant degree, indicating that all members of the study sample make sure to respect others' feelings when using online environments. This finding is consistent with that of Ng [44], who examined how college students in Hong Kong and mainland China use online communication tools to maintain positive social relationships. The study found that students were aware of the potential for miscommunication online and actively worked to use appropriate language and tone to avoid misunderstandings. These results

corroborate the findings of a great deal of the previous work by Hamat et al. [45], who explored how college students in Malaysia use social media to communicate with their peers. The study found that students were aware of the potential for online conflict and practiced self-regulation to avoid offending others. Comparison of the findings with those of other studies confirms that university students are aware of the importance of respecting others' feelings when using online environments and actively work to maintain positive relationships and avoid conflict. However, there is still a need for ongoing education and support to help students develop the skills and strategies needed to navigate online interactions in a respectful and responsible manner.

Table 10. Means and Standard Deviations of Digital Manners.

N	Items	M	SD	Rank	Sig.
1	I always make sure to respect others' feelings when using electronic environments on the internet.	3.83	0.98	3	High
2	I always make sure to respect others' opinions and expertise when using electronic environments on the internet.	3.86	0.97	2	High
3	I always make sure that everyone has equal time to share and express opinions when using electronic environments on the internet.	3.70	1.03	4	High
4	I always make sure not to interrupt others when it is their turn to speak when using electronic environments on the internet.	3.87	0.95	1	High
5	I express my feelings freely and rationally when I do not feel comfortable using electronic environments on the internet.	3.25	1.23	5	Average
	Total Digital Manners Dimension	3.70	0.79	-	High

4.6. Digital Law

Online digital law refers to the legal framework that governs the use of technology and the internet. It encompasses a wide range of legal issues, including intellectual property rights, data privacy, cybersecurity, and online harassment [46]. Table 11 illustrates that awareness of digital law among higher education students at Saudi universities ranged from 3.93 to 4.26 with a high degree. The study found that students were generally aware of the importance of respecting digital law and avoiding illegal activities such as hacking, piracy, and cyberbullying. This finding was also reported by Ciesielska and Jemielniak [47] who investigated college students' attitudes toward digital piracy. The study found that while students were generally aware that digital piracy is illegal, many of them were still engaged in piracy due to the convenience and affordability of pirated content. This finding is contrary to previous studies by Martzoukou et al. [48] that investigated college students' knowledge and understanding of digital law in Scotland, Ireland, and Greece. The study found that students had limited knowledge of digital law but were generally aware of the need to respect copyright and intellectual property rights when using online environments.

Table 11. Means and Standard Deviations of Digital Law.

N	Items	M	SD	Rank	Sig.
1	I believe that everyone should face the consequences of their actions on the internet.	4.02	1.12	3	High
2	I believe that actions such as trespassing and stealing others' information and possessions are wrong.	4.26	1.04	1	High
3	I believe that programming or unleashing viruses or unwanted advertising messages is a cybercrime.	3.93	0.96	4	High
4	I believe that a cybercrime combat system is important for punishing those who carry out inappropriate actions on the internet.	4.07	1.15	2	High
	Total Digital Law Dimension	4.07	0.88	-	High

4.7. Digital Rights and Duties

The overall mean of digital rights and duties among students of higher education at Saudi universities was 3.58 with a standard deviation of 0.88 and a high degree, as presented in Table 12. The most important result was that students have a duty to respect others' digital rights, such as privacy, freedom of expression, and access to information. These results reflect those of Stoica et al. [49] who investigated the attitudes of university students in Romania towards digital citizenship. The study found that students believed that they had a responsibility to use technology in a responsible and ethical manner, and to respect others' digital rights. Hence, it could conceivably be hypothesized that by promoting digital literacy and responsible behavior, we can help students become responsible digital citizens who contribute positively to the online community and respect the rights of others.

Table 12. Means and Standard Deviations of Digital Rights and Duties.

N	Items	M	SD	Rank	Sig.
1	Every internet user should have digital rights, such as privacy and the right to express opinions.	4.05	1.13	1	High
2	Every internet user should have digital duties, such as respecting others' digital rights.	3.77	1.03	2	High
3	I believe that rights and duties should be identified, discussed, and understood by every internet user.	3.24	1.51	4	Average
4	I believe that understanding rights and duties helps everyone to increase productivity and performance.	3.25	1.22	3	Average
	Total Digital Rights and Duties Dimension	3.58	0.88	-	High

4.8. Digital Health

Digital health information has the potential to transform healthcare delivery and improve students' physical and psychological outcomes. The overall mean of digital rights and duties among students of higher education at Saudi universities was 3.58 with a standard deviation of 0.88 and a high degree, as presented in Table 13. These results are in agreement with those obtained by Jabour et al. [50], who investigated the use of mobile health apps among medical students in Saudi Arabia. The study found that the majority of students used mobile health apps to manage their health and wellbeing, and that they found the apps to be useful and effective. Moreover, these results seem to be consistent with other research into the use of social media for health-related purposes among medical students in Germany. The study found that students used social media to exchange health-related information and to communicate with peers and healthcare professionals [51]. However, in our study, item 3 in Table 13 has the lowest mean at 3.24, with an average degree of significance, indicating that there is a need for further research to explore the benefits and risks of using digital health information among higher education students, as well as to develop effective strategies for promoting digital health literacy and responsible use of digital health tools.

Table 13. Means and Standard Deviations of Digital Health.

N	Items	M	SD	Rank	Sig.
1	I am aware of health and psychological risks related to the overuse of digital technologies such as inactivity, addiction, and stress.	2.96	1.57	4	Average
2	I believe in the importance of maintaining physical and psychological health in these surroundings and the dominant digital world.	3.53	1.13	1	High
3	I try not to overuse digital technology to avoid health and psychological risks.	3.06	1.27	2	Average
4	I believe that the use of digital technology should be moderate.	2.89	1.49	5	Average

Table 13. *Cont.*

N	Items	M	SD	Rank	Sig.
5	I believe in the importance of raising awareness regarding physical and psychological risks related to digital technological overuse and addiction.	3.44	1.21	2	High
	Total Digital Health Dimension	3.17	1.09	-	Average

4.9. Digital Security

Research on digital security among students in higher education has been a growing area of interest in recent years [52]. Looking at Table 14, the current investigation found that the means of digital security among higher education students at Saudi universities ranged from 2.45 to 3.50 with average and high degrees. What stands out in the table is that while students in higher education are generally aware of digital security risks, they may lack the skills and knowledge needed to protect themselves against cyber threats. These results are in accord with recent studies that investigated the digital security behaviors of students in higher education in Norway. The study found that while students had a good understanding of digital security risks, they often engaged in risky behaviors such as using weak passwords and sharing personal information online [53].

Table 14. Means and Standard Deviations of Digital Security.

N	Items	M	SD	Rank	Sig.
1	I have antivirus applications on my mobile phone and laptop.	2.82	1.49	8	Average
2	I always back up my data and important files on a secure, protected external storage disk or in the cloud.	2.88	1.50	7	Average
3	I always save my personal information within password-protected files.	2.71	1.20	10	Average
4	I do not save any private or personal information on public computers, such as the ones in universities or internet cafés.	3.28	1.22	2	Average
5	I immediately take my mobile phone or laptop to repair when I notice any difference or change in its performance.	3.17	1.21	4	Average
6	I am always careful not to provide any unreliable parties or websites with my financial information, such as my bank account or credit cards.	3.50	1.27	1	High
7	I immediately delete any email from an unknown source, or when I doubt its contents.	2.81	1.24	9	Average
8	I do not open any unknown files before checking them through protection applications.	2.92	1.29	6	Average
9	I regularly change my confidential numbers—such as e-mail password—to increase protection.	2.65	1.46	11	Average
10	I always establish hard confidential numbers to increase security and difficulty detecting them.	2.61	1.48	12	Average
11	I always make sure to visit safe and non-suspicious websites.	3.04	1.23	5	Average
12	I always carrt out quick repairs to my mobile phone or laptop to fix it and clean it of waste from browsing the internet.	3.25	1.26	3	Average
13	I always read the privacy policy—if found—before installing any application or software on my mobile phone or laptop.	2.45	1.43	13	Average
	Total Digital Security Dimension	2.93	1.04	-	Average

4.10. Interview Analysis

Digital citizenship education has a significant impact on students' awareness and prevention of cybercrime through the development of responsible online behavior and critical thinking skills. The specific objectives of this interview were to explore participants' experiences and perspectives on digital citizenship and cybercrime prevention and gain a

deeper understanding of how participants navigate digital spaces and engage in digital citizenship practices. Moreover, this interview provides a comprehensive understanding of digital citizenship and cybercrime prevention by integrating qualitative and quantitative data. In order to confirm this hypothesis, an interview was conducted online via Zoom with 64 students. We asked them about how digital citizenship education affects students' awareness and prevention of cybercrime, and what strategies can be employed by higher education institutions to promote digital citizenship and prevent cybercrime? Qualitative data from the interviews were subjected to thematic analysis to identify common themes and patterns, as presented in Figure 2.

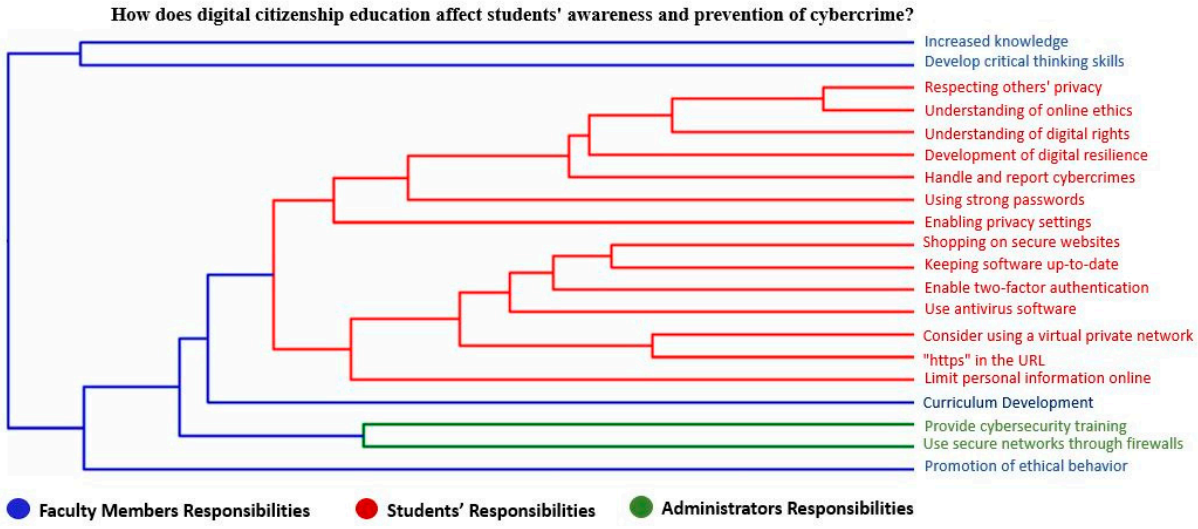

Figure 2. Interview analysis using NVivo 14 software.

The most interesting aspect of this figure is that there are three main axes: education, personal responsibility, and university administration. Education includes incorporating digital citizenship topics into the curriculum, providing training and resources for students and faculties, and promoting awareness and understanding of digital citizenship and cyber-safety. Personal responsibility includes taking steps to protect personal information and devices, using digital technology in a responsible and ethical manner, and reporting any instances of cybercrime or cyberbullying. University administration includes establishing policies and procedures to prevent and address cybercrime and cyberbullying, providing resources and support for victims of cybercrime, and promoting a culture of digital citizenship and cyber-safety across the university community. The three axes are interconnected and complementary, and all are important for promoting digital citizenship and cyber-safety in higher education.

The interview findings indicate that digital citizenship education is a crucial factor in increasing students' awareness of cybercrime and its consequences. Students who receive digital citizenship education are more likely to identify and take appropriate measures to protect themselves against cybercrime such as phishing scams and identity theft. Moreover, digital citizenship education promotes ethical online behavior by encouraging students to respect others' privacy, intellectual property, and digital rights. These results are consistent with previous studies that have shown how understanding online ethics can reduce the likelihood of students engaging in cybercrime or becoming victims of such offenses [54].

The effectiveness of digital citizenship education in preventing cybercrime largely depends on how it is implemented [55]. This study supports evidence that effective implementation requires a comprehensive curriculum, teacher training, and parental involvement. While there is ample room for further research to confirm the positive impact of digital citizenship education on students' awareness and prevention of cybercrime, effective implementation is key to ensuring that students develop the necessary skills and knowledge to protect themselves online.

Taken together, these findings confirm that promoting digital citizenship education can contribute to a more sustainable digital future. The sustainable use of technology means using it in a way that minimizes negative impacts on the environment, society, and the economy. This includes reducing e-waste, using energy-efficient devices, and promoting digital inclusion. By teaching students about digital citizenship and responsible technology use, we can help create a generation of digital citizens who are mindful of their impact on the world around them and who strive to use technology in a way that supports sustainability.

5. Conclusions

As digital technology continues to permeate various aspects of our lives, there has been a corresponding increase in cybercrime. The specific objective of this study was to investigate the effect of digital citizenship skills in the prevention of cybercrime among higher education students. By understanding the current state of digital citizenship among Saudi Arabian students and identifying effective strategies for promoting responsible online behavior, higher education institutions can better equip students with the skills necessary to navigate the digital world safely and responsibly. A mixed-method approach was utilized for this study, combining quantitative and qualitative data collection methods. The research involved the use of surveys and interviews. Findings confirmed that the means measuring the amount of digital citizenship skills in its various dimensions ranged from 2.89 to 4.07 with average and high degrees. The digital law dimension came first, digital manners came second, digital communication came third, digital rights and duties came fourth, digital trade came fifth, digital health came sixth, digital access came seventh, digital security came eighth, and finally digital culture came last. The second major finding was that students may have a limited understanding and practice of digital citizenship, exposing them to increased risks of cybercrime. One of the more significant findings to emerge from this study is that digital citizenship education has a significant impact on students' awareness and prevention of cybercrime through the development of responsible online behavior and critical thinking skills. These findings suggest higher education institutions can promote digital citizenship by developing a comprehensive curriculum that integrates digital citizenship education into academic programs, providing training and resources for students and faculties, promoting awareness and understanding of digital citizenship through university-wide campaigns and events, establishing policies and procedures to prevent and address cybercrime, fostering a culture of digital citizenship, involving parents and the wider community in promoting digital citizenship, and providing infrastructure and support for digital access. By taking a proactive approach to promoting digital citizenship, higher education institutions can help students develop the skills and knowledge they need to use digital technology safely, ethically, and effectively, while also promoting a positive and inclusive digital culture. Please confirm that the intended meaning has been retained; amend further if required.

Author Contributions: H.A.A. and A.M.A.-Z. contributed to conception and design of the study. H.A.A. organized the database. A.M.A.-Z. performed the statistical analysis. H.A.A. and A.M.A.-Z. wrote the first draft of the manuscript. H.A.A. and A.M.A.-Z. wrote sections of the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: The study was conducted according to the guidelines of the Declaration of Helsinki, and approved by the Institutional Review Board (or Ethics Committee) of University of Jeddah, College of Education.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The data that support the findings of this study are available from the corresponding author upon reasonable request.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Symons, D.; Blannin, J. Empowerment and Disempowerment in Peer Observation within Pre-Service Teacher, Technology-Assisted Integrated STEM Education. In *Encyclopedia of Education and Information Technologies*; Springer International Publishing: Cham, Switzerland, 2020; pp. 699–706. [CrossRef]
2. Ellitan, L. Competing in the era of industrial revolution 4.0 and society 5.0. *J. Maksipreneur Manaj. Kop. Dan Entrep.* **2020**, *10*, 1–12. [CrossRef]
3. Sage, K.; Piazzini, M.; Downey IV, J.C.; Ewing, S. Flip it or click it: Equivalent learning of vocabulary from paper, laptop, and smartphone flashcards. *J. Educ. Technol. Syst.* **2020**, *49*, 145–169. [CrossRef]
4. Nigam, A.; Pasricha, R.; Singh, T.; Churi, P. A systematic review on ai-based proctoring systems: Past, present and future. *Educ. Inf. Technol.* **2021**, *26*, 6421–6445. [CrossRef]
5. Newlands, G.; Lutz, C.; Tamò-Larrieux, A.; Villaronga, E.F.; Harasgama, R.; Scheitlin, G. Innovation under pressure: Implications for data privacy during the COVID-19 pandemic. *Big Data Soc.* **2020**, *7*, 2053951720976680. [CrossRef]
6. Long, Y.; Quan, F.; Zheng, Y. Effects of bicultural identity integration and National identity on COVID-19-related anxiety among Ethnic Minority college students: The mediation role of power values. *Psychol. Res. Behav. Manag.* **2021**, *14*, 239–249. [CrossRef]
7. Conway, G.; Hadlington, L. How do undergraduate students construct their view of cybercrime? Exploring definitions of cybercrime, perceptions of online risk and victimization. *Polic. A J. Policy Pract.* **2021**, *15*, 119–129. [CrossRef]
8. Alzubaidi, A. Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon* **2021**, *7*, e06016. [CrossRef]
9. Aljabri, S. Cybersecurity Awareness in Saudi Arabia. *Int. J. Res. Publ. Rev.* **2021**, *2582*, 7421.
10. AlMindeel, R.; Martins, J.T. Information security awareness in a developing country context: Insights from the government sector in Saudi Arabia. *Inf. Technol. People* **2021**, *34*, 770–788. [CrossRef]
11. United Nations. Transforming our world: The 2030 Agenda for Sustainable Development. 2015. Available online: https://sdgs.un.org/goals (accessed on 30 May 2023).
12. Richardson, J.; Milovidov, E. *Digital Citizenship Education Handbook: Being Online, Well-Being Online, and Rights Online*; Council of Europe: Strasbourg, France, 2019.
13. Chen, L.L.; Mirpuri, S.; Rao, N.; Law, N. Conceptualization and measurement of digital citizenship across disciplines. *Educ. Res. Rev.* **2021**, *33*, 100379. [CrossRef]
14. Isman, A.; Canan Gungoren, O. Digital citizenship. *Turk. Online J. Educ. Technol.-TOJET* **2014**, *13*, 73–77.
15. Kim, M.; Choi, D. Development of youth digital citizenship scale and implication for educational setting. *J. Educ. Technol. Soc.* **2018**, *21*, 155–171.
16. Saykili, A. Higher education in the digital age: The impact of digital connective technologies. *J. Educ. Technol. Online Learn.* **2019**, *2*, 1–15. [CrossRef]
17. Prasetiyo, W.H.; Naidu, N.B.M.; Tan, B.P.; Sumardjoko, B. "It really needs to be given to students" digital citizenship understanding amongst student teachers qualitative Nvivo analysis. *J. Civ. Media Kaji Kewarganegaraan* **2022**, *19*, 9–20. [CrossRef]
18. Al-Khater, W.A.; Al-Maadeed, S.; Ahmed, A.A.; Sadiq, A.S.; Khan, M.K. Comprehensive review of cybercrime detection techniques. *IEEE Access* **2020**, *8*, 137293–137311. [CrossRef]
19. Kennedy, J.; Holt, T.; Cheng, B. Automotive cybersecurity: Assessing a new platform for cybercrime and malicious hacking. *J. Crime Justice* **2019**, *42*, 632–645. [CrossRef]
20. Curtis, J.; Oxburgh, G. Understanding cybercrime in 'real world' policing and law enforcement. *Police J.* **2022**, 0032258X221107584. [CrossRef]
21. Button, M.; Blackbourn, D.; Sugiura, L.; Shepherd, D.; Kapend, R.; Wang, V. Victims of cybercrime: Understanding the impact through accounts. In *Cybercrime in Context: The Human Factor in Victimization, Offending, and Policing*; Springer International Publishing: Cham, Switzerland, 2021; pp. 137–156. [CrossRef]
22. Council of Europe. Guidelines on Cyber Security. 2023. Available online: https://www.coe.int/en/web/cyberviolence (accessed on 30 May 2023).
23. Zhu, C.; Huang, S.; Evans, R.; Zhang, W. Cyberbullying among adolescents and children: A comprehensive review of the global situation, risk factors, and preventive measures. *Front. Public Health* **2021**, *9*, 634909. [CrossRef]
24. Akdemir, N.; Lawless, C.J. Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach. *Internet Res.* **2020**, *30*, 1665–1687. [CrossRef]
25. Igba, I.D.; Igba, E.C.; Nwambam, A.S.; Nnamani, S.C.; Egbe, E.U.; Ogodo, J.V. Cybercrime among university undergraduates: Implications on their academic achievement. *Int. J. Appl. Eng. Res.* **2018**, *13*, 1144–1154.
26. Kaur, M.; Saini, M. Indian government initiatives on cyberbullying: A case study on cyberbullying in Indian higher education institutions. *Educ. Inf. Technol.* **2023**, *28*, 581–615. [CrossRef] [PubMed]
27. Sarwatay, D.; Raman, U.; Ramasubramanian, S. Media literacy, social connectedness, and digital citizenship in India: Mapping stakeholders on how parents and young people navigate a social world. *Front. Hum. Dyn.* **2021**, *3*, 601239. [CrossRef]
28. Zhong, J.; Zheng, Y.; Huang, X.; Mo, D.; Gong, J.; Li, M.; Huang, J. Study of the influencing factors of cyberbullying among Chinese college students incorporated with digital citizenship: From the perspective of individual students. *Front. Psychol.* **2021**, *12*, 621418. [CrossRef] [PubMed]
29. Ragnedda, M.; Ragnedda, M. Traditional digital inequalities: Digital divide. In *Enhancing Digital Equity: Connecting the Digital Underclass*; Palgrave Macmillan: Cham, Switzerland, 2020; pp. 39–60. [CrossRef]

30. Adorjan, M.; Ricciardelli, R. Student perspectives towards school responses to cyber-risk and safety: The presumption of the prudent digital citizen. *Learn. Media Technol.* **2019**, *44*, 430–442. [CrossRef]
31. Wijaya Mulya, T.; Hald, G.M. Self-perceived effects of pornography consumption in a sample of Indonesian university students. *Media Psychol.* **2014**, *17*, 78–101. [CrossRef]
32. Akcil, U.; Bastas, M. Examination of university students' attitudes towards e-learning during the COVID-19 pandemic process and the relationship of digital citizenship. *Contemp. Educ. Technol.* **2020**, *13*, ep291. [CrossRef]
33. Al-Zahrani, A. The Role of Islamic Universities in Saudi Arabia in Sensitizing its Students about the Risks of Cybercrime and Ways of Preventing it. *J. Islam. Univ. Arab. Lang. Soc. Sci.* **2019**, *2*, 385–468.
34. Creswell, J.W.; Klassen, A.C.; Plano Clark, V.L.; Smith, K.C. Best practices for mixed methods research in the health sciences. *Bethesda Natl. Inst. Health* **2011**, *2013*, 541–545.
35. Al-Zahrani, A. Toward digital citizenship: Examining factors affecting participation and involvement in the Internet society among higher education students. *Int. Educ. Stud.* **2015**, *8*, 203–217. [CrossRef]
36. Sotiriadou, P.; Brouwers, J.; Le, T.A. Choosing a qualitative data analysis tool: A comparison of NVivo and Leximancer. *Ann. Leis. Res.* **2014**, *17*, 218–234. [CrossRef]
37. Hudgell, C. Combating cybercrime is everybody's responsibility. *Keep. Good Co.* **2013**, *65*, 270–274.
38. Hollandsworth, R.; Dowdy, L.; Donovan, J. Digital citizenship in K-12: It takes a village. *Techtrends Link. Res. Pract. Improv. Learn.* **2011**, *55*, 37–47. [CrossRef]
39. Walters, M.G.; Gee, D.; Mohammed, S. A literature review: Digital citizenship and the elementary educator. *Int. J. Technol. Educ.* **2019**, *2*, 1–21.
40. Vlachopoulos, D.; Makri, A. Online communication and interaction in distance higher education: A framework study of good practice. *Int. Rev. Educ.* **2019**, *65*, 605–632. [CrossRef]
41. Odiboh, O.; Olonode, A.; Adesina, E.; Yartey, D. May, Influence of e-communication and digital culture on Nigeria's indigenous socio-cultural systems: A focus on Abeokuta and Ota, Nigeria. In Proceedings of the 2018 4th International Conference on Information Management (ICIM) 2018, Oxford, UK, 25–27 May 2018; pp. 71–75. [CrossRef]
42. Balakrishnan, V.; Gan, C.L. Students' learning styles and their effects on the use of social media technology for learning. *Telemat. Inform.* **2016**, *33*, 808–821. [CrossRef]
43. Yosep, I.; Hikmat, R.; Mardhiyah, A. Nursing intervention for preventing cyberbullying and reducing its negative impact on students: A scoping review. *J. Multidiscip. Healthc.* **2023**, *16*, 261–273. [CrossRef] [PubMed]
44. Ng, D.T.K. Online aviation learning experience during the COVID-19 pandemic in Hong Kong and Mainland China. *Br. J. Educ. Technol.* **2022**, *53*, 443–474. [CrossRef]
45. Hamat, A.; Embi, M.A.; Hassan, H.A. The use of social networking sites among Malaysian university students. *Int. Educ. Stud.* **2012**, *5*, 56–66. [CrossRef]
46. Stuckey, K.D. *Internet and Online Law*; Law Journal Press: Philadelphia, PA, USA, 2022.
47. Ciesielska, M.; Jemielniak, D. Fairness in digital sharing legal professional attitudes toward digital piracy and digital commons. *J. Assoc. Inf. Sci. Technol.* **2022**, *73*, 899–912. [CrossRef]
48. Martzoukou, K.; Kostagiolas, P.; Lavranos, C.; Lauterbach, T.; Fulton, C. A study of university law students' self-perceived digital competences. *J. Librariansh. Inf. Sci.* **2022**, *54*, 751–769. [CrossRef]
49. Stoica, M.; Ghilic-Micu, B.; Mircea, M. Restarting the information society based on blockchain technology. *Inform. Econ.* **2019**, *23*, 39–48. [CrossRef]
50. Jabour, A.M.; Rehman, W.; Idrees, S.; Thanganadar, H.; Hira, K.; Alarifi, M.A. The adoption of mobile health applications among university students in health colleges. *J. Multidiscip. Healthc.* **2021**, 1267–1273. [CrossRef] [PubMed]
51. Dadaczynski, K.; Okan, O.; Messer, M.; Leung, A.Y.; Rosário, R.; Darlington, E.; Rathmann, K. Digital health literacy and web-based information-seeking behaviors of university students in Germany during the COVID-19 pandemic: Cross-sectional survey study. *J. Med. Internet Res.* **2021**, *23*, e24097. [CrossRef] [PubMed]
52. Catal, C.; Ozcan, A.; Donmez, E.; Kasif, A. Analysis of cyber security knowledge gaps based on cyber security body of knowledge. *Educ. Inf. Technol.* **2023**, *28*, 1809–1831. [CrossRef]
53. Bygstad, B.; Øvrelid, E.; Ludvigsen, S.; Dæhlen, M. From dual digitalization to digital learning space: Exploring the digital transformation of higher education. *Comput. Educ.* **2022**, *182*, 104463. [CrossRef]
54. Costley, J. Student perceptions of academic dishonesty at a cyber-university in South Korea. *J. Acad. Ethics* **2019**, *17*, 205–217. [CrossRef]
55. Sikra, J.; Renaud, K.V.; Thomas, D.R. UK cybercrime, victims and reporting: A systematic review. *Commonw. Cybercrime J.* **2023**, *1*, 28–59.