sustainability

Article

Education, Online Presence and Cybersecurity Implications: A Study of Information Security Practices of Computing Students in Saudi Arabia

Saqib Saeed

SAUDI ARAMCO Cybersecurity Chair, Department of Computer Information Systems,
College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University,
P.O. Box 1982, Dammam 31441, Saudi Arabia; sbsaed@iau.edu.sa

Abstract: Information technology is considered as a key enabler to achieve “education for all” as a sustainable development goal; however, involvement in the education sector has introduced security risks along with benefits. Students’ exposure to the internet has increased the probability of cybersecurity attacks. To foster a more sustainable use of technology, it is crucial that students are made aware of information security risks and can keep themselves protected in the online sphere. In this paper, we present the results of a cross-sectional study that explores information-security awareness among students in Saudi Arabia. Empirical data were collected using an online questionnaire and a factor analysis was conducted using partial least-squares structured equation modelling. Based on the existing literature, we focused on four key constructs: password management, infrastructure management, email management, and the perception of security. The results of this study have highlighted that email management and infrastructure management were seen as relevant factors, whereas password management and the perception of security were not considered relevant factors by the respondents. We have also chalked out recommendations to improve cybersecurity awareness among students. The findings of this study will potentially help educational institutions and parents to prepare students in adopting security practices while they are online.

Keywords: cybersecurity; human security; privacy; security perception; security perception; user education

Citation: Saeed, S. Education, Online Presence and Cybersecurity Implications: A Study of Information Security Practices of Computing Students in Saudi Arabia. *Sustainability* **2023**, *15*, 9426. https://doi.org/10.3390/su15129426

Academic Editors: Linor L. Hadar, Ilana Paul-Binyamin and Antonio P. Gutierrez de Blume

Received: 24 April 2023
Revised: 2 June 2023
Accepted: 10 June 2023
Published: 12 June 2023

1. Introduction

The 2030 agenda for sustainable development by the United Nations has laid out seventeen goals to improve the quality of life for all humans on earth. The fourth of these goals emphasizes improving the quality of education and aims for inclusive and equitable quality education and enhancing lifelong learning opportunities for people [1]. To achieve this goal, academic institutions and other stakeholders are jointly carrying out efforts to improve education quality, with a focus on inclusivity, imparting lifelong learning skills, and providing resources for lifelong learning. Information technology can play a key role toward achieving this goal; however, there is a need to understand the implications of technology to design and develop sustainable solutions to achieve the “education for all” goal.

Technology has revolutionized the education sector, where internet connectivity and audio-visual aids have not only transformed conventional education but have also paved the way for online degrees and open courseware. [2]. Initial technological interventions in education include e-portfolios, cyber infrastructures, digital libraries, and online learning object repositories that have improved the quality of the learning experience [3]. To establish sustainability, however, such technological interventions and practices need not be copied directly from developing countries, but rather these need to be aligned and appropriated to local culture and national needs [4]. For instance, the use of artificial-intelligence-based technologies is on the rise in different domains but the adoption of such systems in academia has ethical, pedagogical, and technical implications which need to be researched extensively [5]. Educational technologies are complex and embedded in social context and learners and teachers can employ diverse ways and objectives to interact with these educational technologies [6]. Recently, during the COVID-19 pandemic, transition to online education has remained the only possibility for educational institutions to impart education.

Furthermore, an excessive online presence of students for engaging in online learning also poses additional threats in terms of cybersecurity. Therefore, to foster a more sustainable use, it is crucial that users are highly aware of cybersecurity threats and can protect themselves while being online. Recent literature reviews highlight that an increased awareness of security concerns improves the cybersecurity of end users [7–9]. Keeping this in view, in this paper, we are exploring the cybersecurity awareness of university students in Saudi Arabia, registered in undergraduate computing programs.

The Kingdom of Saudi Arabia is an important case setting due to the large student population and internet density. Saudi Arabia has a total population of 35.59 million [10]. There are more than 6 million students, in around 33,500 schools, 29 government universities and 14 private universities alongside many institutes [11]. During January 2022, there were a total of 34.84 million internet users, amounting to 97.9 percent of the population. Furthermore, the number of social media users is 29.30 million, constituting 82.3 percent of the population [10]. We specifically investigated a university in the Eastern Province of Saudi Arabia and collected data from undergraduate students registered in computing programs. The students were exposed to online learning during COVID-19. Normally, technically advanced users have higher cybersecurity sensitivity due to their technological background [12], so the findings will help to understand the cybersecurity awareness of this segment of the student body, which is supposed to be a technically advanced user set. Therefore, in our model, we have used infrastructure management, email management, password management and perception of security as key constructs. Our core finding is to identify which factors are considered relevant by students for their information security and how the information security behavior of students can be further improved.

The rest of the paper is structured as follows: Section 2 discusses related work followed by the research methodology in Section 3. Section 4 presents the findings of the study, followed by a discussion in Section 5 and a conclusion in Section 6.

2. Information Security and Online Education

In this section, we discuss related work from three different aspects. Initially, we highlight how sustainability is relevant to information security; secondly, we discuss online learning and cybersecurity implications, and this is followed by information security studies conducted in the context of Saudi Arabia.

2.1. Information Security and Sustainability

Sustainability has been explored in the information security literature in different contexts. Some researchers have highlighted the sustainability of technological infrastructure as a measure of security. For instance, Zegzhda [13] discussed how cyber-physical systems integrate computing with executive processes, so availability, privacy and integrity are not effective controls because executive systems cannot be reversed. Therefore, they proposed the sustainability of cyber-physical systems to be a criterion to measure the persistence of a cyber-physical system under destructive information security actions. On the other hand, some researchers have termed information security to foster sustainable technological infrastructure in an organizational context. For example, Choi [14] termed information security a critical barrier to foster sustainable computing and proposed that a transformational leadership approach by information security managers can improve information security. Similarly, Chu and So [15] also discussed the importance of sustainable information systems requiring appropriate information security management and stated that information security managers need to identify which information security behaviors will lead employees to report information security beaches. Some researchers have established that sustainability is an important factor contributing toward the continuity of information security practices within an organizational context. For example, Wang et al. [16] discussed how employee awareness is a key factor in fostering a sustainable security protection mechanism in organizations. In our work, we also use Wang et al.'s views on sustainability to highlight that employing optimal information security practices leads to a more sustainable use of technology for students.

2.2. Cybersecurity and Online Learning

Technological adoption in the education sector has been explored by many researchers. Kosasi et al. [17] carried out a literature review and discussed how, although there are a number of blockchain-based technologies available, there is still a significant potential for more blockchain technologies in the higher education sector. Similarly, Alam [18] discussed how blockchain-based digital certificates can be employed for learners to access online learning resources. Vlachogianni and Tselios [19] adopted a system-usability scale to evaluate the usability of different educational resources and found that the majority of online resources, university websites, and tutoring platforms have good usability. Lai et al. [20] identified the critical factors in evaluating the use of technology in the education sector, developed an instrument comprised of twenty-eight items belonging to eight different factors and evaluated its validity over a large set of students. Minamatov and Nasirdinova [21] highlighted that teachers need mastery in using digital technologies, such as text editors, spreadsheets, emails, browsers and multimedia equipment, to deliver quality education. Chen et al. [7] carried out a bibliometric analysis of papers published during 2000–2019 to understand the adoption of artificial intelligence in education domains. It found data mining for student performance prediction, automated special education tutoring systems, intelligent educational robots, computer-supported collaborative learning and recommended systems for learning as core topics of interest.

Recently, COVID-19 has changed not only the way we live but also the way we teach and learn [22]. In the post-COVID period, higher education institutions have strengthened their online infrastructure to support students' learning, and a variety of other learning resources are publicly available on the internet. This transformation has increased the online time of students which has made them more susceptible to cybersecurity threats. Arampatzis and O'Hagan [23] highlighted that increased digitalization during the pandemic period has increased the probability of cybersecurity threats due to human factors. Bukauskas et al. [24] presented their findings on how an extensive digital transformation and specialized computing skills are required by the workforce to keep their infrastructure secured. They remapped cybersecurity competencies for small nation states to enable the desired security competencies in the computing workforce. Sabillon [25] carried out an empirical study in a Canadian higher education institute and presented a cybersecurity-awareness training model for corporate sector. They also stressed the need for continued research on cybersecurity awareness to keep users abreast with changing cybersecurity challenges. Hewitt and White [8] discussed how, when people's fear of becoming a cyber victim grows, they report more security problems, and visiting unreliable websites is positively correlated with reported security events in home computers. Furthermore, they did not find any evidence of correlation between the education and cyber-optimistic bias of respondents. Olayinka and Win [26] found extensive digital transformations within business, and using diverse applications to monitor COVID-19 has introduced many security implications which require innovative solutions. Sintema [27] carried out a study in Zambia and highlighted that school closure due to COVID-19 was going to result in a higher failure rate in the national examination. Aykan and Yıldırım [28] investigated the implications of embedding the lesson-study model in online STEM education during COVID-19 and found that it resulted in improved lesson planning; however, lack of lesson planning experience, time and environmental conditions were quite challenging. Snell-Rood et al. [29] used a bio-inspiration approach to teach a biology course themed around the COVID-19 pandemic. Initially, students used mind mapping to model the problem and sub-problems relevant to the content, and later conducted an in-depth review of the literature as part of a student project. They proposed that such an approach could be used to teach a variety of topics using this inquiry-based pedagogy. Baptista et al. [30] examined how physics teachers used a STEM activity in the context of the pandemic and found that teachers who were able to innovate pedagogical approaches, integrate scientific and technical knowledge, and motivate students were able to deliver scientific knowledge to students effectively.

COVID-19 induced a transition to online learning which has made cybersecurity for students an interesting research area. Triplett [31] carried out a review study to find out how children's cybersecurity awareness was important, and concluded that the adoption of game-based strategies to increase children's awareness could be effective. Zorlu [32] conducted an empirical study with students of Bartin University, Turkey, and found that college students required awareness to keep themselves protected against cyberbullying and cybersecurity threats. The results highlighted that female students had higher awareness as compared to male students. It was also found that the intended use of the internet, cyberbullying exposure and online catfishing activities are key factors in determining awareness. Khan et al. [33] carried out an empirical study with undergraduate students and found that protection motivation theory-based training can positively change cybersecurity behavior, so practitioners should target the inclusion of a self-efficacy component of protection motivation theory in their training modules. Kasunic and Bracun [34] carried out an empirical study on applied science students at Zagreb University of Applied Sciences and found that there was cybersecurity awareness among students exhibited by careful accessing of email links, social media posts and websites. However, there was no significant difference in cybersecurity awareness between employed students and full-time students' security behavior. Lourenço et al. [35] highlighted that, in the post covid era, students and teachers are exposed to increased use of technology, and a rise in cybercrime in society advocates for more awareness and training to enhance the knowledge of the public. Eltahir and Ahmed [36] conducted an empirical study on Sudanese university students and found that the male students had relatively higher cybersecurity awareness in comparison to the female students. Furthermore, the cybersecurity behaviors of advanced computer users were different than those of moderate ones.

English and Maguire [37] explored student expectations in two UK universities to understand the concerns with cybersecurity curricula in a bid to improve the cybersecurity modules. Netshakhuma [38] carried out a cybersecurity assessment study in South African universities and found poor implementation of cybersecurity strategies by employees and students. Conducting similar studies in other geographical regions to enrich the body of knowledge has been stressed. Hong et al. [39] conducted an empirical study in China and found that education level has a significant impact on cybersecurity behavior. They found significant differences in the cybersecurity behavior of non-final year students, final year students and working graduates. Adamu et al. [40] explored cybersecurity awareness in the northeastern region of Nigeria and found that students had limited cybersecurity awareness in areas like internet banking while in cases of cyberbullying, self-protection, and internet addiction, there was reasonable awareness. Garba et al. [41] investigated Nigerian universities and found a lack of skills in protecting their data even though they claimed to be aware of cybersecurity. Furthermore, many universities did not prepare students to protect their personal data. Senthilkumar and Easwaramoorthy [42] investigated cybersecurity awareness among students in Tamil Nadu, India and found that students had a good level of awareness to keep themselves secure from cyber-attacks. Slusky and Partow-Navid [43] conducted an empirical study with the business students at California State University and found that problems with security awareness were not due to lack of security knowledge; rather students lacked application of their security knowledge in real life situations. Therefore, the academic curricula need to adopt context-based security awareness to students.

2.3. Information Security Studies in the Context of Saudi Arabia

There has been little research exploring cybersecurity implications in Saudi Arabia. Johri and Kumar [44] carried out an empirical study to evaluate the cybersecurity satisfaction of banking customers in Saudi Arabia and found that there was a need for more cybersecurity awareness for customers to ensure safe online transactions. Saeed investigated information security practices of office employees in Saudi Arabia and outlined a set of recommendations to improve information security [45]. Almarhabi et al. [46] presented a framework for the Saudi government to balance system restrictions, privacy concerns and risks of security due to a Bring your own device approach by users. Aljedaani et al. [47] empirically investigated the security perception of end users of two mobile health applications in Saudi Arabia and found that the majority of respondents were unaware of security features, so a set of usable security guidelines was proposed. AlGhamdi et al. [48] presented a model to identify factors affecting the perception of employees in adhering to information security compliance and applied it in Saudi Arabian government organizations. Mohammed and Bamasoud [49] conducted a literature review and found that there was an innate need to enhance cybersecurity awareness among university students in Saudi Arabia. Alghamdi [50] outlined a set of security threats relevant to high school students in Saudi Arabia and highlighted regular communication among schoolteachers and parents to control the negative implications of information technology. Alqahtani [51] highlighted that passwords, the use of web browsers and social media are key factors contributing toward the cybersecurity awareness of students. Alotaibi and Mukred [52] conducted an empirical study in the city of Riyadh in Saudi Arabia and identified the factors contributing to cyber-violence behaviors among university students.

Although there has been some literature focusing on cybersecurity aspects, the diversity of students' academic and geographical background and technological and cultural environment provides different challenges for cybersecurity awareness. Therefore, it is scientifically interesting to enrich this body of knowledge by developing more case studies in different geographical and cultural contexts to document best practices. Therefore, in this paper, we have explored cybersecurity awareness among computing university students in Saudi Arabia to understand their information security awareness.

3. Materials and Methods

This study is a part of a long-running project where we have been exploring information security behaviors among different types of users. In our earlier work, we investigated e-commerce shoppers [53] and office employees [45]. In this study we have focused on students to understand their information security behaviors. In the literature, we have found infrastructure management [54], password management [55], email management [56] and security perceptions of users [57] as key factors in fostering a positive information security behavior; therefore, our model is comprised of these four constructs. We have used questionnaires as a data collection tool for this cross-sectional study. In the literature [58–61], there are some cybersecurity awareness questionnaires, so for each construct of our model, we identified potential questions from these questionnaires. Furthermore, we designed additional questions for each of these four constructs. Once the questionnaire was prepared, the final version was reviewed by two colleagues for content accuracy, and it was further refined based on the feedback of reviewers. Once the questionnaire was finalized it was uploaded online in Google forms. The link was shared with potential students in the University and our qualification criteria was that respondents needed to be enrolled in a computing program. Before starting the questionnaire, the respondents were asked for their willingness to participate in the study, and told that they could leave the survey at any time. The survey did not ask for any identifiable information from respondents to keep the confidentiality of the respondents. We received a total of 198 responses. There were 56 male students and 142 female students. Based on the model in Figure 1, we formulated the following 4 hypotheses for our study.

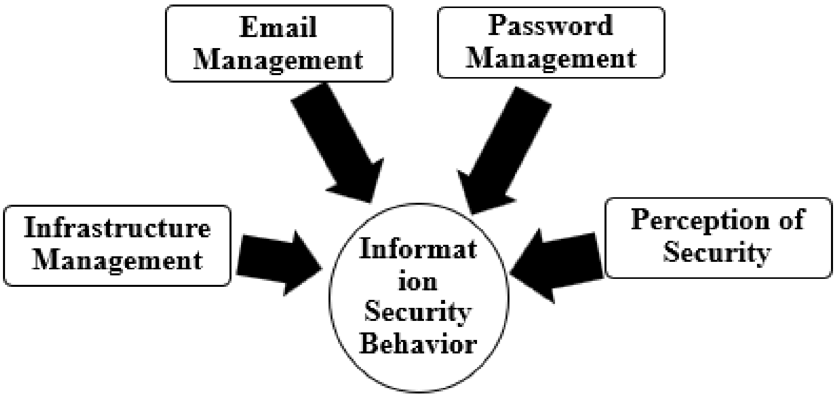

Figure 1. Research Model of the Study.

H1: *Effective password management practices lead to effective information security behavior of university students in Saudi Arabia.*

H2: *Employing appropriate measures to secure computing infrastructure leads to effective information security behavior of university students in Saudi Arabia.*

H3: *Employing secure email management practices leads to effective information security behavior of university students in Saudi Arabia.*

H4: *A positive perception of computer security leads to effective information security behavior of university students in Saudi Arabia.*

After the data collection phase, to validate our hypotheses, we coded the Excel data into numeric form and performed a factor analysis using Smart PLS 4 [62]. The bootstrapping method was applied with 5000 iterations and *p*-values were extracted to accept or reject a hypothesis.

4. Results

In our survey, there were four important sections. In the first section there were questions relevant to infrastructure management, password management, email management and perception of security related questions. As shown in Table 1, most of the respondents had an antivirus program installed on their computers which was regularly updated as well. Empirical data also highlighted that more than 60% of respondents had a firewall installed on their computers and only 31% respondents had any anti spyware software installed. Only 34% of respondents allowed scripting on their computers. Furthermore, 53% respondents reported that they locked their computers while they stepped away from the computer and 70% respondents mentioned that they used password protected screensavers.

Related to password management, we asked seven questions in our questionnaire whose results are in Table 2. In the first question we asked, in the case of wireless network connection, whether encryption or access restrictions were applied. In total, 29% respondents strongly agreed, and 24%respondents agreed to the fact that they secure their home wireless network. In response to the second question, 29% respondents strongly agreed and 32% agreed that they use same password to access multiple systems. Furthermore, 34% respondents strongly agreed, and 36% respondents agreed that they only changed their passwords when it was enforced by the policy of the respective platform/application. In the next question, 27% respondents strongly agreed, and 25% respondents agreed that they used their old password as a basis for their new password; similarly, 24% strongly agreed and 26% agreed that they documented their usernames/passwords in a written form or an electronic file. Usernames and passwords could be stored in software applications, such as internet browsers. In our survey, 51% respondents strongly agreed and 39% agreed that they used software applications to store their password. Password sharing is very dangerous for security and in our survey 20% of respondents strongly agreed and 21% agreed that they shared their passwords with other colleagues.

Table 1. Responses for Infrastructure-Management-related Questions.

Survey Question No	Infrastructure Management (ISM)-Related Questions	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Q4	My personal computer has an anti-virus program installed. (ISM 1)	37%	44%	3%	7%	10%
Q5	The antivirus program is regularly updated. (ISM 2)	37%	33%	1%	16%	12%
Q6	I have a firewall installed on my computer. (ISM 3)	33%	31%	2%	21%	13%
Q7	I use an anti-spyware tool on my computer. (ISM 4)	15%	16%	2%	31%	37%
Q8	I allow "scripting" on my computer. (ISM 5)	13%	21%	5%	31%	30%
Q9	I always log off or lock the computer when I step away from it. (ISM 6)	29%	24%	4%	21%	22%
Q10	I use a password protected screensaver. (ISM 7)	35%	35%	5%	15%	11%

Table 2. Responses to Password-Management-related Questions.

Survey Question No	Password Management (PM)-Related Questions	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Q11	If I use a wireless network at home, I secure my wireless network connection (e.g., encryption enabled or access restriction) (PM 1)	29%	24%	2%	25%	21%
Q12	I use the same password to access multiple systems. (PM 2)	29%	32%	1%	12%	26%
Q13	I change my password when it is mandatory to change due to application requirements. (PM 3)	34%	36%	5%	14%	12%
Q14	When I change my password, I use my old password as a basis. (PM 4)	27%	25%	2%	24%	23%
Q15	I keep my username/passwords in an electronic file or write them down. (PM 5)	24%	26%	4%	23%	24%
Q16	I use software to keep track of my passwords. (PM 6)	51%	39%	1%	4%	6%
Q17	I share my password with other colleagues. (PM 7)	20%	21%	2%	26%	30%

As shown in Table 3, in the context of email management, we asked four questions. In the first question we asked whether you would open emails from unknown senders. A total of 24% of respondents strongly agreed and 67% agreed that they might open emails from unknown senders. Furthermore, 50% respondents strongly agreed and 46% agreed that they might even access email attachments from unknown senders. Only 9% of respondents strongly agreed and another 9% agreed that they might use encryption to secure email communication. In the last question in this section, we asked respondents whether they reviewed the security settings of web-based email applications and only 26% strongly agreed and 21% agreed that they would review security settings.

Table 3. Responses to Email-Management-related Questions.

Survey Question No	Email Management (EM)-Related Questions	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Q18	I open emails even if I do not know who the sender is. (EM 1)	24%	67%	1%	3%	5%
Q19	I even open attachments from the emails where I do not know who the sender is. (EM 2)	50%	46%	1%	2%	2%
Q20	I use encryption when sending emails. (EM 3)	9%	9%	2%	30%	51%
Q21	While using web-based email or calendar software, I pay attention to the security settings of the web-based software. (EM 4)	26%	21%	2%	28%	22%

In this perception-of-security-related section of the questionnaire, we asked seven questions related to the perception of security of users and the results are shown in Table 4. In the first question we asked, do you think that you can protect your computer from hackers? In total, 33% strongly agreed and 44% agreed that they thought that they could protect their computer from hacking/phishing. A total of 24% of respondents strongly agreed and another 39% agreed that paying special attention to security aspects did not make any difference in securing computers. A total of 13% of respondents strongly agreed and another 28% agreed that the information contained in their computer was not interesting for hackers. Furthermore, 7% respondents agreed and another 23% agreed that if people had bad intentions, they would be able to hack into the computer and network. In response to the question stating that attention to computer security is needed, but people should not overreact, only 5% of respondents strongly agreed and another 38% agreed. A total of 12% of the respondents strongly agreed and 29% agreed that they did not use internet for financial transactions. In the last question, 4% of respondents strongly agreed and another 13% agreed that they were worried about computer security.

Table 4. Responses for Perception-of-Security-related Questions.

Survey Question No	Perception of Security (POS)-Related Questions	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Q22	I think I can protect my computer from hackers/phishers, if I take good care of computer security. (POS 1)	33%	44%	17%	3%	4%
Q23	It does make a difference if I pay special attention to computer security, such as installing a browser that is less vulnerable. (POS 2)	24%	39%	22%	11%	5%
Q24	The information that I keep on my computer is not interesting enough for people to try and hack into my computer. (POS 3)	13%	28%	35%	14%	10%
Q25	It does not matter what I do; if people have bad intentions, they will be able to hack into my computer and our network. (POS 4)	7%	23%	32%	26%	12%
Q26	Attention to computer security is needed, but people should not overreact. (POS 5)	5%	38%	35%	19%	4%
Q27	I do not like to use the Internet for financial transactions. (POS 6)	12%	39%	34%	11%	4%
Q28	Computer security worries me. (POS 7)	4%	13%	28%	40%	15%

Factor analysis was performed on the empirical data and as shown in Figure 2, infrastructure management, password management, email management, and perception of security were used as main constructs. The R-square value for the model was 0.969, which is considered acceptable [63]. Path coefficient analysis highlighted that email management to security behavior has a value of 0.621 showing a strong positive association. In the case of infrastructure management to security behavior the path coefficient value of 0.544 highlights a moderately positive association. In the case of password management to security behavior, the path coefficient value of 0.105, and for perception of security-to-security behavior the path coefficient value of 0.076, show a very weak or no association. To check the discriminant validity of the model we used the Fornell–Larcker criterion [64]. As shown in Table 5, the value of email management (0.517) is higher than the value of all the other constructs in the same column, which is true for all other columns. As a result, hypotheses H1 and H4 were rejected, whereas H2 and H3 were approved.

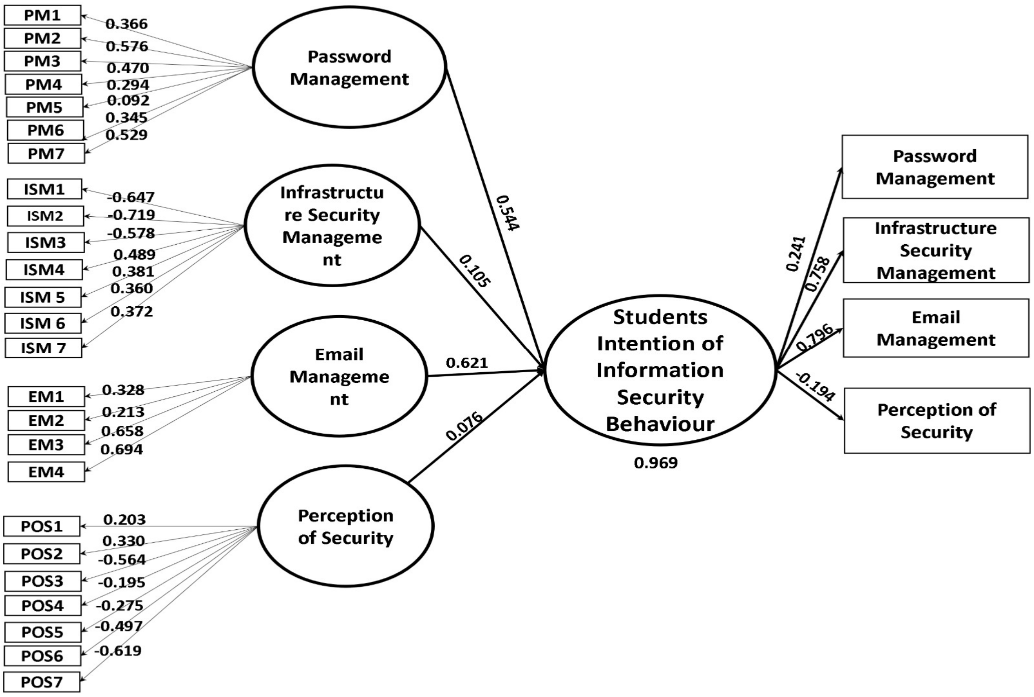

Figure 2. PLS model of the empirical data.

Table 5. Discriminant validity using Fornell-Larcker Criterion.

	Email Management	IS Management	Password Management	Perception of Security
Email Management	0.517			
IS Management	0.261	0.524		
Password Management	0.242	0.222	0.411	
Perception of Security	0.171	0.221	0.178	0.416

The mean, standard deviation, t statistics and p values of the model are given in Table 6. In the case of email management and infrastructure management the mean values are around 0.5, whereas in the case of password management and perception of security its value is on the lower side. Similarly, in case of T statistics, a value greater than +2 and less than -2 is considered acceptable so in our case email management and infrastructure management were seen as relevant factors for security behavior, whereas password management and perception of security were not considered relevant. In the case of the p-value [65], a value lower than 0.05 is considered significant and again it was seen that email management and infrastructure management were relevant factors whereas password management and perception of security proved insignificant.

Table 6. Mean, Standard Deviation, T Statistics and *p* Values.

	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (O/STDEV)	*p* Values
Email Management-to-Security Behavior	0.561	0.097	6.373	0.000
IS Management-to-Security Behavior	0.502	0.099	5.470	0.000
Password Management-to-Security Behavior	0.153	0.145	0.726	0.468
Perception of Security-to-Security Behavior	0.129	0.132	0.573	0.567

Normally, it is recommended that for a factor to be significant the factor loading value should be at least 0.2; however, the higher the value, the higher the significance is. We kept the cutoff point as 0.5 and revised the model which is shown in Figure 3.

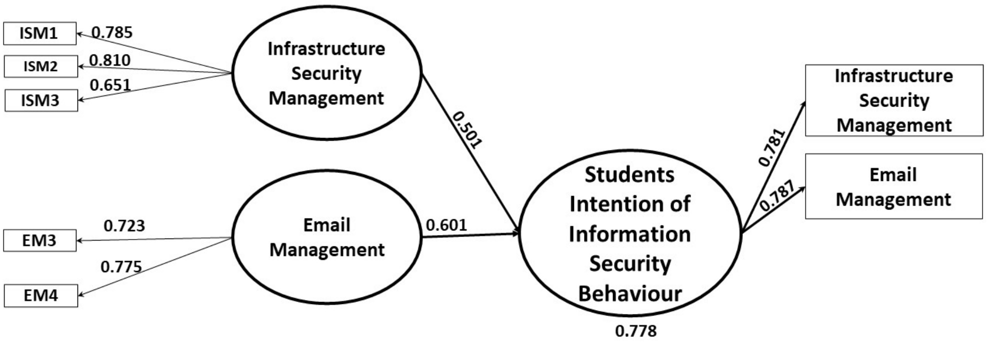
ISM1
0.785
ISM2
0.810
0.651
ISM3
Infrastructure Security Management
0.501
Infrastructure Security Management
0.781
0.787
Email Management
0.723
EM3
0.775
EM4
Email Management
0.601
Students Intention of Information Security Behaviour
0.778

Figure 3. Revised PLS model of the empirical data.

5. Discussion

“Education for all“ is an important sustainable development goal and during the pandemic online education proved to be a crucial enabler to impart education to learners. However, virtual learning environments require students to be online for an extended period which makes them prone to cyber-attacks. To foster a more sustainable use of online resources, a secure online learning environment needs to be enabled by providing students with a higher level of cybersecurity awareness. Cybersecurity is very critical to the storage of online data [66] and like other business domains [67] the education sector also needs to deal with this aspect optimally to enhance online learning. Therefore, it is imperative that while designing software systems for education, it is considered that systems need to be secure and usable. To be usable, a user-centric design approach may be adopted so that systems are aligned with user practices [68,69]. In our study, factor analysis highlighted that respondents reported infrastructure management and email management to be the key factors in their information security behaviors. In our earlier work [45], business employees did not consider infrastructure management as a key factor, and the reason could be that majority of business organizations have an IT department dedicated to maintaining the IT infrastructure, so therefore business respondents did not feel infrastructure management to be a key issue in their information security behaviors; however, earlier literature [70,71] has highlighted that this is relevant. Email management was also considered a relevant factor, which is in line with the earlier studies [56,72,73]. The perception of security and password management were not considered a relevant factor by our respondents; however, earlier studies [45,74] outlined them as a relevant factor. Password management was considered relevant by business employees in our earlier study [45] but computing students did not think it was a relevant factor. One of the potential reasons could be that the respondents were computing students who considered themselves technically advanced so they might have assumed that they were more aware of security threats, so the perception factor was irrelevant.

5.1. Theoretical Implications

Many theoretical frameworks have been established within the literature, such as protection motivation theory [53,75], and the theory of planned behavior [45,76] used in the cybersecurity literature to understand the information security behaviors of users. Protection motivation theory highlights how users respond to different security threats while working with information technology applications. On the other hand, the theory of planned behavior focuses more on when a user perceives a certain action to be useful, has the required skills and acquires appropriate support from his peers, and then it is expected that they will indulge in their desired behavior. In our case, we can refer to password management, email management and infrastructure management as perceived behavioral controls whereas perception of security could be termed as a behavioral attitude. In our case, we found that email management and infrastructure management contribute to students' intentions to engage in secure behavior.

5.2. Managerial Implications

The results of our study are helpful for educational managers, students, and policymakers. Even though our respondents were technically advanced students, we believe students from other disciplines may not have had such a high level of cybersecurity agility; therefore, we have presented a set of guidelines, shown in Figure 4, to ensure students improve their information security behavior. Students should ensure that the network from where they connect, the applications they use, operating systems and devices are secure. Additionally, the students should use online payments only on secure websites and adopt secure browsing behavior by avoiding risky sites. Educational institutions should also contribute to improving the information security behavior of students. Academic institutions need to have training programs for students to keep themselves secure while being online. Academic institutions need to have a documented institutional security policy so that students are aware of expected online behavior while on institutions' networks. This will also help them in adopting a similar cautious approach while they connect from their personal networks. This could be followed up with rewards and punishment policies for students to strictly enforce information security policy. Academic institutions can also arrange different events like hackathons, awareness workshops, secure browsing days etc. to reinforce secure behavior among students.

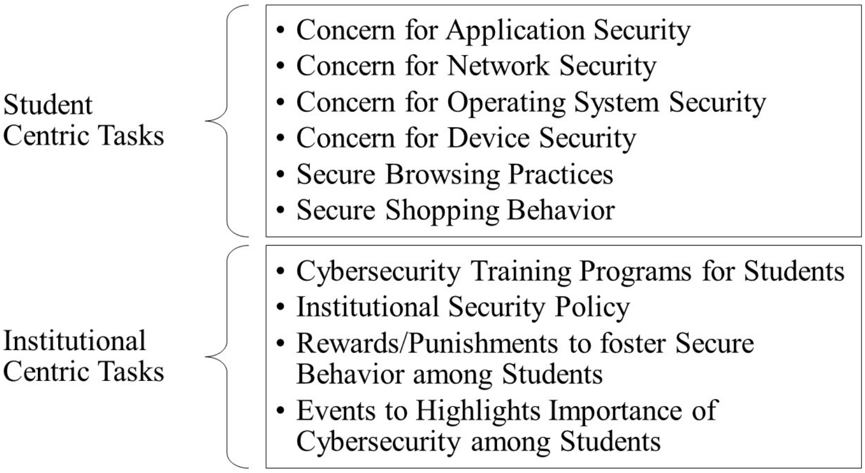
Student Centric Tasks
• Concern for Application Security
• Concern for Network Security
• Concern for Operating System Security
• Concern for Device Security
• Secure Browsing Practices
• Secure Shopping Behavior
Institutional Centric Tasks
• Cybersecurity Training Programs for Students
• Institutional Security Policy
• Rewards/Punishments to foster Secure Behavior among Students
• Events to Highlights Importance of Cybersecurity among Students

Figure 4. Guidelines to improve information security behaviors of students.

5.3. Study Limitations and Future Directions

One of the limitations of our work is that the student sample was not large enough and was not representative of the whole student population of Saudi Arabia. Therefore, the findings may not be generalized for the entire student population of Saudi Arabia. However, our study provides an interesting insight which can be further explored in depth with a large dataset. Furthermore, in the future, we intend to extend the work in different geographical regions of Saudi Arabia and would complement it with a qualitative study to understand the motivators and demotivators of information security behaviors among students. It is also scientifically very interesting to compare student perceptions in different geographical regions to understand the cultural implications on cybersecurity awareness and perceptions of students.

6. Conclusions

Quality education is crucial in attaining sustainable development goals and technology has huge potential to improve education quality and its reach. Information security, however, is a critical issue for the sustainable use of technology. In the post-pandemic era, online education has become an integral tool for academic institutions and learners and thus information security has become a major factor for students as well. In this paper, we have explored the information security behavior of computing students in a university in Saudi Arabia. We have collected the empirical data with the help of a questionnaire which was analyzed using a partial least-squares method. The findings highlighted that the respondents did not consider password management and security perception as relevant factors for information security; however, they considered email management and infrastructure management as key issues for secure information security behaviors. We further drilled down in these four categories to identify the sub-factors and found many factors which were highlighted as important in the literature but considered not relevant by our respondents. Therefore, we have identified actions to be taken by students as well as their institutions to foster secure behavior among students. The findings are of interest to academic institutions, students, and government agencies to improve information security in society.

Funding: This research was funded by SAUDI ARAMCO Cybersecurity Chair, Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia.

Institutional Review Board Statement: The study was conducted in accordance with the Declaration of Helsinki and approved by the department of computer information systems in the 24th board meeting held on 13 June 2022 and Institutional review board approval was granted on 12 February 2023. (IRB-2023-09-67).

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

Data Availability Statement: The data of this study can be requested from the corresponding author.

Acknowledgments: The authors would like to thank respondents (for filling the survey), Hina Gull (for support in data collection and analysis) and Tooba Nasir (for language review of the paper).

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

References

1. UN Sustainable Development Goals. Available online: https://sdgs.un.org/ (accessed on 17 October 2022).
2. Raja, R.; Nagasubramani, P.C. Impact of modern technology in education. *J. Appl. Adv. Res.* **2018**, *3*, 33–35. [CrossRef]
3. Ratheeswari, K. Information communication technology in education. *J. Appl. Adv. Res.* **2018**, *3*, 45–47. [CrossRef]
4. Hamidi, F.; Meshkat, M.; Rezaee, M.; Jafari, M. Information technology in education. *Procedia Comput. Sci.* **2011**, *3*, 369–373. [CrossRef]
5. Alam, A.; Mohanty, A. Foundation for the Future of Higher Education or 'Misplaced Optimism'? Being Human in the Age of Artificial Intelligence. In *Innovations in Intelligent Computing and Communication: First International Conference, ICIICC 2022, Bhubaneswar, Odisha, India, 16–17 December 2022, Proceedings*; Springer International Publishing: Cham, Switzerland, 2023; pp. 17–29.
6. Dron, J. Educational technology: What it is and how it works. *AI Soc.* **2022**, *37*, 155–166. [CrossRef]
7. Chen, X.; Zou, D.; Xie, H.; Cheng, G.; Liu, C. Two Decades of Artificial Intelligence in Education. *Educ. Technol. Soc.* **2022**, *25*, 28–47.
8. Hewitt, B.; White, G.L. Optimistic Bias and Exposure Affect Security Incidents on Home Computer. *J. Comput. Inf. Syst.* **2022**, *62*, 50–60. [CrossRef]

9. Nemec Zlatolas, L.; Feher, N.; Hölbl, M. Security perception of IoT devices in smart homes. *J. Cybersecur. Priv.* **2022**, *2*, 65–73. [CrossRef]
10. Data. Available online: https://datareportal.com/reports/digital-2022-saudi-arabia (accessed on 20 May 2023).
11. Arabnews. Available online: https://www.arabnews.com/node/2077826/saudi-arabia (accessed on 20 May 2023).
12. Mehrnezhad, M.; Toreini, E. What is this sensor and does this app need access to it? *Informatics* **2019**, *6*, 7. [CrossRef]
13. Zegzhda, D.P. Sustainability as a criterion for information security in cyber-physical systems. *Autom. Control Comput. Sci.* **2016**, *50*, 813–819. [CrossRef]
14. Choi, M. Leadership of information security manager on the effectiveness of information systems security for secure sustainable computing. *Sustainability* **2016**, *8*, 638. [CrossRef]
15. Chu, A.M.; So, M.K. Organizational information security management for sustainable information systems: An unethical employee information security behavior perspective. *Sustainability* **2020**, *12*, 3163. [CrossRef]
16. Wang, G.; Tse, D.; Cui, Y.; Jiang, H. An Exploratory Study on Sustaining Cyber Security Protection through SETA Implementation. *Sustainability* **2022**, *14*, 8319. [CrossRef]
17. Kosasi, S.; Rahardja, U.; Lutfiani, N.; Harahap, E.P.; Sari, S.N. Blockchain technology-emerging research themes opportunities in higher education. In Proceedings of the 2022 International Conference on Science and Technology (ICOSTECH), Batam City, Indonesia, 3–4 February 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–8.
18. Alam, A. Platform Utilising Blockchain Technology for eLearning and Online Education for Open Sharing of Academic Proficiency and Progress Records. In *Smart Data Intelligence: Proceedings of ICSMDI 2022*; Springer Nature Singapore: Singapore, 2022; pp. 307–320.
19. Vlachogianni, P.; Tselios, N. Perceived usability evaluation of educational technology using the System Usability Scale (SUS): A systematic review. *J. Res. Technol. Educ.* **2022**, *54*, 392–409. [CrossRef]
20. Lai, J.W.; Bower, M.; De Nobile, J.; Breyer, Y. What should we evaluate when we use technology in education? *J. Comput. Assist. Learn.* **2022**, *38*, 743–757. [CrossRef]
21. Minamatov, Y.E.O.G.L.; Nasirdinova, M.H.Q. Application of ICT in Education and Teaching Technologies. *Sci. Prog.* **2022**, *3*, 738–740.
22. Jarlhem, J.; Stigsson, J. Digital Vulnerability Awareness: In a "Working from Home" Environment during COVID-19. Bachelor Thesis, Diva, Uppasala University, Uppasala, Sweden, 2022. Available online: https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1576133&dswid=3885 (accessed on 10 November 2022).
23. Arampatzis, A.; O'Hagan, L. Cybersecurity and Privacy in the Age of the Pandemic. In *Handbook of Research on Cyberchondria 2022, Health Literacy, and the Role of Media in Society's Perception of Medical Information*; IGI Global: Hershey, PA, USA, 2022; pp. 35–53.
24. Bukauskas, L.; Brilingaitė, A.; Juozapavičius, A.; Lepaitė, D.; Ikamas, K.; Andrijauskaitė, R. Remapping cybersecurity competences in a small nation state. *Heliyon* **2023**, e12808. [CrossRef]
25. Sabillon, R. The Cybersecurity Awareness Training Model (CATRAM). In *Research Anthology on Advancements in Cybersecurity Education*; IGI Global: Hershey, PA, USA, 2022; pp. 501–520.
26. Olayinka, O.; Win, T. Cybersecurity and Data Privacy in the Digital Age: Two Case Examples. In *Handbook of Research on Digital Transformation, Industry Use Cases, and the Impact of Disruptive Technologies*; IGI Global: Hershey, PA, USA, 2022; pp. 117–131.
27. Sintema, E.J. Effect of COVID-19 on the performance of grade 12 students: Implications for STEM education. *Eurasia J. Math. Sci. Technol. Educ.* **2020**, *16*, em1851. [CrossRef]
28. Aykan, A.; Yıldırım, B. The Integration of a lesson study model into distance STEM education during the COVID-19 pandemic: Teachers' views and practice. *Technol. Knowl. Learn.* **2021**, *27*, 609–637. [CrossRef]
29. Snell-Rood, E.C.; Smirnoff, D.; Cantrell, H.; Chapman, K.; Kirscht, E.; Stretch, E. Bioinspiration as a method of problem-based STEM education: A case study with a class structured around the COVID-19 crisis. *Ecol. Evol.* **2021**, *11*, 16374–16386. [CrossRef]
30. Baptista, M.; Costa, E.; Martins, I. STEM Education during the COVID-19: Teachers' Perspectives about Strategies, Challenges and Effects on Students' Learning. *J. Balt. Sci. Educ.* **2020**, *19*, 1043–1054. [CrossRef]
31. Triplett, W.J. Addressing Cybersecurity Challenges in Education. *Int. J. STEM Educ. Sustain.* **2023**, *3*, 47–67. [CrossRef]
32. Zorlu, E. An Examination of the Relationship between College Students' Cyberbullying Awareness and Ability to Ensure their Personal Cybersecurity. *J. Learn. Teach. Digit. Age* **2023**, *8*, 55–70. [CrossRef]
33. Khan, N.F.; Ikram, N.; Murtaza, H.; Javed, M. Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's Model. *Comput. Secur.* **2023**, *125*, 103049. [CrossRef]
34. Kasunic, N.; Bracun, S. Cybersecurity awareness among applied sciences student population. *Int. J. Educ. Pedagog. Sci.* **2023**, *17*, 15–19.
35. Lourenço, J.; Morais, J.C.; Sá, S.; Neves, N.; Figueiredo, F.; Santos, M.C. Cybersecurity Concerns Under COVID-19: Representations on Increasing Digital Literacy in Higher Education. In *Perspectives and Trends in Education and Technology*; Springer: Singapore, 2023; pp. 739–748.
36. Eltahir, M.E.; Ahmed, O.S. Cybersecurity Awareness in African Higher Education Institutions: A Case Study of Sudan. *Inf. Sci. Lett.* **2023**, *12*.
37. English, R.; Maguire, J. Exploring Student Perceptions and Expectations of Cyber Security. In Proceedings of the 7th Conference on Computing Education Practice, Durham, UK, 6 January 2023; pp. 25–28. [CrossRef]

38. Netshakhuma, N.S. Cybersecurity Management in South African Universities. In *Cybersecurity Issues, Challenges, and Solutions in the Business World*; IGI Global: Hershey, PA, USA, 2023; pp. 196–211.
39. Hong, W.C.H.; Chi, C.; Liu, J.; Zhang, Y.; Lei, V.N.L.; Xu, X. The influence of social education level on cybersecurity awareness and behaviour: A comparative study of university students and working graduates. *Educ. Inf. Technol.* **2023**, *28*, 439–470. [CrossRef]
40. Adamu, A.G.; Siraj, M.M.; Othman, S.H. An assessment of cybersecurity awareness level among Northeastern University students in Nigeria. *Int. J. Electr. Comput. Eng.* **2022**, *12*, 572.
41. Garba, A.; Sirat, M.B.; Hajar, S.; Dauda, I.B. Cyber security awareness among university students: A case study. *Sci. Proc. Ser.* **2020**, *2*, 82–86. [CrossRef]
42. Senthilkumar, K.; Easwaramoorthy, S. A Survey on Cyber Security awareness among college students in Tamil Nadu. In Proceedings of the IOP Conference Series: Materials Science and Engineering, Vellore, India, 2–3 May 2017.
43. Slusky, L.; Partow-Navid, P. Students Information Security Practices and Awareness. *J. Inf. Priv. Secur.* **2012**, *8*, 3–26. [CrossRef]
44. Johri, A.; Kumar, S. Exploring Customer Awareness towards Their Cyber Security in the Kingdom of Saudi Arabia: A Study in the Era of Banking Digital Transformation. *Hum. Behav. Emerg. Technol.* **2023**, *2023*, 2103442. [CrossRef]
45. Saeed, S. Digital Workplaces and Information Security Behavior of Business Employees: An Empirical Study of Saudi Arabia. *Sustainability* **2023**, *15*, 6019. [CrossRef]
46. Almarhabi, K.; Bahaddad, A.; Alghamdi, A.M. Security management of BYOD and cloud environment in Saudi Arabia. *Alex. Eng. J.* **2023**, *63*, 103–114. [CrossRef]
47. Aljedaani, B.; Ahmad, A.; Zahedi, M.; Babar, M.A. End-users' knowledge and perception about security of clinical mobile health apps: A case study with two Saudi Arabian mHealth providers. *J. Syst. Softw.* **2023**, *195*, 111519. [CrossRef]
48. AlGhamdi, S.; Win, K.T.; Vlahu-Gjorgievska, E. Employees' intentions toward complying with information security controls in Saudi Arabia's public organisations. *Gov. Inf. Q.* **2022**, *39*, 101721. [CrossRef]
49. Mohammed, M.; Bamasoud, D.M. The Impact of Enhancing Awareness of Cybersecurity on Universities Students: A Survey Paper. *J. Theor. Appl. Inf. Technol.* **2022**, *100*.
50. Alghamdi, A.A. Cyberthreats Facing High School Students and Methods of Addressing them. *J. Inf. Secur. Cybercrimes Res.* **2022**, *5*, 116–123. [CrossRef]
51. Alqahtani, M.A. Factors Affecting Cybersecurity Awareness among University Students. *Appl. Sci.* **2022**, *12*, 2589. [CrossRef]
52. Alotaibi, N.B.; Mukred, M. Factors affecting the cyber violence behavior among Saudi youth and its relation with the suiciding: A descriptive study on university students in Riyadh city of KSA. *Technol. Soc.* **2022**, *68*, 101863. [CrossRef]
53. Saeed, S. A Customer-Centric View of E-Commerce Security and Privacy. *Appl. Sci.* **2023**, *13*, 1020. [CrossRef]
54. Koushik, P.; Chandrashekhar, A.M.; Takkalakaki, J. Information security threats, awareness and cognizance. *Int. J. Tech. Res. Eng.* **2015**, *2*, 19–28.
55. Tarwireyi, P.; Flowerday, S.; Bayaga, A. Information security competence test with regards to password management. In Proceedings of the 2011 Information Security for South Africa, Johannesburg, South Africa, 15–17 August 2011; IEEE: Piscataway, NJ, USA, 2011; pp. 1–7.
56. Kruger, H.; Drevin, L.; Steyn, T. Email security awareness—A practical assessment of employee behaviour. In Proceedings of the Fifth World Conference on Information Security Education, West Point, NY, USA, 19–21 June 2007; Springer: New York, NY, USA, 2007; pp. 33–40.
57. Huang, D.L.; Rau PL, P.; Salvendy, G. Perception of information security. *Behav. Inf. Technol.* **2010**, *29*, 221–232. [CrossRef]
58. Security Awareness Survey. Available online: https://www.securitymentor.com/resources/surveys/security-awareness-survey (accessed on 17 October 2022).
59. Hammarstrand, J.; Fu, T. Information Security Awareness and Behaviour: Of Trained and Untrained Home Users in Sweden. Bachelor's Thesis, University of Borås, Borås, Sweden, 2015.
60. Computer and Information Security End User Questionnaire. Available online: https://cqpi.wisc.edu/wp-content/uploads/sites/599/2016/07/Pilot_Study_Questionnaire.pdf (accessed on 17 October 2022).
61. SANS Security Awareness, Human Risk Assessments and Surveys, SANS Institute. Available online: https://www.sans.org/blog/getting-support-for-your-human-risk-assessments-and-surveys/ (accessed on 17 October 2022).
62. Smartpls4. Available online: https://www.smartpls.com/ (accessed on 20 May 2023).
63. Frost, J. How to Interpret R-Squared in Regression Analysis. Available online: https://statisticsbyjim.com/regression/interpret-r-squared-regression/ (accessed on 20 May 2023).
64. Discriminant Validity. Available online: https://www.analysisinn.com/post/discriminant-validity-through-fronell-larcker-criterion/#:~:text=The%20Fronell%2DLarcker%20criterion%20is,construct%20and%20any%20other%20construct (accessed on 17 October 2022).
65. What are T Values and P Values in Statistics? Available online: https://blog.minitab.com/en/statistics-and-quality-data-analysis/what-are-t-values-and-p-values-in-statistics (accessed on 20 May 2023).
66. Shahid, J.; Ahmad, R.; Kiani, A.K.; Ahmad, T.; Saeed, S.; Almuhaideb, A.M. Data protection and privacy of the internet of healthcare things (IoHTs). *Appl. Sci.* **2022**, *12*, 1927. [CrossRef]
67. Gull, H.; Saeed, S.; Iqbal, S.Z.; Bamarouf, Y.A.; Alqahtani, M.A.; Alabbad, D.A.; Saqib, M.; Al Qahtani, S.H.; Alamer, A. An Empirical Study of Mobile Commerce and Customers Security Perception in Saudi Arabia. *Electronics* **2022**, *11*, 293. [CrossRef]

68. Saeed, S.; Bamarouf, Y.A.; Ramayah, T.; Iqbal, S.Z. *Design Solutions for User-Centric Information Systems*; IGI Global: Hershey, PA, USA, 2016.
69. Saeed, S.; Malik, I.A.; Wahab, F. Usability evaluation of Pakistani security agencies websites. *Int. J. E-Politics (IJEP)* **2013**, *4*, 57–69. [CrossRef]
70. Sanok, D.J., Jr. An analysis of how antivirus methodologies are utilized in protecting computers from malicious code. In Proceedings of the 2nd Annual Conference on Information Security Curriculum Development, Kennesaw, GA, USA, 23–24 September 2005; pp. 142–144.
71. Al-Saleh, M.I.; Espinoza, A.M.; Crandall, J.R. Antivirus performance characterisation: System-wide view. *IET Inf. Secur.* **2013**, *7*, 126–133. [CrossRef]
72. Hayajneh, T.; Mohd, B.J.; Itradat, A.; Quttoum, A.N. Performance and information security evaluation with firewalls. *Int. J. Secur. Appl.* **2013**, *7*, 355–372. [CrossRef]
73. Wei, J.; Chen, X.; Wang, J.; Hu, X.; Ma, J. Forward-secure puncturable identity-based encryption for securing cloud emails. In Proceedings of the European Symposium on Research in Computer Security, Luxembourg, 23–27 September 2019; Springer: Cham, Switzerland, 2019; pp. 134–150.
74. Villamarín-Salomón, R.; Brustoloni, J.; DeSantis, M.; Brooks, A. Improving User Decisions About Opening Potentially Dangerous Attachments in E-Mail Clients. In Proceedings of the Poster, Symposium on Usable Privacy and Security, CMU, Pittsburgh, PA, USA, 12–14 July 2006.
75. Kim, J.; Mou, J. Meta-analysis of Information Security Policy Compliance Based on Theory of Planned Behavior. *J. Digit. Converg.* **2020**, *18*, 169–176.
76. Sommestad, T.; Karlzén, H.; Hallberg, J. The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Inf. Comput. Secur.* **2015**, *23*, 200–217. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.