electronics

MDPI

Article

Comparing Three Countries' Higher Education Students' Cyber Related Perceptions and Behaviours during COVID-19

Andrea Tick [1,*], Desireé J. Cranfield [2], Isabella M. Venter [3], Karen V. Renaud [4,*] and Rénette J. Blignaut [5]

1 Institute of Management and Quantitative Methods, Óbuda University, 1034 Budapest, Hungary
2 School of Management, Swansea University, Swansea SA1 8EN, UK; d.j.cranfield@swansea.ac.uk
3 Department of Computer Science, University of the Western Cape, Bellville 7535, South Africa; iventer@uwc.ac.za
4 Computer and Information Sciences, University of Strathclyde, Glasgow G1 1XQ, UK
5 Department of Statistics and Population Studies, University of the Western Cape, Bellville 7535, South Africa; rblignaut@uwc.ac.za
* Correspondence: Tick.Andrea@uni-obuda.hu (A.T.); karen.renaud@strath.ac.uk (K.V.R.)

Abstract: In 2020, a global pandemic led to lockdowns, and subsequent social and business restrictions. These required overnight implementation of emergency measures to permit continued functioning of vital industries. Digital technologies and platforms made this switch feasible, but it also introduced several cyber related vulnerabilities, which students might not have known how to mitigate. For this study, the Global Cyber Security Index and the Cyber Risk literacy and education index were used to provide a cyber security context for each country. This research project—an international, cross-university, comparative, quantitative project—aimed to explore the risk attitudes and concerns, as well as protective behaviours adopted by, students at a South African, a Welsh and a Hungarian University, during the pandemic. This study's findings align with the relative rankings of the Oliver Wyman Risk Literacy and Education Index for the countries in which the universities reside. This study revealed significant differences between the student behaviours of students within these universities. The most important differences were identified between students' risk attitudes and concerns. It was also discovered that South African students reported having changed their protective online behaviours to the greatest extent, since the pandemic commenced. Recommendations are made suggesting that cyber security training and education, as well as improving the digital trust and confidence in digital platforms, are critical.

Keywords: COVID-19 pandemic; higher education; cyber related risk perceptions; protective behaviours

Citation: 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. https://doi.org/10.3390/electronics10222865

Academic Editor: Christos J. Bouras

Received: 29 October 2021
Accepted: 18 November 2021
Published: 20 November 2021

1. Introduction

In 2020/2021, the World Health Organisation (WHO) declared a global pandemic, and many countries instituted unprecedented measures to contain the spread of the virus, restricting social interactions, closing non-critical businesses, and requiring remote working. This forced universities to switch to exclusive use of remote educational platforms, not necessarily designed for universities: "While these platforms allowed institutions to fill an urgent need, they caused novel and well-publicized security and privacy problems" [1] (p. 653).

As a consequence, remote learning, working and socialising became the new normal. Reliance on digital technologies grew exponentially, impacting health service delivery, the economy, and the higher education community [2]. A heavy reliance on personal digital technologies led to a greater vulnerability in the cyber domain [2]. Mee, Brandenburg and Lin [3] (p. 4) suggest that "cyber security and the management of cyber risk by individuals, already a major issue before the COVID-19 pandemic, has become much more pressing overnight as enterprises around the world experiment with work from

home arrangements". Lallie et al. [4] discovered that 86% of the cyber-attacks globally during COVID-19 involved phishing and smishing. They also found that COVID-19 related malware was the second largest attack vector, appearing in 65% of cases. A recent study that considered the period from the 31 December 2019–14 April 2020, suggests that a 51% increase in cyber-attacks occurred during the pandemic, with 30,000 of these being COVID-19 related cyber-attacks [5]. Of these, 17% were globally directed, with 14% specifically directed at the UK, 14% at the USA, and 25% at China, with 30% being directed at other countries such as Japan, Singapore, Italy, Spain, etc. (see Figure 1) [4]. Hence, by April 2020, most cyber-attacks targeted the whole world, specifically focusing on tax rebates due to COVID-19 or contact tracing phishing messages [4].

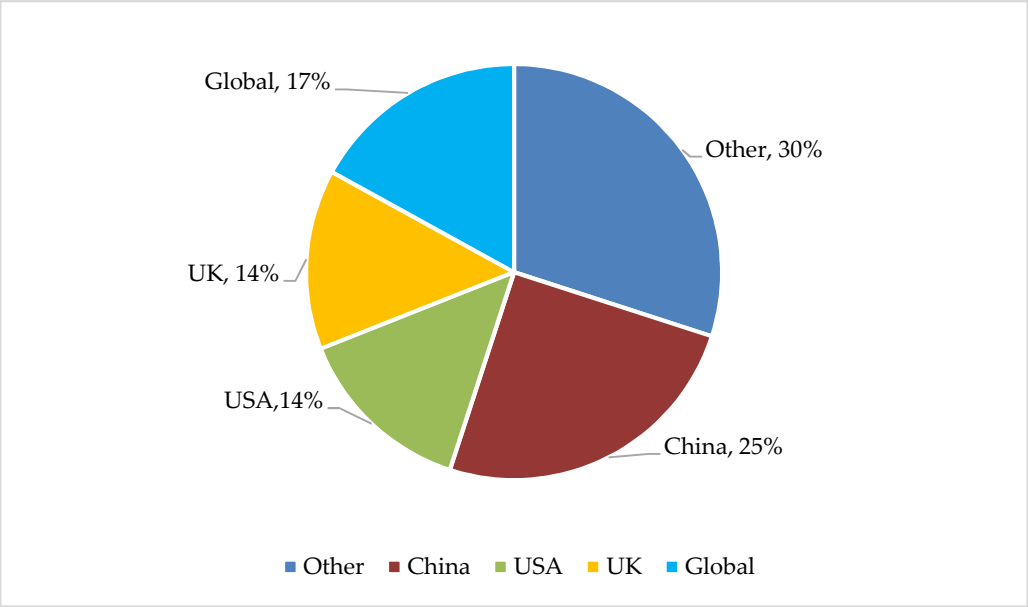

Figure 1. Cyber-attack distribution across countries considered.

This study involved students from a university in each of three countries: United Kingdom (Wales), South Africa, and Hungary. All experienced lockdowns. In the United Kingdom (UK), the first lockdown ordered people to 'stay at home', with the legal lockdown measures coming into force on the 26 March 2020. In South Africa, the first lockdown measures also came into effect on the 26 March 2020, and Hungary commenced lockdown on the 28 March 2020. Virtual learning replaced face-to-face delivery at all educational levels [6]. Usually, such a switch to virtual delivery would be instituted with a great deal of preparation and after a period of reflection [7]. However, the lockdowns necessitated a sudden switch, and neither educators nor students were prepared for this seismic shift.

2. Background

The core online risk terms used in this paper are defined in Sections 2.1 and 2.2 the country differences are discussed to provide the necessary conceptual and contextual background for this paper.

2.1. Cyber Terms

To inform the subsequent discussion, rigorous definitions of all the key cyber related terms used in this paper from the research literature are now provided.

Craigen, Diakun-Thibault, and Purse [8] (p. 1) define cyber security as: "the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights". This definition makes it clear that cyber security applies to the protection of information and devices, specifically the confidentiality, integrity and availability thereof [9].

It does not apply specifically to the protection of the humans using such devices. Their wellbeing is related to cyber safety, as defined next.

Byron [10] suggests that online harms, which are related to Grey's [11] definition of cyber safety, can be categorised into one of the three C's: content, conduct and contact. Grey explains that cyber safety is thus related to upsetting information (content), responsible use of information and communication technologies (conduct), and safeguarding against individuals who contact others with ill intentions (contact).

Brandeis and Warren [12] was one of the first publications to attempt to delineate privacy. They refer to privacy as "the right to be left alone". Westin [13] (p. 7) defines privacy as "the claim of individuals, groups or institutions to determine when, how and to what extent information about them is communicated to others". This more nuanced definition resonates with individuals having a sense of control over their own information, whereas Brandeis and Warren's perspective, while still eliciting an intuitive sense of privacy, also seems to be closer to cyber safety's "contact" dimension in the physical domain, than being related to information privacy, which is a concern in the cyber realm. Hence, Westin's conceptualisation is equally relevant in the cyber era as it was in 1968, and it shall be used to delineate privacy in this research study.

All these cyber terms are related to risk management. If people do not perceive these risks to be significant, they are unlikely to act to mitigate them. Pidgeon et al. [14] (p. 89) suggest that risk perception can be defined as "people's beliefs, attitudes, judgments and feelings, as well as the wider social or cultural values and dispositions that people adopt, towards hazards and their benefits".

Risk perceptions lead to protective behaviours. The kinds of behaviours people can engage in are related to [15,16]: (1) starting to use protective measures or using security tools (e.g., using a VPN), (2) desisting from unwise behaviours (e.g., choosing weak passwords), or (3) proactively looking out for possible attacks (e.g., not clicking on a Phishing message, which could compromise accounts).

Figure 2 depicts the core aspects of these four key concepts, and the protective behaviours they lead to, which is relied on for the rest of this paper.

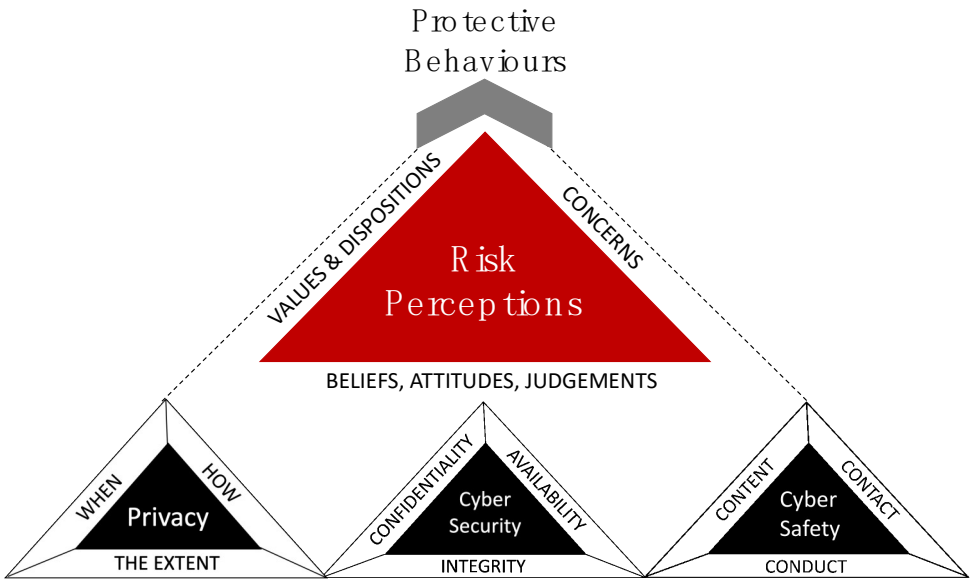

Figure 2. Key risk management cyber related concepts.

2.2. Country Differences

The universities in each of the countries are not homogenous entities, being heterogenous in nature. Students studying at each of these universities come from diverse cultures, backgrounds and countries. Yet, as groups of residential students, they were equally impacted by the way their specific country supported their higher education institutions and

the participating students during the transition to online learning, and all along its duration. As such, it is important to describe the context for each country's cyber environment, given our focus on cyber related risks.

The following published country cyber indices are relevant: The Global Cyber Security Index (GCI)—launched in 2015 by the International Telecommunication Union (ITU)—is based on a complex set of indicators to monitor the level of cyber security commitment of 150 participating countries (according to five pillars); Another framework is the Oliver Wyman Forum's Cyber Risk Literacy and Education Index—this framework measures literacy at the population level and thus allows countries to discover best global practices and to focus their attention and investments on areas of weakness. The aim is to keep the risky online world—an increasingly digitized and interconnected space—properly secured from fast paced embryonic cyber risks [3].

The Wyman Index is based on five key drivers and nine related pillars. For all the five drivers in Figure 3 it should be noted that the UK outperforms Hungary and South Africa.

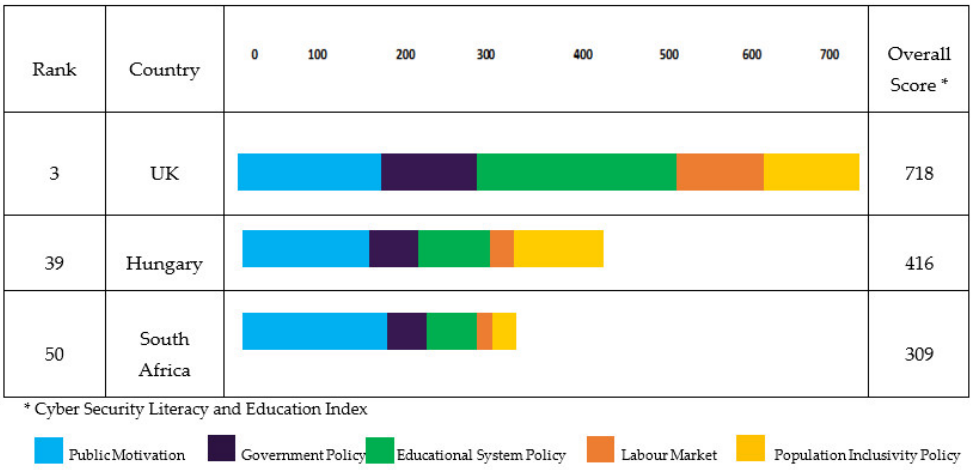

Figure 3. Wyman's Cyber Security and Education Index-comparison of Hungary, South Africa and United Kingdom [3].

The five drivers represent items that measure trends or changes in each country's average cyber literacy level. Public motivation—measures the population's commitment to practicing cyber security, with metrics for adherence to safe cyber practices, Government policy—evaluates government policies to enhance the cyber risk literacy and education, with metrics for the geography's national cyber security strategy, Educational system—measures whether cyber risk instruction is encouraged or mandated, with metrics to assess primary and secondary school curricula, assessing formal education, and labour upskilling, Labour Market—measures the employers demand for cyber-security literacy skills, with metrics for the increase in cyber security related roles and the number of cyber security start-ups, and Population inclusivity—measures equitable access to digital technologies and formal education in a geography, with Internet access and school completion rate metrics [3,17].

For each driver in the Wyman Index, relevant pillars, contributing to the measure and ranking of that driver, is given. Figure 4 depicts the three countries considered in this study, in terms of five of the Wyman Index pillars related to higher education: Cyber risk awareness and motivation (Public Motivation), Formal education (Educational System), Skill demand from employer expectations (Labour Market), Technological inclusivity and educational inclusivity (Population Inclusivity).

It is worth noting that the Cyber Risk Literacy and Education Index rankings includes countries that are considered developed or "*are economically influential enough for cyber risk literacy to be a topic relevant for their populations*" [17] (p. 12). A lower score does not imply that a country's population is not ready to understand cyber related risks, but rather that

other challenges, such as developing infrastructure or investment in basic digital education and rolling out ubiquitous Internet access, might be a higher priority [17].

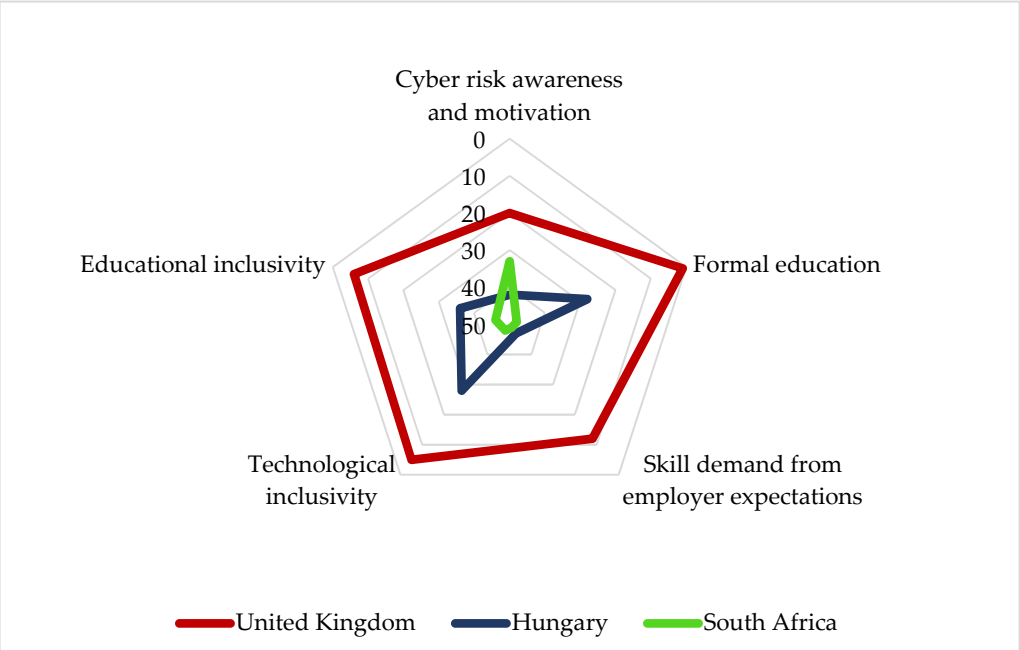

Figure 4. Cyber Security Risk Literacy and Education Index ranking, with the relevant pillars, adopted from Wyman Forum [17].

During the COVID-19 pandemic, several research studies were conducted and continues to be conducted around the impact of COVID-19 on society [6,7,18,19]. To the best of our knowledge, comparative research on countries with such vastly different economic and social backgrounds is limited. Some noteworthy studies are worth mentioning: Two researchers carried out a comparative study on cyber security awareness on smartphone usage in Hungary and Vietnam [20]; Zwilling et al. [21] conducted a comparative research study of four countries—Israel, Slovenia, Poland and Turkey—with different economic, educational and cultural backgrounds; A comparative research study between the countries of the Middle East and North Africa (MENA) was conducted by Mawgoud et al., focuses its attention on this region and highlights its high volatility and vulnerability to cyber threats and attacks [22]; A study by Lesjak et al. compared student cyber security awareness between Israelis and Slovenians and found significant differences in levels of cyber security awareness which called for enhanced cyber education practices [23].

The three participating universities are situated within three countries, which offer a rich opportunity for comparison–one being ranked high, one at the bottom and one in-between: Wales (the UK) is the 3rd country in the Oliver Wyman index, indicating a high population level cyber risk literacy and education. South Africa is 50th on the list, while Hungary is 39th. With respect to the educational system's contribution to the countries' overall score, the UK is 2nd, Hungary 35th and South Africa 44th. Based on these published literacy levels, we could expect to see the highest levels of risk perception and changed behaviour during COVID-19 in the Welsh University students, the least from the South African students and the Hungarian students somewhere in-between.

In comparing the risk perceptions and cyber related behaviours of the three countries' students, the focus is on: (1) their online risk perceptions (their attitude and concerns towards online risks), and (2) risk management behaviours (which protective behaviours they engage in). Within 'risk perception', attitudes and concerns were considered to be influenced by each country's responses during the COVID-19 pandemic. 'Values' and 'dispositions', were not tested as these are individual characteristics which could

be expected to have similar variability across all student bodies and are less likely to be affected by country context as much as the other two.

The following research questions were posed:

RQ1. [Risk perceptions] What are the attitudes and concerns of participating students of the cyber related risks of the online environment?

RQ1a. [Attitudes] What are the attitudes to cyber related risks?

RQ1b. [Concerns] Which online concerns do they have?

RQ2. [Behaviours] Did the students report changing their protective behaviours with the shift to online learning?

3. Methods

This research study is part of a larger study on the eLearning perspectives of students and staff during the COVID-19 pandemic. For this paper, the focus is on the concerns and perceptions of cyber related risks and the protective behaviours reported by the participating students.

The survey questionnaire (see Appendix A for the full questionnaire) included 14 questions on cyber related issues. The survey was piloted with approximately 10 students at each university and at different levels of study to test the survey for clarity and to afford refinement.

3.1. Ethics

The researchers received permission to disseminate the questionnaire to the student population of the participating universities. Ethical approval was obtained from ethical review boards. Students were not remunerated and answered the questions anonymously.

3.2. Recruiting and Data Collection

The main study respondents were recruited by means of a link distributed to all students at each university by email. The questionnaire could be completed in English (which is the language of instruction at both the Welsh and South African Universities) or in Hungarian.

Online questionnaires were administered using Qualtrics. This presented the most feasible way of consulting the three countries' students during the pandemic [24]. Data was collected from October to November 2020 and collected separately at the three universities. The three databases were collated and analyse as one dataset.

3.3. Analysis

To confirm the validity of the identified categories, factor analysis was carried out using the principal component method with a varimax rotation. Based on the determined categories, comparative statistical analyses were carried out using the Chi^2 test to answer the two research questions.

After data was collected, it was analysed to reveal the similarities and differences in the cyber related risk perceptions (attitudes and concerns) and protective behaviours of the students. The statistical programmes Statistical Analysis System (SAS) version 9.4 and Statistical Package for the Social Sciences (SPSS) version 25 were used to support the analysis.

4. Results

4.1. Student Demographics

A total number of 559 questionnaires were completed by the participating students. The data was cleaned, removing incomplete responses. A total of 512 data entries remained to support the analysis: 240 from Hungary, 141 from Wales and 131 from South Africa (see Figure 5).

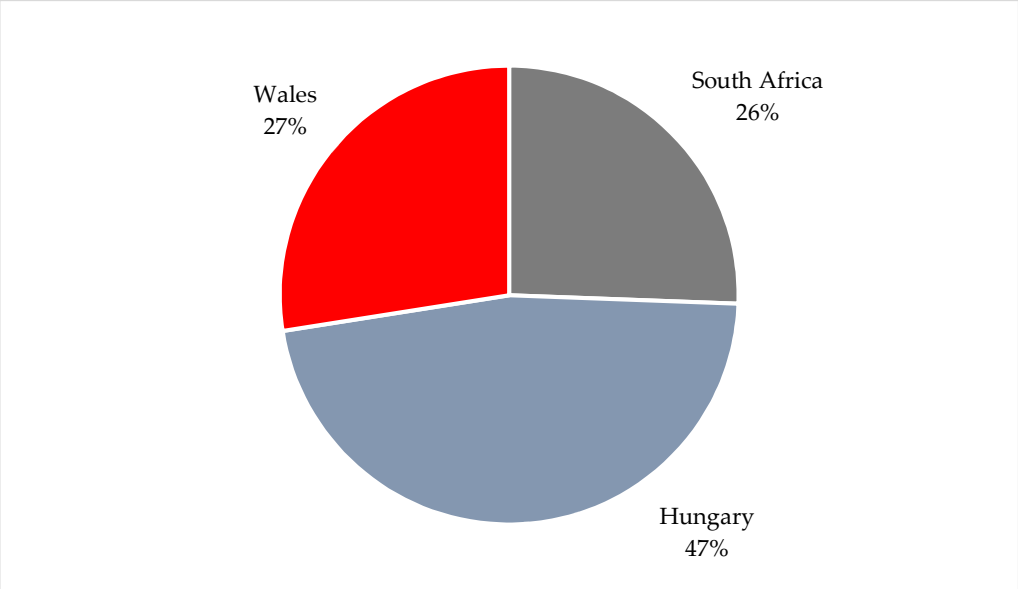

Figure 5. Student participants by university in the different countries (%).

The students who were studying at these three universities were from 46 different countries (Angola, Azerbaijan, British, China, Congo, Ethiopia, France, Ghana, Greece, Hong Kong, Hungary, Indonesia, Ireland, Japan, Jordan, Kazakhstan, Kenya, Kuwait, Kyrgyzstan, Latvia, Libya, Lithuania, Malaysia, Mexico, Moldovia, Mongolia, Morocco, Lesotho, Namibia, Nigeria, Norway, Poland, Portugal, Romania, Russia, Rwanda, Saudi Arabia, Slovakia, South Africa, Spain, Thailand, Turkey, Vietnam, Yemen, Zambia, Zimbabwe). This confirms the heterogeneity of student demographics across these universities.

Most participants were undergraduates (95%) from various degree programmes, across a range of subjects from within social and other sciences. In this case, 27% of the respondents were in their first year of study, 20% in the second year, 29% in their third year, 21% were in their fourth year. Very few (4.1%) of the students were pursuing postgraduate studies (see Figure 6). Although all the universities had students from other countries the Welsh participating university had the most international students. Slightly more males (54%) than females (45%) answered the questionnaire with 1% not identifying as either of the genders.

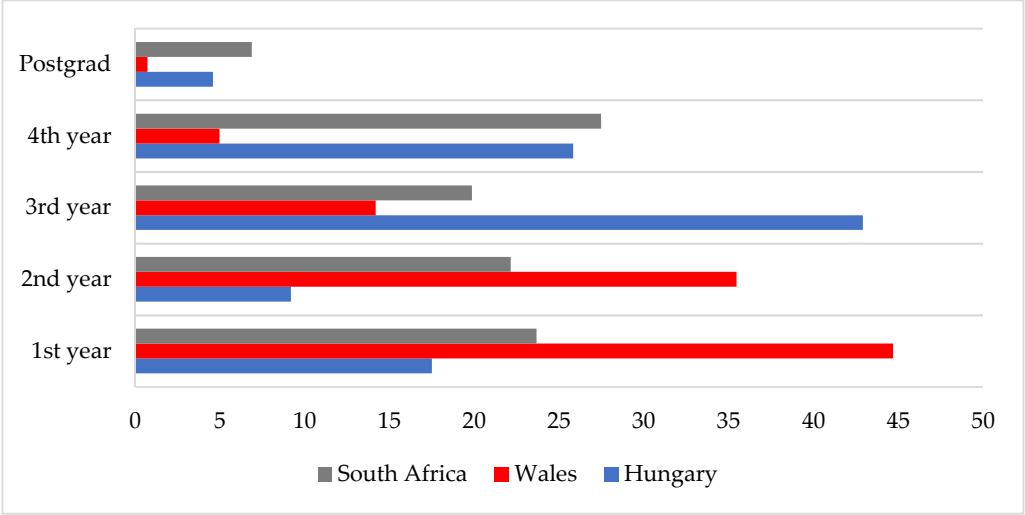

Figure 6. Student participants by academic year of study (%).

Almost all respondents (95%) were in their 20's, with a few outliers. Most students remained in the country where they were studying during lock-down.

4.2. Reliability of the Cyber Related Categories

The internal reliability of the cyber related questions was tested using the Cronbach's Alpha reliability test. According to Taber [25] different qualitative descriptors are assigned to different Cronbach's alpha throughout research papers. Based on their results, Cronbach's alpha values ranging between 0.76 and 0.95 are considered fairly high, high and good [25]. The overall reliability of this study's questions equalled 0.789 (on the standardized question this value was 0.759)—a Cronbach Alpha scale of over 0.7 means that the questions are reliable, see Table 1 [26].

Table 1. Factor loadings and item reliability of the three categories.

Categories and Questions in Terms of Cyber Related Security, Privacy and Safety	Factor Analysis	Item Reliability Cronbach's Alpha
Category 1: Risk perception: attitudes		
Social networking (Safety and Privacy)	0.670	0.770
Public Wi-Fi (Security and Privacy)	0.749	0.763
Online banking (Security)	0.780	0.758
COVID-19 tracking (Privacy)	0.678	0.777
Online shopping (Security)	0.772	0.762
Video conferencing and online meetings (Privacy)	0.720	0.773
Learning Management Systems (for example Canvas, Blackboard, KMOOC, Moodle, iKamva, etc.) (Security)	0.681	0.775
Category 2: Risk perception: concerns		
I am concerned about issues of security when engaging in digital learning	0.873	0.778
I am concerned about issues of privacy when engaging in digital learning	0.866	0.774
I am concerned about issues of malware when engaging in digital learning	0.835	0.774
I am concerned about issues of fraud when engaging in digital learning	0.826	0.774
I am more aware of cyber security issues since the pandemic and the shift to online teaching and learning (enhanced risk concerns)	0.615	0.782
Category 3: Protective behaviours		
I have changed my online security and safety behaviour due to COVID-19	0.729	0.802
I use a VPN when I go online (Security and Privacy)	0.664	0.792

In the case of cyber related 'attitudes' the Cronbach Alpha was 0.845. While each question's individual Cronbach Alpha was greater than 0.76. The questions of the cyber related 'concerns' showed high internal reliability with a Cronbach Alpha equal to 0.831. Each question's individual Cronbach Alpha was greater than 0.77 whereas the 'Protective behaviours during COVID-19′ were close to 0.8.

Factor analysis confirmed that the identified cyber related category items are related and give a reliable framework for the evaluation of the data. It must be noted that the questionnaire was designed by the researchers and was not a standardized questionnaire. The factor analysis employing the Principal Component method with Varimax rotation and Cronbach Alpha confirmed the three categories.

The factoring Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy equated 0.855, while the Bartlett's Test of Sphericity proved to be significant ($p = 0.000$). Both imply that the data are appropriate for factor analysis.

When presenting the factor analysis results it can be seen how the questions group into the three categories. There was a certain redundancy between the variables hence, the existence of the three categories is valid (see Figure 7).

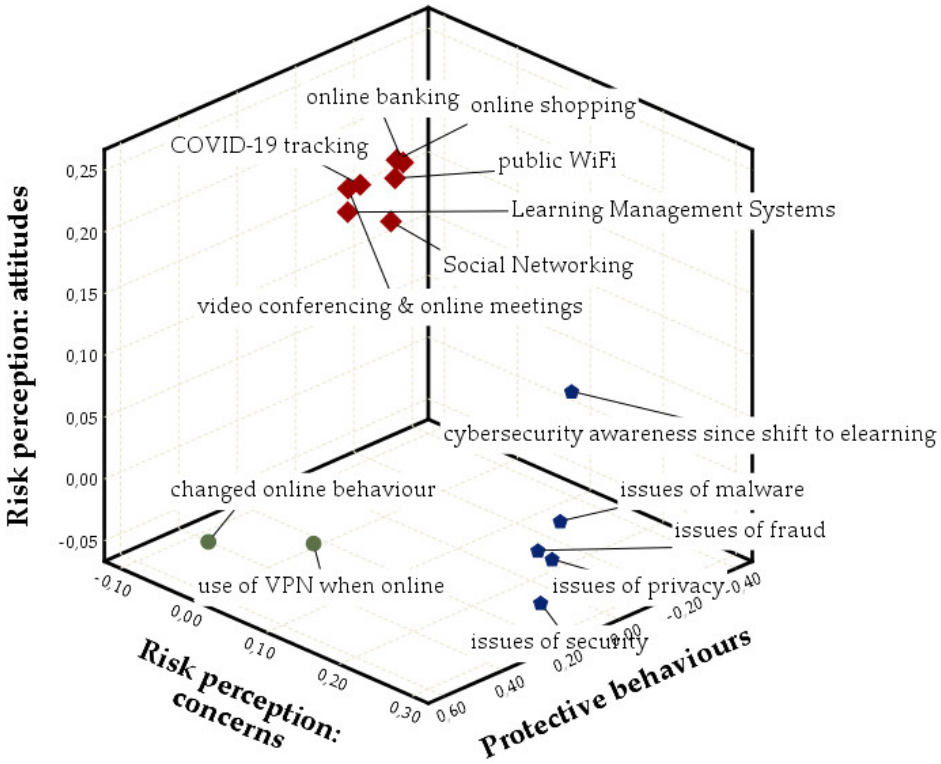

Figure 7. Grouping of the risk perceptions, risk concerns and protective behaviours categories.

4.3. Bi-Variate Analysis

In Table 2 the country comparison of all the questions is summarised with an asterisk indicating significant differences.

Table 2. Country comparisons of individual questions.

Categories and Questions	Chi^2	*p*-Value
Categories 1: Risk perceptions: attitudes		
Social networking (Safety and Privacy)	23.66	0.0026 *
Public Wi-Fi (Security and Privacy)	24.45	0.0019 *
Online banking (Security)	24.94	0.0016 *
COVID-19 tracking (Privacy)	13.85	0.0858
Online shopping (Security)	23.01	0.0034 *
Video conferencing and online meetings (Privacy)	14.88	0.0616
Learning Management Systems (for example Canvas, Blackboard, KMOOC, Moodle, iKamva, etc.) (Security)	14.14	0.0782
Categories 2: Risk perceptions: concerns		
I am concerned about issues of security when engaging in digital learning	41.11	<0.0001 *
I am concerned about issues of privacy when engaging in digital learning	36.42	<0.0001 *
I am concerned about issues of malware when engaging in digital learning	88.23	<0.0001 *
I am concerned about issues of fraud when engaging in digital learning	65.89	<0.0001 *

Table 2. *Cont.*

Categories and Questions	Chi^2	*p*-Value
I am more aware of cyber security issues since the pandemic and the shift to online teaching and learning (enhanced risk awareness)	74.49	<0.0001 *
Categories 3: Protective behaviours		
I have changed my online security and safety behaviour due to COVID-19	18.76	<0.0001 *
I use a VPN when I go online (Security and Privacy)	57.92	<0.0001 *

* Indicating *p*-value < 0.05.

4.3.1. Risk Perception of Cyber Security and Cyber Safety

Attitudes

Differences were found in risk perceptions between the different countries' students (see Table 2). In all countries, over 60% considered social networking usage to be risky, in terms of both cyber security and cyber safety (Chi^2 = 23.66 and p = 0.0026) (see Figure 8).

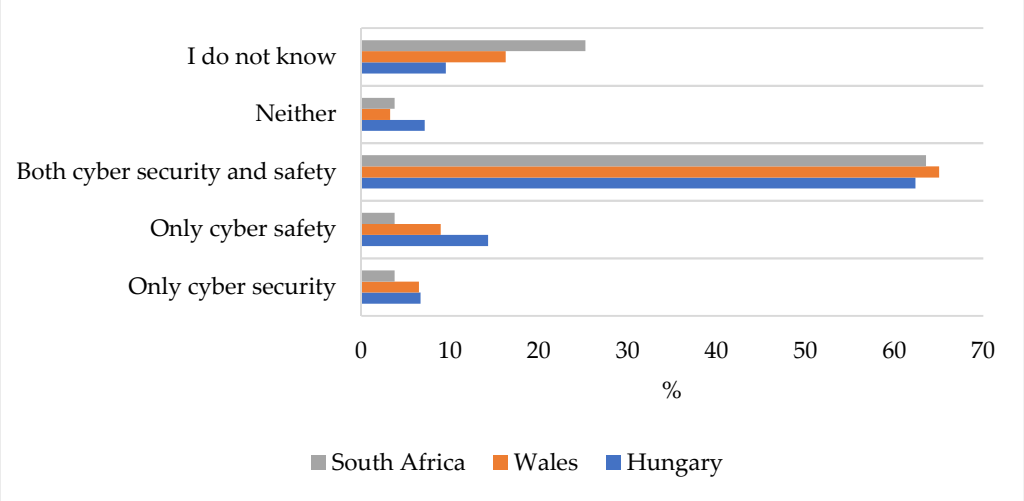

Figure 8. Perception of cyber security and cyber safety issues with social networking platforms.

The majority felt similarly about using public Wi-Fi. However, Hungarian and Welsh students considered this more of a cyber security issue, while the South African students' (22%) did not (Chi^2 = 24.45 and p = 0.0019). The majority of students felt that online banking had cyber security and cyber safety implications (see Figure 9), with some Hungarian and Welsh students considering it merely a cyber security issue, whereas 15% of the South African students indicated that they did not know whether online Internet banking posed any cyber related risk (Chi^2 = 24.94 and p = 0.0016).

The participating students were undecided about the cyber security, cyber safety and privacy implications of COVID-19 tracking apps (Chi^2 = 13.85 and p = 0.0858) as well as video conferencing applications (Chi^2 = 14.88 and p = 0.0616) and learning management systems (Chi^2 = 14.14 and p = 0.0782). The majority of students across all universities were aware of potential cyber security and cyber safety implications when undertaking online shopping. Hungarian and Welsh students were more aware of these cyber security related risks (Chi^2 = 23.01 and p = 0.0034).

Concerns

In order to gain insight into student's cyber related perceptions (and given that feelings/concerns are part of this—see Figure 2, a sentiment analysis was conducted based on their responses, and it was found that the answers were distributed almost evenly for disagree, neutral and agree. In this case, 39% of the respondents were concerned about

privacy issues while 30% were concerned about cyber security issues when engaging in digital learning.

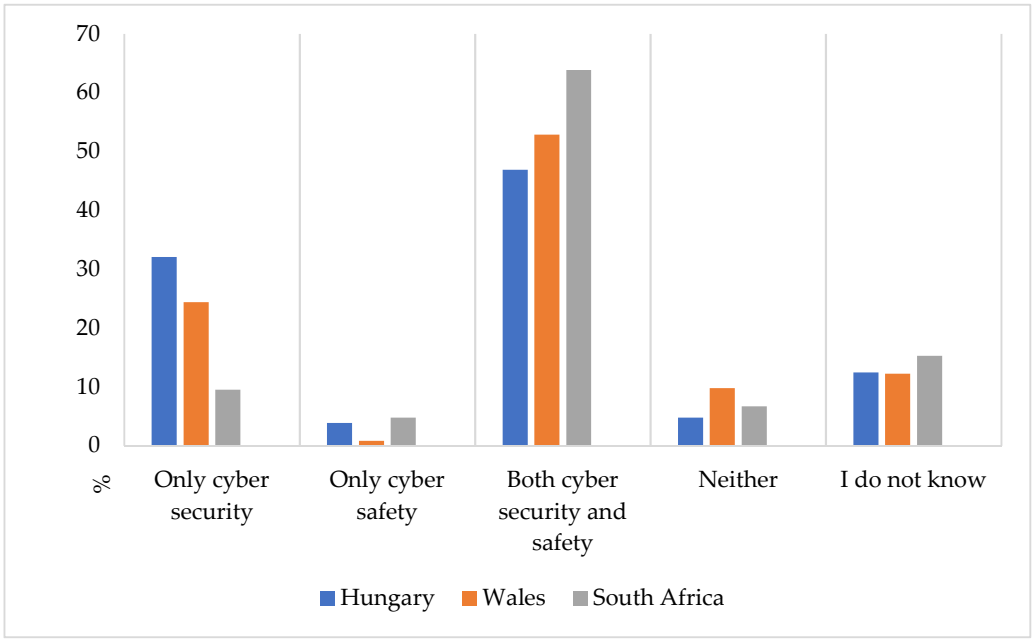

Figure 9. Perception of the cyber security and cyber safety in terms of online banking.

On conducting a country comparison, significant differences were detected. More of the South Africans expressed concerns about cyber security issues (52%) ($Chi^2 = 62.72$ and $p < 0.0001$), privacy issues (62%) ($Chi^2 = 65.78$ and $p < 0.0001$), and in particular cyber security fraud issues (63%) ($Chi^2 = 88.22$ and $p < 0.0001$) and cyber security malware issues (70%) ($Chi^2 = 101.72$ and $p < 0.0001$) when engaging in digital learning since the pandemic than students at the Welsh or the Hungarian students (see Figure 10).

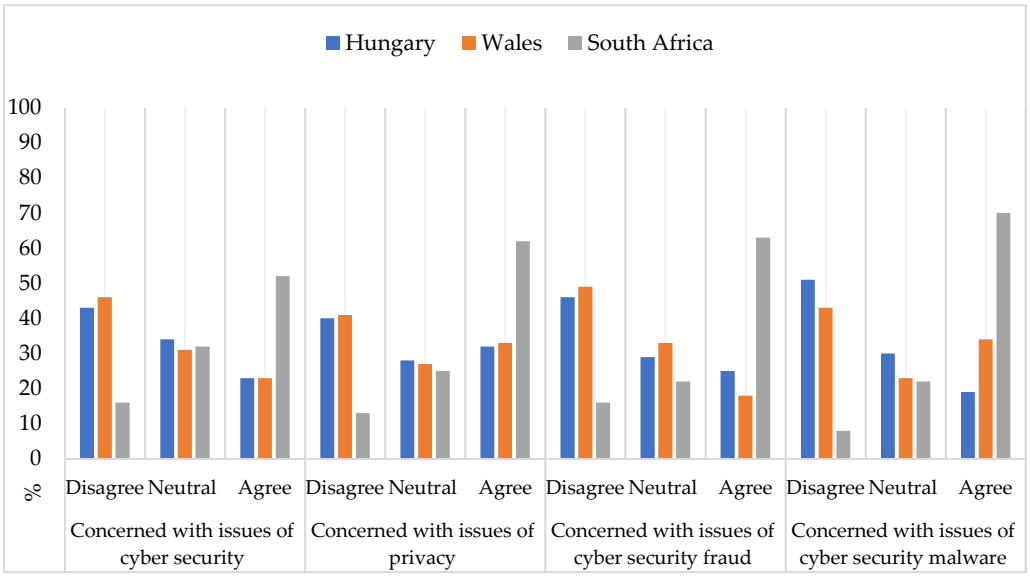

Figure 10. Cyber security risk perceptions (concerns) during digital learning and the shift to on-line learning during COVID-19 per university.

Figure 11 shows that the participating students from the universities within the three countries responded significantly different ($Chi^2 = 74.49$, $p = 0.0001$) to the shift to digital

online learning. The students from the South African university (61%) were more aware of the cyber security issues resulting from the shift to online teaching. Fewer of the Welsh university's students (37%), and even fewer of the Hungarian university's students (16%) were aware.

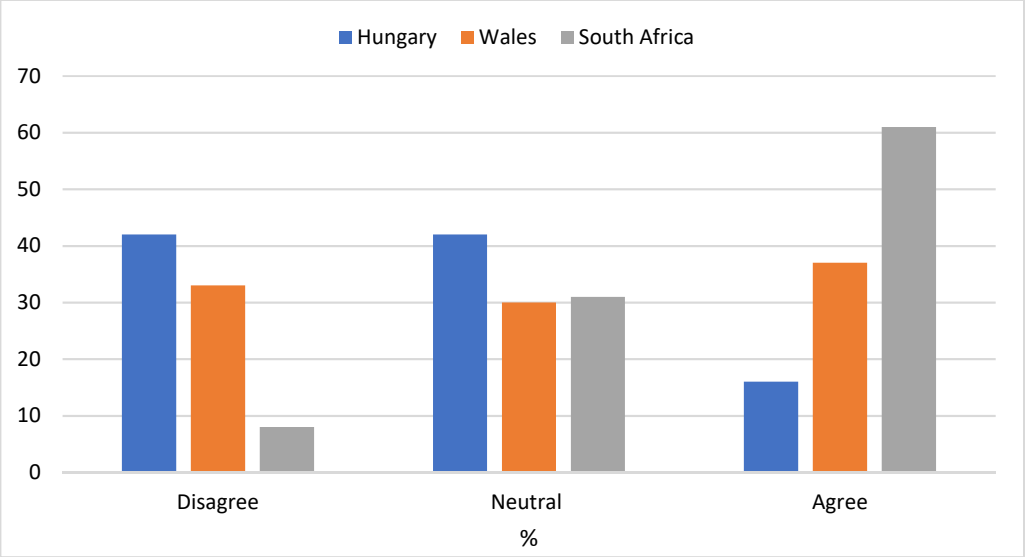

Figure 11. Cyber security risk perception (concerns) changes due to the shift to online teaching.

4.3.2. Protective Behaviours during the COVID-19 Pandemic

The reported protective behaviour category comprised two questions. The first concerns the use of virtual private networks (VPN) and the second considers the change in online behaviours. Hungarian-(40%) and Welsh students (43%) sometimes used the university's VPN, whereas South Africans (45%) did not know how to use VPNs ($Chi^2 = 57.92$ and $p < 0.0001$) (see Figure 12).

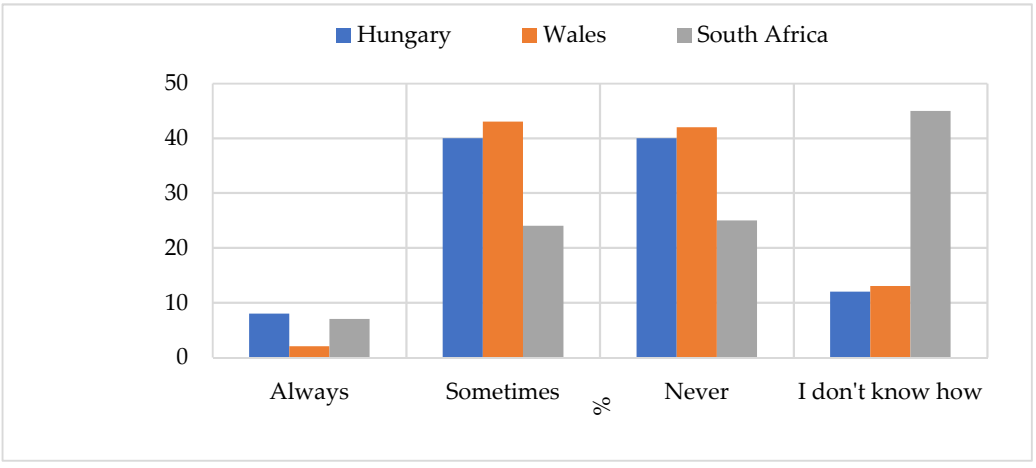

Figure 12. I use a VPN when I go online.

Half of the South Africans reported having adapted their online behaviours since digital learning commenced, whereas only 30% of the Welsh and 24% of the Hungarians indicated that they had achieved likewise ($Chi^2 = 18.76$ and $p < 0.0001$) (see Figure 13).

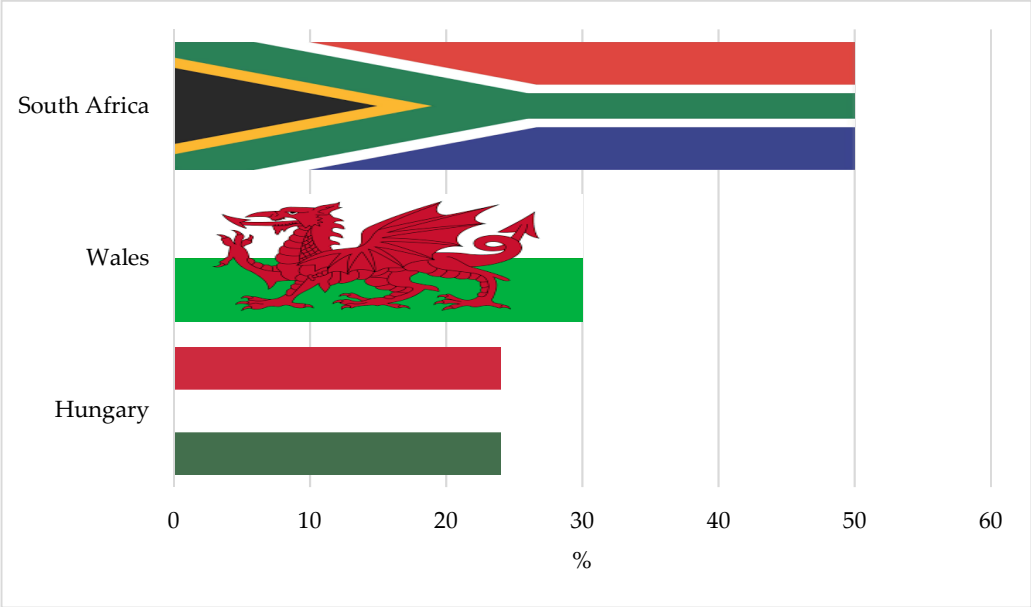

Figure 13. Students indicating that their online cyber-security and cyber-safety behaviour changed during COVID-19.

5. Discussion

The research aimed to investigate and understand the impact of COVID-19, on the risk perceptions—in terms of cyber security and cyber safety—of higher education students, during the first and second wave of the pandemic. In addition, it was investigated, whether these students—due to the shift to a single mode of learning—exhibited any change in their online behaviour as a consequence of the COVID-19 pandemic. Two primary research questions were posed, and these will be revisited and then discussed.

RQ1. [Risk perceptions] What are the attitudes and concerns of participating students of the cyber related risks of the online environment?

RQ1a. [Attitudes] What are the attitudes to cyber related risks?

RQ1b. [Concerns] Which online concerns do they have?

RQ2. [Behaviours] Did the students report changing their protective behaviours with the shift to online learning?

When revisiting the research questions the following was noted:

Attitudes

A large majority of all respondents, from all participating universities, acknowledged the cyber related implications of digital applications and platforms. However, they were unclear as to whether there were cyber security and/or cyber safety implications related to: (1) COVID-19 tracking applications, (2) video conferencing applications, and (3) learning management systems. Alexei and Alexei [27] (p. 1) contend that learning management systems do indeed have several technical and human vulnerabilities. Furthermore, since cloud computing, eLearning platforms and video conferencing applications have become the primary modalities for facilitating eLearning, the risks of distributed denial-of-service (DDoS) attacks/denial-of-service (DoS) attacks, cross-site scripting, spoofing, unauthorized data access and infection with malicious programs, but also the theft of personal data, has increased dramatically [27]. It must be noted that the students themselves were unable to mitigate these particular vulnerabilities, since they were required to use their university's learning management systems. Similarly, since video conferencing applications were the main form of communication and delivery of online classes.

The Cyber Risk Literacy and Education Index [17] does not rank South Africa lowest when comparing the participating countries for the pillar '*cyber risk awareness and motivation*' (see Figure 4) [17]. In 2017, Shabe et al. [28] explored the state of cyber security concerns among mobile phone users living in Rocklands Township, South Africa. Shabe's study,

using the scorecard approach, revealed that individual mobile phone users are more exposed to cyber-attacks due to their lack of cyber concerns. Dlamini et al. reported that African countries, mostly developing countries, can raise cyber awareness only if the countries collaborate and step up jointly against cyber-attacks, prepare cooperative cross-border educational and training programmes throughout the African continent [29]. The authors take examples from developed countries with highly cyber-preparedness (USA, UK, Estonia and Korea) and point out the urgency of actions to be taken, such as bridging the digital divide, improving digital literacy, the dominant use of mobile devices and wireless networks. Hence, despite the high levels of awareness demonstrated by our South African participants, there is still a clear need for cyber related risk awareness training given the region's high volatility and vulnerability to cyber-attacks [22].

Earlier research at a Hungarian university revealed that students behave differently when using eLearning systems [30,31]. Furthermore, cyber related risk awareness needs to be improved. Universities' participation in improving student cyber related awareness becomes more important as online education is embraced. Universities should inform students of protective behaviours they can engage in related to cyber security and cyber safety [32]. This is especially important as they use the mandated online learning environments. The authors take examples from developed countries with highly cyber-preparedness (USA, UK, Estonia and Korea) and point out the urgency of actions to be taken, such as bridging the digital divide, improving digital literacy, the dominant use of mobile devices and wireless networks.

A study conducted in 2020, considering smart phone security awareness and practices of students at a Welsh University, indicated that the level of cybersecurity awareness, in general could be improved [33]. This current study suggests that the students do indeed have a measure of cyber related risk perceptions (attitudes), although the country comparisons revealed significant differences. There is therefore still a clear need for cyber related skills training.

Concerns

Sentiment analysis revealed that the cyber security, safety, and privacy concerns were evenly spread. Some of the respondents were concerned about privacy while others were concerned about cyber security when engaging in digital eLearning. In general, South Africans were more concerned about privacy, cyber security (fraud, malware etc.), as compared to the Welsh and Hungarian students. According to the NCSI National Cyber Security Index which measures country's cyber security capacity [15], the UK ranks 18th with a score of 77.92, Hungary ranks 32nd, and has a score of 64.92, while South Africa ranks 83rd, and has a score of 36.36 (see Table 3). Comparing all the countries' National Cyber Security Index (NCSI) and Digital Development Level (DDL), a strong relationship was found using Spearman's rank correlation ($\rho = 0.709$, $p = 0.000$), suggesting that the higher a country's digital development level, the higher its cyber security index.

Table 3. National Cyber Security Index (NCSI) [15].

Country	National Cyber Security Index (NCSI)	Rank NCSI	Digital Development Level (DDL)	Rank (DDL)	Difference (NCSI-DLL)
South Africa	36.36	83	47.43	85	↓ −11.07
Hungary	64.94	32	64.68	42	↑ 0.26
United Kingdom	77.92	18	81.39	7	↓ −3.47

The difference between the Digital Development Level (DDL)—the average fulfilment of ICT development and networked readiness—and the NCSI explains the difference between technology development and implementation and the governments' ability to protect as well as train and motivate its citizens. For example, for South Africa the DDL is relatively

high, however, students do not trust their cyber security capacity, which is reflected in the National Cyber Security Index. Cohney et al. [1] recommends strengthening regulatory mechanisms to provide appropriate baseline privacy and security protections. Students from Hungary and the United Kingdom were less concerned with cyber security issues, which is also reflected in the higher National Cyber Security Indices of both countries.

Changes in Protective Behaviours

The researchers wanted to determine whether students had changed their online behaviours during the COVID-19 pandemic lockdowns. Half of the South African students reported having adapted their online behaviours, while only a third of the Welsh and Hungarians had achieved likewise. This confirms the Wyman's Cyber Security and Education Index rankings, given that the United Kingdom is ranked 4th for the formal education pillar, implying that their cybersecurity education is much better than Hungary (ranked 28th) and South Africa (ranked 48th). This digital development level of the countries is reflected in the behaviour of the different university's students.

South African students did not know how to use Virtual Private Networks (VPNs) perhaps because they were not given the opportunity to do so or because it is costly. However, South African students had to adapt to the greatest extent to using the digital learning environment since the outbreak of COVID-19 because most had accessed the university's online environment from university facilities. This was not the case for the Hungarian and Welsh students. Respondents from Hungary and Wales were clearly digitally more prepared for an exclusively online learning environment than the South African Students. Previous research shows that South African students struggle to afford online access [34] and this might explain the difference. Yet, during the pandemic, all South African students were given computers and data bundles to facilitate access to university resources from their mobile phones. On the other hand, no such accommodation was made for the Welsh and Hungarian students. Even so, it is likely that most of these students had broadband at home in Hungary [31] and in Wales [2].

6. Contributions

In this paper, we make the following contributions:

We contribute to the body of knowledge of cyber security and cyber safety behaviour, and in particular the cyber security and safety risk perceptions -attitudes and concerns—as well as student behavioural changed in online learning environment during COVID-19 lockdown.

We undertook an original, international (three countries, both developed and developing/developed), comparative, quantitative research project which has revealed significant differences between the participating universities, with the most important differences being risk perception attitude and concerns, followed by changed behaviour. The differences between student cyber-related risk perception attitude, concerns as well as changed behaviour can be attributed to the differing cyber security awareness, digital development level, and furthermore, different level of cyber security literacy and education of the participating countries: South Africa, Wales, and Hungary.

Based on the results from this study, several suggestions are made to influence future pedagogical approaches to university cyber-related training.

7. Limitations and Future Research

The research focused on one university in each of the three countries. Further research will need to be conducted to include more universities to gain greater insights. All findings rely on self-reporting, which has undeniable shortcomings. However, given that the study was carried out during the pandemic, this was considered the best way to reach all the students studying remotely. Only two questions were included to reveal behavioural changes, which might not have uncovered all possible changes and/or behaviours. Even so, these questions served to provide evidence of changes triggered by heightened risk perceptions and the switch to online learning.

8. Conclusions and Recommendations

Based on these published literacy levels, it would be expected to see the highest levels of risk perception and changed behaviour during COVID-19 in the Welsh University students, the least from the South African students and the Hungarian students somewhere in-between.

This study sought to compare, and contrast risk perceptions and protective behaviours engaged in by students in three countries with very different levels of cyber risk literacy. While all students had to switch to remote learning overnight, each student's context was different, and would have influenced their risk perceptions and behaviours.

The following can be concluded:

Attitudes: This study suggests that students have a measure of cyber related risk perceptions (attitudes). However, due to the significant differences between countries, there is a clear need for cyber related skill training, especially in South Africa. The Oliver Wyman Index suggests that the cyber risk literacy of the Welsh students ought to have been the highest, with the South Africans having the lowest levels. Our studies aligned with this index, confirming the need for South Africa to invest more resources into raising cyber awareness across their society. If students are insufficiently aware, it is unlikely that the rest of the population will be any more literate.

Concerns: All students demonstrated a measure of concern about privacy and cyber security while engaging with digital eLearning. Students in South Africa, in particular, did not trust the cybersecurity capability of their digital provisions, reflected in the National Cyber Security Index, despite the relatively high digital development level.

Changes in protective behaviours: The switch to online learning was more drastic for a larger proportion of the South African university's students, since many did not engage with a learning management system from home, before the lockdown. Despite this, the South African university supported their students by providing them with mobile data as well as computers and the necessary resources to ensure that they were able to continue learning. The other two countries' students were not given this advantage. The fact that South African university's students changed their protective behaviours to the greatest extent, is probably attributable to these factors.

Country similarities and differences: The only similarity that was found between the cyber security risk perception (attitudes) of students was related to the COVID-19 tracking systems. All other comparisons related to risk perception (attitudes), reflected significant differences. The same was found for the risk perceptions (concerns). Students from the South African university indicated that they were more aware of cybersecurity issues since the pandemic and shift to online learning. In the case of the Hungarian university's students, the responses were distributed between 'disagree' and 'neutral', while very few agreed with the statement. The Welsh university's student responses were more evenly distributed. In terms of changed online cybersecurity behaviour, the study suggests that the South African university's' students' behaviour changed to the greatest extent.

Recommendations: The pandemic ushered in unprecedented challenges for everyone who experienced a lockdown, but for students it was acutely challenging. Our study highlighted the need for targeted and sustained efforts to be engaged in to ensure that those who are now conducting their learning online have an accurate awareness of cyber risk perceptions and know how to protect themselves and their information online. There is a need to foster digital trust to build confidence across society, with South Africa demonstrating the greatest need. There is a clear need to do more in terms of cybersecurity training and education, and universities should focus on addressing this need [35].

Author Contributions: Conceptualization—D.J.C., I.M.V., A.T. and K.V.R.; methodology—D.J.C., A.T., I.M.V. and R.J.B.; validation—A.T., R.J.B., I.M.V. and D.J.C.; formal analysis—A.T. and R.J.B.; investigation—D.J.C., I.M.V., A.T. and R.J.B.; writing—original draft preparation, D.J.C., I.M.V. and A.T.; writing—review and editing—D.J.C., I.M.V., A.T., K.V.R. and R.J.B.; visualization—D.J.C., I.M.V., A.T., R.J.B. and K.V.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: The study was conducted according to the guidelines of the Declaration of Helsinki, and approved by the Ethics Committee of Swansea University (approval on the 23 June 2020) and Human and Social Sciences Ethics Committee, HS20/5/20, University of the Western Cape (approval on the 30 September 2020).

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

Data Availability Statement: The data collected can be made available upon request.

Acknowledgments: The authors would like to thank Paul Jones, Head of School, Swansea University, for supporting this collaboration between the three countries, by providing funds to initiate the collaboration with South Africa and Hungary. The authors would also like to thank all three participating universities for providing the researchers with the time to conduct the research.

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

Appendix A. Questionnaire Impact of COVID-19 on Student Learning 2020

Dear Participant

The "lockdown" has dramatically changed the landscape of higher education institutions. Previously institutions had a choice in their pedagogical practices, which included various teaching delivery modes. Suddenly a single mode of delivery had to be adopted, and all services had to be migrated to digital platforms. The impact on all cohorts of students is uncertain. This cross-university, international, comparative, quantitative research project aims to investigate and understand: (1) The impact of COVID-19 on the student learning experience; (2) How the choice of digital technologies for the purposes of education affects equitable student access; (3) What the behavioural changes, if any, of students are in relation to cybersecurity and cybersafety.

This collaborative research has received ethical clearance. If you agree to participate, your identity and responses will be anonymised. The questionnaire is used purely for research purposes. The information contained in the questionnaire will not be used in any other way and will be safely stored and deleted once the research is completed.

When answering the questionnaire, please think of your academic experience during 2020. This questionnaire should not take longer than 15 min to complete.

Thank you for taking the time to complete the questionnaire. Your responses will assist in the understanding of the impact of online teaching on student's experience.

For further information or if you have any queries, please email wssh.research@gmail.com.

A. DEMOGRAPHICS

Q1. At what University are you currently studying?

1. Óbuda University, Hungary
2. University of the Western Cape, South Africa
3. Swansea University, Wales
4. Other

Q2. Please select your academic year of study

1. Year 1 of undergraduate study
2. Year 2 of undergraduate study
3. Year 3 of undergraduate study
4. Year 4 of undergraduate study
5. Postgraduate study
6. Other? _____

Q3. Which of the following best describes the main subject area you are studying for your current degree/diploma qualification?

1. Computer Science
2. Management

3. Business
4. Economics
5. Marketing
6. Accounting
7. Finance
8. Psychology
9. Physics
10. Mathematics
11. Engineering
12. Statistics
13. Other: _____

Q4. What gender type do you identify with?

Male	Female	Non-Binary	Other
1	2	3	4

Q5. Which country do you live in currently, during the lockdown? _____

Q6. What is your nationality? _____

Q7. What is your age? _____

B. ACCESS TO THE ONLINE DIGITAL LEARNING ENVIRONMENT

Q8. From where do you MOSTLY access the university's online environment?

At Home (or Where You Reside) Using Broadband Wi-Fi	At Home (or Where You Reside) Using Mobile Wi-Fi	At an Internet Cafe	At a Friend/Family Member's House	At a Facility Provided by the University	At a Public, Free Wi-Fi Spot
1	2	3	4	5	6

Q9. What device do you MOSTLY use to access online materials?

Own Phone	Someone Else's Phone	Own Laptop	Someone Else's Laptop	Own Personal Computer	Someone Else's Personal Computer	Own Tablet	Someone Else's Tablet	Any Other Device, Like a Smart Tv etc.
1	2	3	4	5	6	7	8	9

Q10. How long have you been using a digital device to access the Internet?

1–2 Years	3–4 Years	4–5 Years	More Than 5 Years
1	2	3	4

The COVID-19 pandemic may have had an impact on the costs of your studies and accessing the online learning platform. Which of these apply to you?

	Increased	Stayed the Same	Decreased
Q11. Accommodation costs	1	2	3
Q12. Internet access costs	1	2	3
Q13. Digital equipment costs	1	2	3

Rate on a scale of 1–5 the extent to which the given statements suit you.

Dimension of System Access	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Q14. I am satisfied with my Internet access	1	2	3	4	5
Q15. The university digital learning environment is always accessible to me	1	2	3	4	5
Q16. The university's digital learning system is always fully operational	1	2	3	4	5

C. STUDENT LEARNING EXPERIENCE DURING COVID-19

Rate on a scale of 1–5 the extent to which the given statements suit you.

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Dimension of learning environment	1	2	3	4	5
Q17. I have a good learning environment at home (or where I reside)	1	2	3	4	5
Q18. I have the appropriate digital equipment to access the university digital environment	1	2	3	4	5
Q19. I preferred accessing the digital learning environment more than the in-person on campus learning	1	2	3	4	5
Dimension of participation	1	2	3	4	5
Q20. I found it easy to interact with my lecturers and peers during an online lecture/seminar session	1	2	3	4	5
Q21. I always have my video on when attending an online session	1	2	3	4	5
Q22. I miss the in-person interaction with other students	1	2	3	4	5
Dimension of concentration	1	2	3	4	5
Q23. I cannot concentrate and engage with the learning effectively when the lecture or seminar video is longer than 15 min	1	2	3	4	5
Dimension of digital learning	1	2	3	4	5
The online academic education during the pandemic, helped me to become more independent as a learner	1	2	3	4	5
The online academic education during the pandemic, improved my digital literacy	1	2	3	4	5

D. DIGITAL TECHNOLOGIES USED

Please rate how you experienced the following:

Use of Digital Technologies	Took a Long Time to Get Used to	Took Some Time to Get Used to	Was Easy to Use
Q24. The use of online collaborative tools (like Zoom, Skype, and Teams, etc.)	1	2	3
Q25. The universities online learning platform	1	2	3

Q26. How did you manage the transition to online learning?

It Was Easy	It Was Challenging	It Was Neither Easy Nor Challenging
1	2	3

Q27. Which of the following technologies did you mostly use to access your peers, lecturers, learning material etc during the pandemic? Choose five from the list below, and add to it, if necessary.

Technologies	Rank Your Preference (1–5)
WhatsApp	
The University's online learning platform	
Zoom	
Skype	
Microsoft Teams	

Technologies	**Rank Your Preference (1–5)**
Google Hangouts	
Google Meets	
Dropbox	
Google Drive	
Telegram	
iMessenger	
Email	
SMS (short messaging service)	
Other (please list)	

When considering digital learning, how important is it to you that the following features are available

	Not at All Important	**Slightly Important**	**Not Sure**	**Important**	**Very Important**
Q28. Content visible on a mobile device	1	2	3	4	5
Q29. Slides with voice over recording	1	2	3	4	5
Q30. Live interactive online lectures	1	2	3	4	5
Q31. Teamwork and working together with others online	1	2	3	4	5
Q32. Prescribed or recommended books available as an e-book	1	2	3	4	5
Q33. End-of-chapter/or assignment questions/quiz with feedback	1	2	3	4	5
Q34. Completing set online tasks, that forms part of the final grade	1	2	3	4	5

Rate the extent to which the given statements suit you.

Dimension of Student Engagement	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
Q35. I prefer to work independently	1	2	3	4	5
Q36. I like to actively participate in online discussions	1	2	3	4	5

E. CYBERSECURITY AND CYBERSAFETY

Are you more aware of cybersecurity issues since the pandemic and the shift to online teaching and learning?

Cyber Security	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
Q37. I am concerned about issues of security when engaging in digital learning	1	2	3	4	5
Q38. I am concerned about issues of privacy when engaging in digital learning	1	2	3	4	5
Q39. I am concerned about issues of fraud when engaging in digital learning	1	2	3	4	5
Q40. I am concerned about issues of malware when engaging in digital learning	1	2	3	4	5
Q41. I am more aware of cybersecurity issues since the pandemic and the shift to online teaching and learning	1	2	3	4	5

Q44. I have changed my online security and safety behaviour due to COVID-19

Yes	No
1	2

Which of the following (functions or apps) do you think could have potential cybersecurity/cybersafety implications?

Function	Only Cyber Security	Only CyberSafety	Both Cyber Security and Cyber Safety	Neither	I Do Not Know
Q45. Social Networking, such as Facebook	1	2	3	4	5
Q46. Use of public Wi-Fi	1	2	3	4	5
Q47. On-line internet banking	1	2	3	4	5
Q48. COVID-19 tracking apps	1	2	3	4	5
Q49. On-line shopping	1	2	3	4	5
Q50. Video conferencing applications (Zoom, Microsoft Teams, etc.)	1	2	3	4	5
Q51. Learning Management Systems (for example Canvas, Blackboard, KMooc, Moodle, iKamva, etc.)	1	2	3	4	5

I use a VPN when I go online

Always	Sometimes	Never	I do not know how
1	2	3	4

Thank you.

References

1. Cohney, S.; Teixeira, R.; Kohlbrenner, A.; Narayanan, A.; Kshirsagar, M.; Shvartzshnaider, Y.; Sanfilippo, M. Virtual Classrooms and Real Harms: Remote Learning at US Universities. The Advanced Computing Systems Association: Berkeley, CA, USA, 2021.
2. International Telecommunication Union (ITU). *Global Security Index 2020*; International Telecommunication Union (ITU): Geneva, Switzerland, 2020.
3. Mee, P.; Brandenburg, R.; Lin, W. *Oliver Wyman Forum Global Cyber Risk Literacy and Education Index*; Oliver Wyman Forum: New York, NY, USA, 2021.
4. Lallie, H.S.; Shepherd, L.A.; Nurse, J.R.; Erola, A.; Epiphaniou, G.; Maple, C.; Bellekens, X. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Comput. Secur.* **2021**, *105*, 102248. [CrossRef]
5. World Economic Forum. *COVID-19 Risks Outlook: A Preliminary Mapping and Its Implications*; The World Economic Forum: Geneva, Switzerland, 2020.
6. Toti, G.; Alipour, M.A. Computer Science Students' Perceptions of Emergency Remote Teaching: An Experience Report. *SN Comput. Sci.* **2021**, *2*, 378. [CrossRef] [PubMed]
7. DeWitt, P. This Is What Students Want Us to Know About Pandemic Learning. 3 May 2020. Available online: https://www.edweek.org/education/opinion-this-is-what-students-want-us-to-know-about-pandemic-learning/2020/05 (accessed on 19 October 2021).
8. Craigen, D.; Diakun-Thibault, N.; Purse, R. Defining cybersecurity. *Technol. Innov. Manag. Rev.* **2014**, *4*. [CrossRef]
9. ISO. ISO/IEC 27001. 2013. Available online: https://www.iso.org/standard/54534.html (accessed on 20 October 2021).
10. Byron, T. Safer Children in a Digital World the Report of the Byron Review. 2008. Available online: https://childcentre.info (accessed on 31 May 2020).
11. Grey, A. Cybersafety in Early Childhood Education. *Australas. J. Early Child.* **2011**, *36*, 77–81. [CrossRef]
12. Brandeis, L.; Warren, S. The right to privacy. *Harv. Law Rev.* **1890**, *4*, 193–220.
13. Westin, A.F. Privacy and freedom. *Wash. Lee Law Rev.* **1968**, *25*, 166–170.
14. Pidgeon, N.F.; Hood, C.; Jones, D.; Turner, B.; Gibson, R. Risk perception. In *Risk Analysis, Perception and Management: Royal Society Study Group*; Royal Society: London, UK, 1992; pp. 89–134.
15. e-Government Academy Foundation Company. *National Cyber Security Index*; e-Governance Academy Foundation: Tallinin, Estonia, 2021. Available online: https://ncsi.ega.ee/ncsi-index/?order=rank (accessed on 20 October 2021).
16. Finney, G. *Well Aware*; Greenleaf Book Group LLC: Austin, TX, USA, 2020.
17. Oliver Wyman Forum. Cyber Risk Literacy and Education Index. 2021. Available online: https://www.oliverwymanforum.com/cyber-risk/cyber-risk-literacy-education-index/methodology.html (accessed on 28 August 2021).

18. Grant, K.; Gedeon, S. The Impact of COVID-19 on University Teaching. In *The University of the Future-Responding to COVID-19*; ACPIL: Reading, UK, 2020; p. 161.
19. Robinson-Neal, A. Reflections on Educational Practice: COVID-19 Influences. *Acad. Lett.* **2021**. [CrossRef]
20. Mai, P.T.; Tick, A. Cyber Security Awareness and Behavior of Youth in Smartphone Usage: A Comparative Study between University Students in Hungary and Vietnam. *Acta Polytech. Hung.* **2021**, *18*, 67–89. [CrossRef]
21. Zwilling, M.; Klien, G.; Lesjak, D.; Wiechetek, Ł.; Çetin, F.; Basim, H.N. Cyber Security Awareness, Knowledge and Behaviour: A Comparative Study. *J. Comput. Inf. Syst.* **2020**, 1–16. [CrossRef]
22. Mawgoud, A.A.; Taha, M.H.N.; Khalifa, N.E.M.; Loey, M. Cyber Security Risks in MENA Region: Threats, Challenges and Countermeasures. In Proceedings of the International Conference on Advanced Intelligent Systems, Marrakech, Morocco, 8–11 July 2019.
23. Lesjak, D.; Zwilling, M.; Klein, G. Cyber Crime and Cyber Security awareness among Students: A Comparative Study in Israel and Slovenia. *Issues Inf. Syst.* **2019**, *20*, 80–87.
24. Adams, A.; Cox, L. Questionnaires, in-depth interviews and focus groups. In *Research Methods for Human Computer Interaction*; Cambridge University Press: Cambridge, UK, 2008; pp. 17–34.
25. Taber, K.S. The Use of Cronbach's Alpha When Developing and Reporting Research Instruments in Science Education. *Res. Sci. Educ.* **2018**, *48*, 273–1296. [CrossRef]
26. Cortina, J.M. What is coefficient alpha? An examination of theory and applications. *J. Appl. Psychol.* **1993**, *78*, 98–104. [CrossRef]
27. Alexei, A.; Alexei, A. Cyber security threat analysis in higher education. *Int. J. Sci. Technol. Res.* **2021**, *10*, 128–133.
28. Shabe, T.; Kritzinger, E.; Loock, M. Scorecard Approach for Cyber-Security Awareness. In *Natural Computing Series*; Huang, T., Lau, R., Huang, Y., Spaniol, M., Yuen, C., Eds.; Springer: New York, NY, USA, 2017; pp. 144–153.
29. Dlamini, I.; Taute, B.; Radebe, J. Framework for an African Policy Towards Creating Cyber Security Awareness. In Proceedings of the Southern African Cyber Security Awareness Workshop (SACSAW) 2011, Gaborone, Botswana, 12 May 2011.
30. Tick, A. Evaluating e-learning acceptance and usage motivation including IT Security Awareness amid Z generation Hungarian students with xTAM. In Proceedings of the 2019 IEEE 23rd International Conference on Intelligent Engineering Systems (INES), Gödöllő, Hungary, 25–27 July 2019.
31. Tick, A. IT Security as a Special Awareness at the Analysis of the Digital/E-Learning Acceptance Strategies of the Early Z Generation. In Proceedings of the 2018 IEEE 22nd International Conference on Intelligent Engineering Systems (INES), Las Palmas, Spain, 21–23 June 2018.
32. Moallem, A. Cyber Security Awareness Among College Students. In *Advances in Human Factors in Cybersecurity*; Ahram, T., Nicholson, D., Eds.; Springer: Cham, Germany, 2019.
33. Cranfield, D.J.; Venter, I.M.; Blignaut, R.J.; Renaud, K. Smartphone security awareness, perceptions and practices: A welsh higher education case study. In Proceedings of the 4th International Technology, Education and Development Conference, Valencia, Spain, 8–10 March 2020.
34. Venter, I.M.; Daniels, A.D. Towards bridging the digital divide: The complexities of theSsouth African story. In Proceedings of the 14th Annual International Technology, Education and Development Conference INTED2020, Valencia, Spain, 2–4 March 2020.
35. Venter, I.M.; Blignaut, R.J.; Renaud, K.V.; Venter, M.A. Cyber security education is as essential as "the three R's". *Heliyon* **2019**, *5*, e02855. [CrossRef] [PubMed]