electronics

MDPI

Article

A Quadruple "E" Approach for Effective Cyber-Hygiene Behaviour and Attitude toward Online Learning among Higher-Education Students in Saudi Arabia amid COVID-19 Pandemic

Mostafa Aboulnour Salem [1,*] and Abu Elnasr E. Sobaih [2,3,*]

[1] Deanship of Development and Quality Assurance, King Faisal University, Al-Ahsa 31982, Saudi Arabia
[2] Management Department, College of Business Administration, King Faisal University, Al-Ahsa 31982, Saudi Arabia
[3] Hotel Management Department, Faculty of Tourism and Hotel Management, Helwan University, Cairo 12612, Egypt
* Correspondence: masalem@kfu.edu.sa (M.A.S.); asobaih@kfu.edu.sa (A.E.E.S.)

Abstract: The spread of SARS-CoV-2 (COVID-19) has made online learning more common worldwide than ever before. However, recent research showed that higher-education students in the Kingdom of Saudi Arabia (KSA) were exposed to cyber threats and attacks during online learning that affected their attitudes toward online learning, despite a high level of cybersecurity infrastructure and digital capabilities in KSA universities. There were several calls for enhancing higher-education students' cyber-hygiene awareness to improve their cybersecurity behaviours, develop healthy cyber-hygiene habits, and ensure positive attitudes toward online learning amid COVID-19. The current research developed an integrated cyber-hygiene model for improving this behaviour entitled the quadruple "E" approach (QEA), which includes four stages: educate (E1), explore (E2), execute (E3), and evaluate (E4). The research compares students' cyber-hygiene behaviour and attitude toward online learning pre- and post-implementation of QEA. A sample of 446 bachelor students distributed between females and males in four public KSA universities was adopted during the academic year 2021. The results showed statistically significant differences in students' cyber-hygiene behaviour and attitude toward online learning pre- and post-adoption of the QEA. Students showed more positive cyber-hygiene behaviour and attitudes toward online learning post-QEA adoption than pre-QEA implementation. In addition, female students have more positive behaviour and attitudes than their male counterparts post the adoption of QEA. The current research stimulates positive cyber-hygiene behaviour and enhances attitudes toward online learning in universities, which have implications for the sustainability of KSA higher education, particularly in relation to SDGs 4 and 10.

Keywords: cyber-hygiene behaviour; cyber-hygiene awareness; cyber threats; online learning; quadruple "E" approach (QAE); COVID-19

Citation: Salem, M.A.; Sobaih, A.E.E. A Quadruple "E" Approach for Effective Cyber-Hygiene Behaviour and Attitude toward Online Learning among Higher-Education Students in Saudi Arabia amid COVID-19 Pandemic. *Electronics* **2023**, *12*, 2268. https://doi.org/10.3390/electronics12102268

Academic Editors: Sébastien Jacques, Mohammed Amin Almaiah, Ahmad Al-Khasawneh and Omar Almomani

Received: 5 April 2023
Revised: 15 May 2023
Accepted: 16 May 2023
Published: 17 May 2023

1. Introduction

Similar to numerous other countries worldwide, the Kingdom of Saudi Arabia (KSA) has turned education from conventional classrooms with physical attendance to online learning with virtual classrooms due to SARS-CoV-2 (COVID-19) in the first quarter of 2020 [1,2]. Amid COVID-19, students in higher-education institutions have adopted online learning at a distance to ensure the sustainability of their learning process [3]. However, students have experienced some difficulties in switching to online learning [4]. Despite the high level of cybersecurity infrastructure in universities and students' digital abilities, recent research [5,6] showed that higher-education students were exposed to cyber threats and cyber-attacks during online learning amid COVID-19, which influenced their attitudes toward online learning [7]. According to Alzubaidi [5], cyber-attacks and cyber threats

came while students were using their personal devices, such as computers, tablets, and mobile phones. Alharbi. 2021 [6] added that several cyber-attacks resulted from a lack of students' awareness of cybersecurity practices and related habits, such as cyber hygiene.

The European Union's Agency for Network and Information Security (ENISA) regards cyber hygiene as being identical to personal hygiene; once aware, it will be uncomplicated daily habits, good behaviours, and periodic check-ups to achieve optimum e-health situations [8]. Additionally, the constant cyber-hygiene habits improve and balance the cybersecurity levels for online learning tools, whether hardware/devices or software/applications [9]. Therefore, cyber hygiene and adequate protective measures mitigate cyber-attack consequences [10]. Cyber-hygiene awareness aims to adopt the best cybersecurity practices to protect and maintain systems and devices connected to the Internet [11]. Moreover, cyber-hygiene enables users of technologies to operate safe and secure online learning behaviours [12]. According to Baraković [13], to avoid increasing cyber risks, students in higher education should have an awareness of and promote cyber-hygiene practices, especially for those with access to essential resources. Likewise, students who utilise mobile devices for learning, open unknown email links, have flexible passwords, use social networking in education, have sensitive data like teachers do, move with their devices, utilise different Wi-Fi networks, etc., should have cyber-hygiene habits [14].

This research has three key objectives. The first objective of the research is to develop an approach for positively influencing higher-education students' cyber-hygiene behaviour and attitude toward online learning in KSA. The second research objective is to assess cyber-hygiene behaviour and attitude toward online learning amid COVID-19 among higher-education students in KSA pre- and post-implementation of the newly developed approach. The third research objective is to compare cyber-hygiene behaviour and attitudes toward online learning amid COVID-19 between male and female higher-education students in KSA post-implementation of the newly developed approach. These three objectives answer three research questions. First, what are the perceptions of higher-education students in KSA regarding cyber-hygiene behaviour and attitudes toward online learning amid COVID-19? Second, what is the structure of the new model to enhance cyber-hygiene behaviour and attitudes toward online learning among higher-education students in KSA amid COVID-19? Third, are there any differences in cyber-hygiene behaviours and attitudes toward online learning between males and females post the implementation of the newly developed approach? Understanding the differences between males and females is important because earlier research showed significant differences between males and females in relation to their attitudes toward online learning amid COVID-19 [15]. Females in KSA universities reported more positive attitudes than males toward online learning amid COVID-19 [15]. This research study investigated whether such differences still existed after the model adoption. The current article is organised as follows: The first section is the introduction, which highlights the research problem, purpose, and question. The second section reviews the previously undertaken related studies. The third section shows the research methodology adopted in the research. The fourth section presents the results. The fifth section is the discussion and conclusions of the significant results. The last section is about limitations and future research work.

2. Theoretical Foundation

2.1. Online Learning and Cyber Threats amid COVID-19

Amid the COVID-19 era, higher-education institutions (HEIs) in KSA, like those in many other countries around the world, were forced to undertake a digital transformation in education methodologies [16]. Thus, students were pushed to learn remotely/online from their regular classroom [3]. Despite many challenges that emerged through the online learning approach, amid COVID-19, the learning infrastructure in the HEIs in the KSA was ready to quickly shift from a traditional to a remote-learning approach [17]. Accordingly, the notable high cybersecurity infrastructure enabled educators and students to continue the remote educational process [18]. Hence, the success of the digital educational transfor-

mation pivoted on adequate infrastructure and high-security data [19]. Despite the strength of cybersecurity systems in the HEIs, various challenges emerged related to cybersecurity among students amid COVID-19 [20]. According to Li and Liu [21], Rathod [22], and Alsaadi [23], many students were exposed to cyber-attacks during the COVID-19 pandemic; some of these attacks occurred during the online learning process. Furthermore, other reports [18] confirmed that cybersecurity awareness among students in the HEIs is poor, and further research studies are needed to address this issue among higher-education students. According to Shadab et al. [24], there is a need to raise awareness among educators and students to ensure the soft, safe, and secure transformation in HEIs amid COVID-19. Alex et al. [25] confirmed that cyber-attacks are more common among students' educational devices, such as personal computers, tablets, and mobile phones.

Research [21,22,26] has shown that most cyber-attacks were mainly due to a lack of students' knowledge regarding cybersecurity skills, understanding, habits, hygiene, and software tools used for protection. In Pakistan, the cybersecurity and cyber-hygiene awareness among students at the HEIs significantly affected online learning security and risk perception, response efficacy and self-efficacy, and attitude toward online education [27]. Similarly, in Bangladesh, the agreed context indicated that the respondents' familiarity with cybersecurity and cyber awareness affected online learning and decreased e-assessment anxiety [28]. A similar conclusion was documented by higher-education students in Malaysia, indicating the requirement to enrich cyber-awareness practices in the HEIs in general in emerging countries [29]. Likewise, awareness campaigns regarding cybersecurity, especially in KSA higher education, had a crucial impact on students' online learning and increased the learning outcomes [30]. Hence, the lack of students' awareness and unawareness of cyber habits, practices, and hygiene led to cyber threats targeting students' smart devices [31]. Alsulami et al. [32] confirmed that the awareness and coaching schedules should focus on suitable habits or practices in cyber-hygiene and cybersecurity for students in the HEIs are necessary to decrease the opportunities of becoming a victim or attack spreader. Likewise, cyber-hygiene behaviours have an influential part on cybersecurity over the world [33]. To the best or researchers' knowledge, there is a lack of research on the best practices of associated awareness with students' good cyber-hygiene behaviours and attitudes to improve the method to gain good online learning.

2.2. Cyber-Hygiene Awareness and Behaviours

Everyone has practiced personal hygiene since childhood, but how many people practice personal cyber hygiene? Primarily, hygiene practices help maintain health and prevent disease attacks; cyber hygiene allows people to save their computers, mobile, email, and others from cyber-attacks [12,24]. The cyber hygiene signifies factors of cyber interaction among people [10]. Moreover, cyber hygiene is a key to cybersecurity, including technologies' self-protection and risk behaviours [24]. Cyber hygiene is defined as appropriately implementing the most valuable cybersecurity practices to decrease the cyber threat and save personal hardware, software, and data [33]. Cyber-hygiene awareness is critical to lowering instigated infringements of cybersecurity, as shown in [34]. Likewise, cyber-hygiene awareness refers to the knowledge and adaptive behaviours for mitigating online risks, such as online learning activities that risk personal data [29]. Cyber-hygiene awareness and behaviours maintain an influential position in cybersecurity terms across the globe, especially in online learning amid the COVID-19 era [13].

Furthermore, several studies [35,36] investigated the effect of cyber-hygiene awareness on sustainable online learning amid COVID-19. According to Eboibi [37] and Ugwu et al. [38], cyber-hygiene awareness helped students in higher education in Nigeria to become more sustainable in their practices and minimise the rate of cyber-attacks among students. Likewise, the study by Toquero [20] and Indolfi et al. [39] among higher-education students in the Philippines showed that they are somewhat aware of the potential cyber-attacks and sometimes practice cyber-hygiene protective behaviours for sustainable remote learning amid COVID-19. In India, the study by Rathod [22] indicated a practical need

to heighten personal cybersecurity among higher-education students who constantly use distance education through the diversity of cyber-hygiene knowledge, awareness, and behaviours. In UAE, implementing the approaches of cyber-hygiene awareness concern applied as a holistic approach in higher education is critical to affecting online learning practices amid COVID-19 [40]. Other articles from the Arab Region empirically examined cyber-hygiene culture and awareness among students in higher-education organisations that were found to have a lack of cyber-hygiene cognition, knowledge, and skills [41,42]. Moreover, many articles in emerging countries recommended further validation of cyber-hygiene awareness, behaviours, and attitudes during online-learning contexts [13,24,43]. Hence, several studies displayed that the cybersecurity awareness approaches in higher education should significantly increase awareness of cyber-hygiene issues [12,37].

Despite the importance of awareness of cyber-hygiene issues as an approach to protecting against cyber threats, both as a critical cybersecurity technique and as an essential factor of sustainable online learning in higher education, limited studies have examined the strategies for enhancing cyber hygiene, behaviours, and their role in students' attitudes toward online learning in KSA. Accordingly, based upon the above debate, the current article expects to understand the role of cyber-hygiene awareness among higher-education students in KSA toward online learning amid global health emergencies, i.e., COVID-19.

3. Research Methodology

3.1. Phase 1: Developing a Quadruple "E" Approach

As discussed earlier, amid the COVID-19 pandemic, students in KSA higher-education institutions reported negative attitudes toward online learning [2,13,24,43]. This negative attitude toward online learning among students is supplemented by weak awareness of cybersecurity [44–47]. However, cyber-hygiene behaviours and habits are highly acknowledged for achieving a positive attitude toward online learning [43,44,46]. Hence, the first phase of the current study aimed to achieve the first research objective by developing an integrated approach to enhance cyber-hygiene awareness among higher-education students. This approach (a quadruple "E" approach) has the following four main stages (Figure 1):

- Educate (E1): In this stage, the educators provide students with knowledge, skills, and competencies to increase cyber-hygiene awareness.
- Explore (E2): In this stage, the students learn individually to enrich their knowledge, skills, and competencies to increase cyber-hygiene awareness.
- Execute (E3): In this stage, the students practice cyber hygiene on their devices according to the knowledge, skills, and competencies gained in the E1 and E2 stages.
- Evaluate (E4): This stage assesses cyber-hygiene behaviour and attitudes toward online learning among students who practice cyber hygiene on their devices according to the knowledge, skills, and competencies gained in the E1, E2 and E3 stages.

To achieve Stage 1, i.e., educate (E1), of the quadruple "E" approach, the literature related to cyber hygiene [9,48,49] and cybersecurity [43,50,51] were analysed. Furthermore, the educational contents provided were developed based on the educational theories: Piaget's Cognitive Constructivism [52], Skinner's Behaviourism Learning [53], and Self-Regulated Learning (SRL) [54]. Additionally, the contents included eleven learning modules: the first module was a briefing (M1); the subsequent two modules were the main issues—personal cyber-hygiene definition (M2) and personal cyber-hygiene benefits (M3); the following modules were about personal cyber-hygiene tips—mobile security tips (M4), passwords tips (M5), email-phishing tips (M6), social networks tips (M7), sensitive/non-sensitive tips (M8), move with device tips (M9), and general protection tips (M10); and the last module was discussion (M11). Furthermore, 20 experts and specialists in network security, cybersecurity, information technology, and instructional technology have reviewed the learning modules in some Middle Eastern countries (see Table 1).

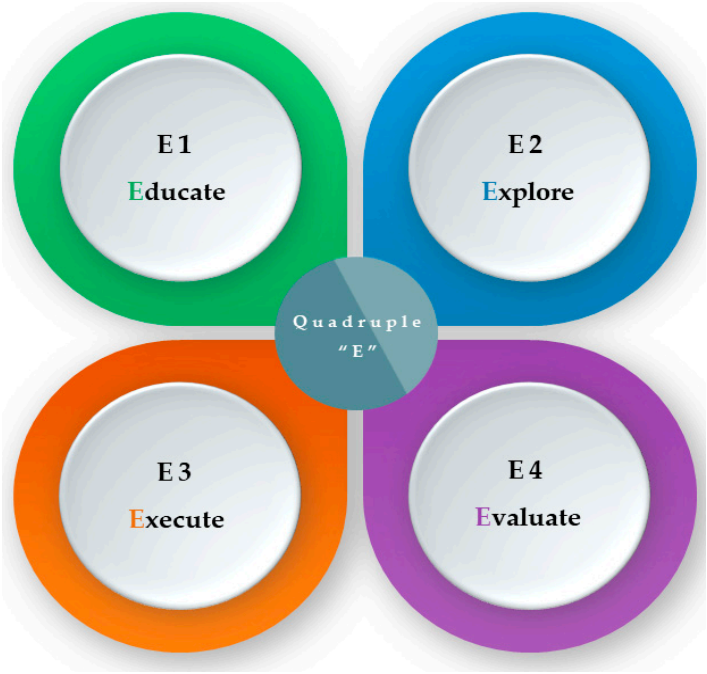

Figure 1. A quadruple "E" approach.

Table 1. Experts' demographical characteristics.

Profile	Frequency	Percentage
Gender		
Male	6	30%
Female	14	70%
Country		
Egypt	8	40%
Jordan	5	25%
Saudi Arabia	7	35%
Experts' minor specialist		
Network security	8	40%
Cybersecurity	2	10%
Information technology	3	15%
Instructional technology	7	35%
Sum	20	100%

Experts were identified based on their minor specialists (Table 1) to help review the modules. Experts were identified by using personal networks. There was also a snowballing effect, as some experts recommended other experts who met the criteria. All experts were academics with at least ten years of work experience in their minor. Likewise, the learning modules were spread through either experts' emails or social networks, i.e., WhatsApp, on 1 September 2021 based on their preferences of the contact way. The modules were kept for three weeks of discussion with the experts. Day by day, replies were checked and monitored. Experts were asked to assess the contents developed of all modules. They were asked to comment on the quality of the information provided, which was developed based on the literature review, as discussed earlier. Several parts of the modules were modified based on the comments of the experts; hence, 11 modules were finalised instead of 12 as sensitive tips, and non-sensitive tips were integrated into a module. Experts were asked to assess the revised modules. Overall, experts were satisfied with the developed contents and with a mean score of 4.641 or above (see Table 2; full details about the modules are in the Supplementary Materials).

Table 2. Experts' assessment of the validity of the learning modules (n = 20).

Learning Modules	Min	Max	M	SD	Skewness	Kurtosis
M1	4	5	4.652	0.310	−1.205	1.034
M2	3	5	4.781	0.343	−0.114	1.248
M3	4	5	4.658	0.333	−1.354	1.034
M4	4	5	4.721	0.325	−0.221	1.449
M5	4	5	4.684	0.298	−1.105	1.034
M6	4	5	4.792	0.387	−1.168	1.087
M7	4	5	4.657	0.306	−0.314	1.449
M8	4	5	4.981	0.338	−1.239	0.984
M9	4	5	4.745	0.317	−1.805	1.034
M10	4	5	4.641	0.239	−1.539	1.352
M11	4	5	4.784	0.359	−1.505	1.034

The cyber-hygiene awareness approach learning modules were executed by being integrated into the Computer Introduction Course (CIC, a general mandatory course for all colleges) to develop the student's knowledge and skills, competencies, attitudes, and behaviours in cyber-hygiene security. On 1 October 2021, the learning modules were taught for eleven lectures (165 min, i.e., 15 min per lecture). All sessions were provided by the research team with support from the module tutors. Tutors were informed about the study and were asked to participate voluntarily in the study. They are all interested in participating in and supporting the research study.

To achieve Stage 2, which is to explore (E2) the quadruple "E" approach (QEA), a self-diagnosis application was developed based on the following criteria:

- The content understanding, ambiguously, accessibility, and inclusion of all learning modules' topics.
- Feedback was shown after the selected answer for each question, true or false, with reinforcement.
- Feedback included a list of further readings, tips, and hints students should follow and noteworthy self-diagnosis application based on the eleven learning modules' content (see Figure 2 as an example of self-diagnosis; full details are in the Supplementary Materials).

After designing the self-diagnosis application, the investigator provided it to students by teaching each module of the eleven learning modules to learn individually.

To achieve Stage 3, which is the execute (E3) part of the quadruple "E" approach, a cyber-hygiene checklist was developed. Students used it to apply hygiene practices to their devices according to the knowledge, skills, and competencies gained in the E1 and E2 stages (please see Supplementary Materials). Stage 4, evaluate (E4), is discussed in the next section.

3.2. Phase 2: Evaluating Cyber-Hygiene Behaviour and Attitude toward Online Learning

The study's second phase assesses students' cyber-hygiene behaviour and attitude toward online learning, both before and after the quadruple "E" approach. To examine the students' cyber-hygiene behaviours, an instrument which included 20 items was adopted. Likewise, the instrument displayed satisfactory reliability and emanated from [24,34,55]. The instrument's 20 items were included to define seven factors: mobile security (2 items; $\alpha = 0.719$), passwords (3 items; $\alpha = 0.711$), email phishing (3 items; $\alpha = 0.737$), social networks (2 items; $\alpha = 0.813$), sensitive/non-sensitive data (3 items; $\alpha = 0.791$), move with a device (3 items; $\alpha = 0.772$), and general protection (4 items; $\alpha = 0.701$). The items were on a Likert scale (5 intervals). Students were asked to tick one of five choices to specify the grade to which they reflected the remarked cyber-hygiene behaviours. Five refers to strongly agree, whereas one refers to strongly disagree. Additionally, higher scores refer to negative cyber-hygiene behaviour, whereas lower score refers to positive cyber-hygiene behaviour.

Figure 2. Example of question layout in self-diagnose.

Furthermore, to examine the students' attitudes toward online learning, the investigators adopted an instrument which included 12 items. The instrument displayed satisfactory reliability and emanated from [56–58]. The instrument's 12 items were included to define three factors: mobile security: knowledge development (4 items; $\alpha = 0.811$), skills development (4 items; $\alpha = 0.798$), and learning attitudes (4 items; $\alpha = 0.834$). The items were on a Likert scale (with 5 intervals). The students were asked to select a tick of five choices to specify the grade to which they reflected their attitudes toward online learning. The total number of items in the final questionnaire was 32 items for both cyber-hygiene behaviours (20 items) and attitudes toward online learning (12 items).

We invited about 700 students to participate in the two phases and ended with 446 students participating in the two phases of the research (pre- and post-QEA adoption). The response rate was about 64%. According to Hill [50], the sample size calculation must be based on the total number of items, which should be at least five responses for each item. As highlighted earlier, the items used in the current article were 32. Furthermore, Muthén [51] added that a sample should be more than 150. This sample size was

distributed between females and males in four universities in the KSA (King Faisal University (KFU), Imam Muhammad bin Saud Islamic University (IMSIU), Northern Border University (NBU), and Gazan University (GU)) that covers the prominent locations in the KSA, during the academic year 2022 (see Table 3).

Table 3. Sample demographical characteristics.

The Demographical Items	Frequency	Percentage
	Gender	
Female	244	54.71%
Male	202	45.29%
Total	446	100%
	Universities	
KFU	183	41.03%
IMSIU	84	18.83%
NBU	97	21.75%
GU	82	18.39%
Total	446	100.00%

The surveys were provided to students via their emails with support from the tutors after approval from the universities. The purpose of the study was explained to students, and they were motivated to participate through different social networks, i.e., WhatsApp. They were informed that the results support the development of an approach to enhance students' cyber-hygiene behaviour and attitude toward online learning in KSA universities. There were two phases of the questionnaire distribution pre-QEA and post-QEA adoption. There was a code for each student to match pre- and post-answers together for comparison. There was no power bias or authority over students to participate in the study or express a certain opinion. They were informed that the survey was for scientific research and that their responses would be unidentified. Participation was voluntary and anonymous, and all the essential safeguards were on site to assure data confidentiality. All personally identifiable information about them was removed from the publicly available analysis to ensure that answers could not be recognised. Furthermore, items such as name and age were optional.

Descriptive statistics (mean and standard deviation) were used to analyse the students' cyber-hygiene security behaviours and attitudes toward online-learning sustainability items. The answers of two items were reversed, i.e., 1 becomes 5 and 2 becomes 4 and so on, as suggested by Buss and Perry [59] for proper data analysis. Furthermore, to compare students' cyber-hygiene behaviour and attitudes toward online learning pre- and post-adoption of QEA, the paired sample t-test was undertaken, as suggested by Hinton et al., 2004 [60]. Furthermore, an independent sample t-test was adopted to compare female and male students' cyber-hygiene behaviour and attitudes toward online learning post-adoption of QEA [60]. To examine the size of differences between pre- and post-QEA adoption and the differences between male and female students, eta squared was adopted [60].

4. Results

4.1. The Students' Cyber-Hygiene Behaviours

Descriptive statistics, e.g., mean (M) and standard deviation (SD), were adopted to assess students' cyber-hygiene behaviours among students in higher-education institutions, both pre- and post-adoption of the QEA (Table 4). The results showed that the mean score of students' cyber-hygiene behaviours of pre-QEA adoption was higher than their post-QEA adoption. The pre-QEA adoption varies between M = 3.350 (SD 0.477) and M = 5.000 (SD 0.000). Conversely, the mean of post-QEA adoption varies between M = 1.310 (SD 0.576) and 1.390 (SD 0.595). As highlighted earlier, the high score means negative cyber-hygiene behaviours, whereas the low score means positive cyber-hygiene behaviours. Thus, these results show differences between students' cyber-hygiene behaviour pre- and post-QEA

adoption. To what extent this difference was statistically significant was examined using the paired sample *t*-test.

Table 4. Descriptive statistics of students' cyber-hygiene behaviours.

Pre-QEA		Cyber-Hygiene Behaviours	Post- QEA	
M	**SD**		**M**	**SD**
5.985	0.526	Mobile security	1.334	0.477
4.310	0.576	I am checking software on my smartphone is up to date *.	1.350	0.477
3.350	0.477	I am downloading multimedia, such as music, films, and games, from unlicensed sources.	1.320	0.468
4.886	0.158	Passwords	1.336	0.510
4.660	0.476	For multiple websites, I am utilising the same password.	1.320	0.468
5.000	0.000	I am sharing my passwords with colleagues and friends.	1.390	0.595
5.000	0.000	I am creating my passwords and using those uncomplex ones, i.e., my name, birthdate, and others.	1.320	0.468
4.550	0.476	Email phishing	1.336	0.582
4.340	0.476	I click on any hyperlinks from trusted friends or colleagues and forward them by email.	1.390	0.595
5.000	0.000	I am downloading any material, data, and apps received by email on my devices without checking their authenticity.	1.310	0.576
4.310	0.954	I click on any hyperlinks from unsolicited and unknown sources and forward them by email.	1.310	0.576
4.500	0.463	Social networks	1.310	0.576
4.310	0.463	On social networks, I enjoy sharing my recent location.	1.310	0.576
4.690	0.463	On social networks, enough for me to recognise the sender's photo to accept friendship requests and join.	1.310	0.576
4.770	0.317	Data sensitivity	1.310	0576
4.650	0.477	I do not care about entering payment details on websites, which not have clear security certifications/information.	1.310	0.576
4.660	0.476	I do not care about using personal or shared storage tools to save and exchange sensitive or confidential data.	1.310	0.576
5.000	0.000	I trust my friends and colleagues to have advice on cybersecurity methods to handle sensitive data.	1.311	0.575
4.666	0.316	Move with a device	1.317	0.503
4.344	0.475	In public places, I disable private Wi-Fi and use free-access public Wi-Fi.	1.321	0.467
4.655	0.475	I am bringing my USB to the university to transfer data onto it.	1.311	0.575
5.000	0.000	I store personal, family and friends' data on my e-device (e.g., smartphone/tablet/laptop).	1.321	0.467
4.711	0.479	General protection	1.355	0.531
4.502	0.501	Anti-virus software updates: I check it regularly.	1.321	0.467
5.000	0.000	I do not care about downloading free or purchased anti-virus software from an unknown source.	1.321	0.467
4.652	0.476	I am disabling the anti-virus on my computer to download information from websites.	1.389	0.595
4.691	0.462	I am sending personal information to unknown people over the Internet.	1.389	0.595

* Reversed item: The answer is reversed, i.e., 1 becomes 5 and 2 becomes 4 and so on.

Table 5 compares students' cyber-hygiene behaviour pre- and post-QEA adoption. The comparison included all variables of cyber-hygiene behaviour: mobile security (MS), passwords (Ps), email phishing (EP), social networks (SN), data sensitivity (DS), move with a device (MwD), and general protection (GP). The results of the paired sample t-test indicated significant differences between pre- and post-QEA adoptions in all variables ($p < 0.001$). After the adoption of the approach, the cyber-hygiene behaviours became more positive compared to pre-QEA adoption for the same group of students. The students' cyber-hygiene behaviours were positively impacted because of the integrated learning modules based on Piaget's cognitive constructivist theory that evolved knowledge, skills, and competencies in cyber-hygiene security. Moreover, a self-diagnosis application evolved

the knowledge level related to cyber hygiene; moreover, the assessment activities did not contribute. The effect size was very large, as confirmed by eta squared above 0.90.

Table 5. The paired sample *t*-test for cyber-hygiene behaviours.

Cyber-Hygiene Behaviours		M	SD	*t*	*p*	η^2
Mobile security	pre	7.660	0.953	−90.911	0.000	0.917
	post	2.684	0.707			
Passwords	pre	14.661	0.475	−186.932	0.000	0.948
	post	4.022	1.093			
Email phishing	pre	13.651	1.270	−111.510	0.000	0.955
	post	4.000	1.331			
Sensitive/non-sensitive	pre	9.000	0.000	−116.560	0.000	0.941
	post	2.612	1.157			
Social networks	pre	14.311	0.463	−122.043	0.000	0.964
	post	3.921	1.735			
Move with a device	pre	14.000	0.000	−202.606	0.000	0.957
	post	3.941	1.049			
General protection	pre	18.412	0.905	−158.679	0.000	0.921
	post	5.401	1.497			

4.2. The Students' Attitude toward Online Learning

Descriptive statistics, e.g., mean (M) and standard deviation (SD), were adopted to assess students' attitudes toward online learning in higher-education institutions, both pre- and post-adoption of the QEA (Table 6). The results showed that the mean score of students' attitudes toward online learning of pre-QEA adoption was less than their post-QEA adoption. The pre-QEA adoption varies between M = 1.230 (SD 0.581) and M = 3.350 (SD 0.477). Conversely, the mean of post-QEA adoption varies between 2.350 (SD 0.569) and 5.00 (SD 0.000). It is interesting that students agreed that online learning is of the same value of traditional classroom after the adoption of the model. However, the results show that there are differences between students' attitudes toward online learning pre- and post-QEA adoption. To what extent this difference was statistically significant will be examined using the paired sample *t*-test.

Table 6. Descriptive statistics of students' attitudes toward online learning sustainability.

Pre-QEA		Attitude Toward Online Learning Items	Post-QEA	
M	SD		M	SD
1.038	0.512	Online learning and knowledge development	3.008	0.381
1.230	0.581	I find that online learning helps me learn complicated concepts.	4.350	0.477
1.330	0.470	I think it has reduced the psychological impact of COVID-19.	5.000	0.000
2.350	0.477	I do not trust online learning to complete lectures amid COVID-19 *.	4.350	0.569
1.320	0.518	I believe it has diminished the cyber-attacks amid COVID-19.	4.350	0.477
1.357	0.559	Online learning and skills development	4.512	0.357
1.310	0.576	I see that online learning increases my interaction in lectures.	5.000	0.000
1.380	0.594	I think it gave me new learning skills.	4.350	0.477
1.410	0.598	I believe it has enabled me to learn a lot in a short time.	4.350	0.477
1.330	0.470	I feel it has helped me to learn about cybersecurity skills quickly.	4.350	0.477
1.760	0.412	Online learning and learning attitudes	4.008	0.379

Table 6. *Cont.*

Pre-QEA		Attitude Toward Online Learning Items	Post-QEA	
M	**SD**		**M**	**SD**
1.000	0.000	I think online learning is essential and indispensable even after COVID-19.	4.330	0.470
3.350	0.477	The traditional classroom is better than online learning.	2.350	0.569
1.310	0.576	I believe that teaching methods used via online classrooms are better than teaching methods in traditional classrooms.	5.000	0.000
1.380	0.594	I enjoy the experience and want it to continue.	4.350	0.477

* Reversed item: The answer is reversed, i.e., 1 becomes 5 and 2 becomes 4 and so on.

Table 7 compares students' attitudes toward online learning pre- and post-QEA adoption. The comparison included all variables of attitude toward online learning: knowledge development, skill development and learning attitude. The results of paired sample t-test indicated significant differences between pre- and post-QEA adoptions in all variables ($p < 0.001$). After the adoption of the approach, students' attitudes toward online learning became more positive compared to pre-QEA adoption for the same group of students. According to the data collected, the students' attitudes toward online learning were positively impacted because adopting the cyber-hygiene awareness QEA evolved the ability to solve cyber problems facing students during online learning. Moreover, awareness QEA included diverse knowledge, skills and concepts presented about cyber-hygiene, which were given to students by coaching and motivated them to prevent cyber-attacks early before becoming cyber victims, which enhanced their performance, responses, and attitudes toward online learning sustainability. The effect size was very large, as confirmed by eta squared above 0.90, confirming major differences between the two groups.

Table 7. The paired sample *t*-test for attitudes toward online learning.

Attitude Toward Online Learning		M	SD	*t*	*p*	η^2
Online learning and knowledge development	pre	6.239	1.029	−141.335	0.000	0.936
	post	18.046	1.430			
Online learning and skills development	pre	5.417	1.068	−150.408	0.000	0.918
	post	18.046	1.4317			
Online learning and learning attitudes	pre	7.362	1.050	−185.104	0.000	0.901
	post	16.691	0.953			

4.3. Comparing Male and Female Students' Cyber-Hygiene Behaviours and Attitude toward Online Learning Post QEA Adoption

A comparison was conducted between male and female students in relation to cyber-hygiene behaviour post the adoption of QEA. The results of the independent sample t-test showed a statistically significant difference between male and female students in relation to cyber-hygiene behaviours ($p < 0.001$) post the adoption of QEA (Table 8). The effect size was very large between male and female students, as confirmed by eta squared above 0.90. These results confirm that female students reported positive cyber-hygiene behaviours than male students.

It was also examined whether there are gender differences in relation to attitudes toward online learning post the adoption of QEA. The results of the independent sample t-test showed statistically significant differences between male and female students in relation to attitudes toward online learning ($p < 0.001$) post the adoption of QEA (see Table 9). The effect size was very large between male and female students, as confirmed by eta squared above 0.90. These results confirm that female students reported a more positive attitude toward online learning than male students.

Table 8. Independent sample *t*-test for cyber-hygiene behaviours.

Cyber-Hygiene Behaviours	Gender	M	SD	*t*	*p*	η^2
Mobile security	female	7.00	0.000	−10.785	0.000	0.931
	male	7.69	0.952			
Passwords	female	10.12	0.666	−116.811	0.000	0.914
	male	13.70	0.586			
Email phishing	female	10.00	0.695	−79.618	0.000	0.913
	male	13.32	1.350			
Sensitive/non-sensitive	female	6.70	0.458	−44.017	0.000	0.947
	male	8.62	1.246			
Social networks	female	10.06	0.659	−105.073	0.000	0.932
	male	13.97	0.663			
Move with a device	female	10.41	0.493	−92.675	0.000	0.989
	male	13.38	0.487			
General protection	female	13.69	1.020	−79.551	0.000	0.907
	male	18.19	0.864			

Table 9. Independent sample *t*-test for attitudes toward online learning.

Attitude Toward Online Learning	Gender	N	M	SD	*t*	*p*	η^2
Online learning and knowledge development	Female	244	17.033	1.428	32.207	0.000	0.932
	Male	202	13.652	0.479			
Online learning and skills development	Female	244	18.034	1.428	29.995	0.000	0.989
	Male	202	13.952	1.436			
Online learning and learning attitudes	Female	244	17.691	0.952	69.967	0.000	0.907
	Male	202	13.000	0.000			

5. Discussion

This research developed and examined a quadruple "E" approach (QEA) for enhancing cyber-hygiene behaviour and attitudes toward online learning amid the COVID-19 pandemic among students in KSA universities. The QEA approach included four steps. Step 1 is the education (E1) of students about cyber-hygiene to enhance their knowledge, skills, and overall competencies. Step 2 is the exploration (E2) of self-diagnosis form to learn individually. Step 3 is the execution (E3) of activities based on their learning from Stages 1 and 2. Step 4 is the evaluation (E4) of students' behaviours of cyber-hygiene security and attitudes toward online learning post the adoption of the model. Students' behaviours of cyber-hygiene security and attitudes toward online learning were examined pre the adoption of the model. A comparison of students' cyber-hygiene security and attitudes toward online learning was conducted pre- and post-QEA on a sample of 446 undergraduate students at four public universities in KSA.

The literature [6,28,61] showed that cyber-hygiene awareness of higher-education students in KSA was a major challenge for both educators and higher-education administrators. Hence, there was a need for a best-practice model to enhance students' cyber-hygiene behaviour and create a positive attitude toward online learning. The QEA was developed for this purpose. The results showed positive cyber-hygiene behaviour after the implementation of QEA compared to pre-QEA adoption. Students showed more positive cyber-hygiene behaviour after they trained with the QEA. The QEA raised students' consciousness regarding cyber-hygiene security and created positive cyber-hygiene behaviours. The results obtained with the cyber-hygiene behaviours assessment scales reveal female students have more positive behaviours than their male colleagues do. Female students in higher education in KSA tend to show more positive attitudes and behaviour toward online learning than their male colleagues because they were less likely to have face-to-face learning pre-COVID-19 pandemic [15]. Additionally, these results can be explained by females embracing the QEA model bringing additional consciousness regarding cyber-hygiene security. In addition, this result suggests that male students are less aware of

applying cyber-hygiene best practices, making them the most likely cyber victims. Thus, the results indicate the need to boost additional cyber-hygiene awareness actions for male students [29,34,62]. As highlighted earlier, female students in KSA universities are segregated and do not have direct contact with their male lecturers [15,63]. Hence, they have fewer options to study face-to-face; thus, they already have more experience with online learning. They tend to use digital platforms to contact them even before the COVID-19 pandemic. Thus, they have a more positive attitude toward online learning than male students [2,16,64].

Another challenge for higher-education institutions amid COVID-19 was the insurance of positive attitudes toward online learning among students since many students were exposed to cyber-attacks amid the COVID-19 era. According to Alharbi [65] and Alzahrani [31], several students exposed to cyber deception amid the COVID-19 pandemic had a highly negative attitude toward using technology in learning. Moreover, Mator [34] showed that the awareness of cyber-hygiene habits had reduced several students' exposure to cyber-attacks and made them have positive attitudes toward using technology in learning. This means that the cyber victims were not too knowledgeable of the issue's essence, represented by the lack of cyber-hygiene awareness. Hence, the current research developed the QEA to enhance students' cyber-hygiene behaviour to ensure an effective attitude toward online learning. The results confirmed that students of both genders showed more positive attitudes toward online learning post-QEA adoption compared to pre-QEA adoption. The size of the difference between pre- and post-QEA adoption was very large. These results can be explained by the adoption of the QEA, which influences attitudes toward online learning, and this is in line with earlier studies [32,66,67]. Female students reported more positive attitudes toward online learning post-QEA adoption than male students. This could be because they were already more familiar with online learning than their male colleagues pre-COVID-19 pandemic [59]. Hence, the adoption of QEA has spread more positive attitudes toward online learning among female students than male ones.

The results of the current research have implications for scholars and educators in the higher-education context, especially in relation to the sustainability of higher education. In order to ensure positive cyber-hygiene behaviour and attitude toward online learning in higher-education, educators in universities should promote the dissemination of cyber-hygiene awareness. This could be achieved by using the suggested QEA, which could be considered an essential instrument to encourage good cyber-hygiene habits and practices. Educators should ensure that their students have high cyber-hygiene awareness before engaging them in online learning to stimulate positive cyber-hygiene behaviour and attitude toward online learning among higher-education students in KSA and other similar country contexts. The results of the study contribute to the sustainability of high education, particularly Sustainable Development Goal (SDG) 4 in relation to quality education and SDG 10 in relation to reduced inequalities between males and females in a gender-segregated culture such as KSA. The results of the research support educators in higher education to ensure positive cyber-hygiene behaviour and attitudes toward online learning.

6. Conclusions

The COVID-19 pandemic forced universities to shift traditional education to the online world in order to control the spread of the virus. However, students were affected by cyber threats and attacks during this almost-new experience of online learning, which has had negative impacts on their attitudes toward online learning. The current research is a response to several calls by researchers and educators to find a proper approach to enhancing cybersecurity behaviours and ensure positive attitudes toward online learning among university students, especially amid COVID-19. More specifically, the current research developed an integrated cyber-hygiene model for improving this behaviour that was entitled the quadruple "E" approach (QEA), which includes four stages: educate (E1), explore (E2), execute (E3), and evaluate (E4). Using a sample of 446 bachelor students in four public KSA universities, the research compared cybersecurity behaviours and

attitudes toward online learning among student pre- and post-QEA adoption. The results of this research showed statistically significant differences in students' cyber-hygiene behaviour and attitudes toward online learning pre- and post-adoption of the QEA. In more detail, students showed more positive cyber-hygiene behaviour and attitudes toward online learning post-QEA adoption than pre-QEA implementation. Furthermore, the results confirmed that female students have more positive behaviour and attitudes toward online leaning than their male counterparts post the adoption of QEA. The results of this research stimulate positive cyber-hygiene behaviour and enhance attitudes toward online learning in universities, which have implications for the sustainability of online leaning KSA higher education.

7. Limitation and Future Works

The current article includes some limitations that could be handled in future research. The research adopted a self-reporting survey to examine students' cyber-hygiene behaviour and attitude toward online learning pre- and then post-QEA adoption. The results have great value for higher0education institutions in KSA; however, they have some limitations for generalisation to other countries' contexts without further testing. Future research opportunities could examine the relationship between cybersecurity, cyber hygiene, and the sustainability of online learning in higher education post the COVID-19 pandemic. Furthermore, several mediating and moderating variables, such as experience, competencies, skills, and others could be combined in future research. A comparison between students at different levels (e.g., Level 1 vs. Level 8) could also be conducted in future work. The results of current research could be examined in other countries context.

Supplementary Materials: The supporting information about the quadruple "E" approach can be downloaded at https://2u.pw/sae5f8.

Author Contributions: Conceptualisation, M.A.S. and A.E.E.S.; methodology, M.A.S. and A.E.E.S.; software, M.A.S.; validation, M.A.S. and A.E.E.S.; formal analysis, M.A.S. investigation, M.A.S. and A.E.E.S.; resources, M.A.S. and A.E.E.S.; data curation, M.A.S.; writing—original draft preparation, M.A.S. and A.E.E.S.; writing—review and editing, M.A.S. and A.E.E.S.; visualisation, M.A.S. and A.E.E.S.; supervision, M.A.S. and A.E.E.S.; project administration, M.A.S. and A.E.E.S.; funding acquisition, M.A.S. and A.E.E.S. All authors have read and agreed to the published version of the manuscript.

Funding: The authors extend their appreciation to the Deputyship for Research and Innovation, Ministry of Education in Saudi Arabia, for funding this research work (INST204).

Institutional Review Board Statement: The study was conducted according to the guidelines of the Declaration of Helsinki and approved by the Deanship of Scientific Research Ethical Committee, King Faisal University (project number: INST204; date of approval: 1 November 2021).

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

Data Availability Statement: The data presented in this study are available upon request from the corresponding author. The data are not publicly available, due to privacy concerns.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Salem, M.A.; Alsyed, W.H.; Elshaer, I.A. Before and Amid COVID-19 Pandemic, Self-Perception of Digital Skills in Saudi Arabia Higher Education: A Longitudinal Study. *Int. J. Environ. Res. Public Health* **2022**, *19*, 9886. [CrossRef] [PubMed]
2. Salem, M.A.; Sobaih, A.E.E. ADIDAS: An Examined Approach for Enhancing Cognitive Load and Attitudes towards Synchronous Digital Learning Amid and Post COVID-19 Pandemic. *Int. J. Environ. Res. Public Health* **2022**, *19*, 16972. [CrossRef]
3. Alkinani, E.A. Saudi arabian undergraduate students'perceptions of e-learning quality during COVID-19 pandemic. *Int. J. Comput. Sci. Netw. Secur.* **2021**, *21*, 66–76.
4. Alqahtani, A.Y.; Rajkhan, A.A. E-learning critical success factors during the covid-19 pandemic: A comprehensive analysis of e-learning managerial perspectives. *Educ. Sci.* **2020**, *10*, 216. [CrossRef]
5. Alzubaidi, A. Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon* **2021**, *7*, e06016. [CrossRef]

6. Alharbi, T.; Tassaddiq, A. Assessment of cybersecurity awareness among students of Majmaah University. *Big Data Cogn. Comput.* **2021**, *5*, 23. [CrossRef]
7. Bhosale, S.S.; Patil, R.; Lingayat, G.R. E-Learning Using the Chalkboard System in Light of The Quality of Education and Cyber Security. *Int. J. Curr. Eng. Technol.* **2019**, *9*, 49–54.
8. Vishwanath, A. *The Weakest Link: How to Diagnose, Detect, and Defend Users from Phishing*; MIT Press: Cambridge, MA, USA, 2022.
9. Maennel, K.; Mäses, S.; Maennel, O. Cyber hygiene: The big picture. In Proceedings of the Nordic Conference on Secure IT Systems, Oslo, Norway, 28–30 November 2018; pp. 291–305.
10. Howell, C.J. *Self-Protection in Cyberspace: Assessing the Processual Relationship between Thoughtfully Reflective Decision Making, Protection Motivation Theory, Cyber Hygiene, and Victimization*; University of South Florida: Tampa, FL, USA, 2021.
11. Burlakov, V.V.; Skubriy, E.V.; Orlova, L.N.; Fedotova, G.V.; Sukhinin, A.V. Cyber Security in the Era of COVID-19: Threats to Digital Platforms Stability and Cyber Hygiene Rules. In *Socio-Economic Systems: Paradigms for the Future*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 1565–1574.
12. Butler Lamar, S. Managing cyber hygiene at a higher education institution in the united states. In Proceedings of the SAIS, Stockholm, Sweden, 13–14 June 2022.
13. Baraković, S.; Baraković Husić, J. Cyber hygiene knowledge, awareness, and behavioral practices of university students. *Inf. Secur. J. A Glob. Perspect.* **2022**, 1–24. [CrossRef]
14. Cain, A.A.; Edwards, M.E.; Still, J.D. An exploratory study of cyber hygiene behaviors and knowledge. *J. Inf. Secur. Appl.* **2018**, *42*, 36–45. [CrossRef]
15. Alyahya, M.A.; Elshaer, I.A.; Abunasser, F.; Hassan, O.H.M.; Sobaih, A.E.E. E-learning experience in higher education amid covid-19: Does gender really matter in a gender-segregated culture? *Sustainability* **2022**, *14*, 3298. [CrossRef]
16. Sobaih, A.E.E.; Hasanein, A.; Elshaer, I.A. Higher Education in and after COVID-19: The Impact of Using Social Network Applications for E-Learning on Students' Academic Performance. *Sustainability* **2022**, *14*, 5195. [CrossRef]
17. Hakim, B. Technology integrated online classrooms and the challenges faced by the EFL teachers in Saudi Arabia during the COVID-19 pandemic. *Int. J. Appl. Linguist. Engl. Lit.* **2020**, *9*, 33–39. [CrossRef]
18. Almrezeq, N.J. Exploratory study to measure awareness of cybercrime in Saudi Arabia. *Turk. J. Comput. Math. Educ.* **2021**, *12*, 2992–2999.
19. Wang, C.X. CAFE: An instructional design model to assist K-12 teachers to teach remotely during and beyond the COVID-19 pandemic. *TechTrends* **2021**, *65*, 8–16. [CrossRef]
20. Toquero, C.M. Challenges and opportunities for higher education amid the COVID-19 pandemic: The Philippine context. *Pedagog. Res.* **2020**, *5*, em0063. [CrossRef] [PubMed]
21. Li, Y.; Liu, Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Rep.* **2021**, *7*, 8176–8186. [CrossRef]
22. Rathod, D.G. Review on Cyber Attacks in India. In Proceedings of the 1st International Conference on Advanced Information Technology and Communication (IC-AITC), Kota Bandar Lampung, Indonesia, 3–4 September 2021.
23. Alsaadi, F.M. Predicting Computer Self-Efficacy of E-Learning Systems Security Attacks using Confirmatory factor Analysis. *Int. J. Innovat. Creativ. Change* **2022**, *16*, 271–276.
24. Kalhoro, S.; Rehman, M.; Ponnusamy, V.; Shaikh, F.B. Extracting key factors of cyber hygiene behaviour among software engineers: A systematic literature review. *IEEE Access* **2021**, *9*, 99339–99363. [CrossRef]
25. Wilner, A.S.; Luce, H.; Ouellet, E.; Williams, O.; Costa, N. From public health to cyber hygiene: Cybersecurity and Canada's healthcare sector. *Int. J.* **2021**, *76*, 522–543. [CrossRef]
26. Kavitha, A.; Rao, B.S.; Akhtar, N.; Rafi, S.M.; Singh, P.; Das, S.; Manikandan, G. A Novel Algorithm to Secure Data in New Generation Health Care System from Cyber Attacks Using IoT. *Int. J. Electr. Electron. Res.* **2022**, *10*, 270–275. [CrossRef]
27. Mirza, M.N.; Akram, M.S. 3-Cs of Cyberspace and Pakistan: Cyber Crime, Cyber Terrorism and Cyber Warfare. *Strateg. Stud.* **2022**, *42*, 62–80. [CrossRef]
28. Al Mamun, A.; Ibrahim, J.B.; Mostofa, S.M. Cyber Security Awareness in Bangladesh: An Overview of Challenges and Strategies. *Int. J. Comp. Sci. Informat. Technol. Res.* **2021**, *9*, 88–94.
29. Isa, M.Y.B.M.; Ibrahim, W.N.B.W.; Mohamed, Z. The Relationship Between Financial Literacy and Public Awareness on Combating the Threat of Cybercrime in Malaysia. *J. Ind. Distrib. Bus.* **2021**, *12*, 1–10.
30. Alotaibi, F.; Furnell, S.; Stengel, I.; Papadaki, M. A review of using gaming technology for cyber-security awareness. *Int. J. Inf. Secur. Res. IJISR* **2016**, *6*, 660–666. [CrossRef]
31. Alzahrani, L. Statistical Analysis of Cybersecurity Awareness Issues in Higher Education Institutes. *Int. J. Adv. Comput. Sci. Appl.* **2021**, *12*, 630–637. [CrossRef]
32. Alsulami, M.H.; Alharbi, F.D.; Almutairi, H.M.; Almutairi, B.S.; Alotaibi, M.M.; Alanzi, M.E.; Alotaibi, K.G.; Alharthi, S.S. Measuring Awareness of Social Engineering in the Educational Sector in the Kingdom of Saudi Arabia. *Information* **2021**, *12*, 208. [CrossRef]
33. Kumar, N.; Jain, S.; Shukla, M.; Lodha, S. Investigating Users' Perception, Security Awareness and Cyber-Hygiene Behaviour Concerning QR Code as an Attack Vector. In Proceedings of the International Conference on Human-Computer Interaction, Virtual Event, 26 June–1 July 2022; pp. 506–513.

34. Mator, J.D.; Still, J.D. Impact of the Cyber Hygiene Intelligence and Performance (CHIP) Interface on Cyber Situation Awareness and Cyber Hygiene. In Proceedings of the International Conference on Human-Computer Interaction, Virtual Event, 24–29 July 2021; pp. 298–309.
35. Saleous, H.; Ismail, M.; AlDaajeh, S.H.; Madathil, N.; Alrabaee, S.; Choo, K.-K.R.; Al-Qirim, N. COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities. *Digit. Commun. Netw.* **2022**, *9*, 211–222. [CrossRef]
36. Yegen, C.; Kirik, A.M.; Çetinkaya, A. Sustainability, Digital Security, and Cyber Hygiene During the Covid-19 Pandemic. In *New Normal in Digital Enterprises: Strategies for Sustainable Development*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 91–105.
37. Eboibi, F.E. Cybercriminals and Coronavirus cybercrimes in Nigeria, the United States of America and the United Kingdom: Cyber hygiene and preventive enforcement measures. *Commonw. Law Bull.* **2021**, *47*, 113–142. [CrossRef]
38. Ugwu, C.; Ani, C.; Ezema, M.; Asogwa, C.; Ome, U.; Obayi, A.; Ebem, D.; Olebara, C.; Ukwandu, E. Towards Determining the Effect of Age and Educational Level on Cyber-Hygiene. In Proceedings of the 2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development (NIGERCON), Lagos, Nigeria, 5–7 April 2022; pp. 1–5.
39. Indolfi, G.; Malik, F.; Giometto, S.; Chou, R.; Easterbrook, P.; Lucenteforte, E. The efficacy and safety of direct-acting antivirals among children and adolescents with chronic hepatitis C virus infection: Systematic review with meta-analysis. In *Treatment of Adolescents and Children With Chronic Hcv Infection, And Hcv Simplified Service Delivery And Diagnostics*; WHO: Geneva, Swtizerland, 2022; Volume 4.
40. Ebad, S.A. What topics should or should not be included in software security education—Qualitative content analysis. *Comput. Appl. Eng. Educ.* **2022**, *30*, 1753–1773. [CrossRef]
41. Meland, P.H.; Bernsmed, K.; Wille, E.; Rødseth, Ø.J.; Nesheim, D.A. A retrospective analysis of maritime cyber security incidents. *Int. J. Mar. Navig. Saf. Sea Transp.* **2021**, *15*, 519–530. [CrossRef]
42. Donalds, C.; Barclay, C.; Osei-Bryson, K.-M. *Cybercrime and Cybersecurity in the Global South: Concepts, Strategies and Frameworks for Greater Resilience*; Routledge: Abingdon, UK, 2022.
43. Antunes, M.; Silva, C.; Marques, F. An Integrated Cybernetic Awareness Strategy to Assess Cybersecurity Attitudes and Behaviours in School Context. *Appl. Sci.* **2021**, *11*, 11269. [CrossRef]
44. Tick, A.; Cranfield, D.J.; Venter, I.M.; Renaud, K.V.; Blignaut, R.J. Comparing three countries' higher education students' cyber related perceptions and behaviours during COVID-19. *Electronics* **2021**, *10*, 2865. [CrossRef]
45. Ali, R.; Zafar, H. A security and privacy framework for e-Learning. *Fac. Publ.* **2017**, 4137. Available online: https://digitalcommons.kennesaw.edu/facpubs/4137 (accessed on 1 February 2023). [CrossRef]
46. Syed, S.; Rastogi, A.; Bansal, A.; Kumar, A.; Jindal, A.; Prakash, A.; Agarwal, G.; Varshney, M. Future of e-learning in medical education—Perception, readiness, and challenges in a developing country. In Proceedings of the Frontiers in Education, Lincoln, NE, USA, 13–16 October 2021; p. 598309.
47. Pătrașcu, P. Promoting cybersecurity culture through education. In Proceedings of the Conference eLearning and Software for Education (eLSE), Bucharest, Romania, 27–28 April 2023; pp. 273–279.
48. George, J.; Emmanuel, A. Cyber hygiene in health care data breaches. In *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications*; IGI Global: Hershey, PA, USA, 2020; pp. 1309–1321.
49. Panda, S.; Panaousis, E.; Loukas, G.; Laoudias, C. Optimizing investments in cyber hygiene for protecting healthcare users. In *From Lambda Calculus to Cybersecurity Through Program Analysis*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 268–291.
50. Almomani, I.; Ahmed, M.; Maglaras, L. Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia. *PeerJ Comput. Sci.* **2021**, *7*, e703. [CrossRef] [PubMed]
51. Brun, L.; Bellanova, R. *The Role of the European Union Agency for Network and Information Security (ENISA) in the Governance Strategies of European Cybersecurity*; Université Catholique de Louvain: Ottignies-Louvain-la-Neuve, Belgium, 2018.
52. Wadsworth, B.J. *Piaget's Theory of Cognitive and Affective Development: Foundations of Constructivism*; Longman Publishing: London, UK, 1996.
53. Skinner, B.F. *The Behavior of Organisms: An Experimental Analysis*; BF Skinner Foundation: Cambridge, MA, USA, 2019.
54. Hong, J.-C.; Lee, Y.-F.; Ye, J.-H. Procrastination predicts online self-regulated learning and online learning ineffectiveness during the coronavirus lockdown. *Personal. Individ. Differ.* **2021**, *174*, 110673. [CrossRef]
55. Vishwanath, A.; Neo, L.S.; Goh, P.; Lee, S.; Khader, M.; Ong, G.; Chin, J. Cyber hygiene: The concept, its measure, and its initial tests. *Decis. Support Syst.* **2020**, *128*, 113160. [CrossRef]
56. Afify, M.K. Effect of interactive video length within e-learning environments on cognitive load, cognitive achievement and retention of learning. *Turk. Online J. Distance Educ.* **2020**, *21*, 68–89. [CrossRef]
57. Ali, W. Online and remote learning in higher education institutes: A necessity in light of COVID-19 pandemic. *High. Educ. Stud.* **2020**, *10*, 16–25. [CrossRef]
58. Hayashi, R.; Garcia, M.; Maddawin, A. *Online Learning in Sri Lanka's Higher Education Institutions during the COVID-19 Pandemic*; Asian Development Bank: Mandaluyong, Philippines, 2020.
59. Buss, A.H.; Perry, M. The aggression questionnaire. *J. Personal. Soc. Psychol.* **1992**, *63*, 452. [CrossRef]
60. Hinton, P.R.; Brownlow, C.; McMurray, I. *SPSS Explained*; Psychology Press: Abingdon, UK, 2004.
61. Aljumah, Y.; Ahmed, S.S. A Novel Approach to Get Awareness in Saudi Arabia Regarding Phishing Attacks. In Proceedings of the 2021 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), Kuala Lumpur, Malaysia, 12–13 June 2021; pp. 1–5.

62. Lin, P.-Y.; Chai, C.S.; Jong, M.S.-Y. A PISA-2015 comparative meta-analysis between Singapore and Finland: Relations of students' interest in science, perceived ICT competence, and environmental awareness and optimism. *Int. J. Environ. Res. Public Health* **2019**, *16*, 5157. [CrossRef]
63. Alenezi, A.M.; Salem, M.A. Implementation of smartphones, tablets and their applications in the educational process management at Northern Border University. *Int. J. Educ. Sci.* **2017**, *18*, 56–64.
64. Salem, M.A.; Elshaer, I.A. Educators' Utilizing One-Stop Mobile Learning Approach amid Global Health Emergencies: Do Technology Acceptance Determinants Matter? *Electronics* **2023**, *12*, 441. [CrossRef]
65. Al-Ahdal, A.A.M.H.; Alharbi, M.A. MALL in collaborative learning as a vocabulary-enhancing tool for EFL learners: A study across two Universities in Saudi Arabia. *Sage Open* **2021**, *11*, 2158244021999062. [CrossRef]
66. Sarrab, M.; Al-Shihi, H.; Khan, A.I. An empirical analysis of mobile learning (m-learning) awareness and acceptance in higher education. In Proceedings of the 2015 International Conference on Computing and Network Communications (CoCoNet), Trivandrum, India, 16–19 December 2015; pp. 960–963.
67. Mohamad, S.A.; Kassim, S. Examining the relationship between UTAUT construct, technology awareness, financial cost and E-payment adoption among microfinance clients in Malaysia. In Proceedings of the 1st Aceh Global Conference (AGC 2018), Banda Aceh, Indonesia, 17–18 October 2018; pp. 351–357.