Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (P) Vol.11 No.2, 2022, pp.33-38
© The Research Publication, www.trp.org.in
DOI: https://doi.org/10.51983/ajcst-2022.11.2.3450

Digital Education: The Cybersecurity Challenges in the Online Classroom (2019-2020)

Kamal Aldin Yousif Yaseen
Department of Information System, CEMIS College, University of Nizwa, Nizwa, Oman
E-mail: k.yousif@unizwa.edu.om

(Received 23 September 2022; Revised 12 October 2022; Accepted 31 October 2022; Available online 10 November 2022)

Abstract - **E-learning or digital education is one of the advantages provided by the information revolution, which covered all fields and did not exclude the education sector, as many platforms and applications that provide distance education services were available. Students, professors, and education departments have multiple options to manage the educational and academic process. However, with all these positive advantages, this type of education entailed great risks related to cybersecurity much related research says that the education sector has the greatest percentage of attacks and threats denial of service, ransomware, and phishing attacks. This paper studies and analyses those risks using the Kaspersky DDoS Intelligence System. A part of Kaspersky DDoS Protection and explain the methods of protection for educational institutions.**

Keywords: **E-Learning, Cybersecurity, Online Classrooms, Platforms, Risks, LMS**

I. INTRODUCTION

One of the greatest innovations that this era is witnessing is the information revolution and its technologies, which included all fields with its multiple benefits. The education sector got its abundant fortune from these innovations, as it developed in its methods, techniques, and content. A group of digital platforms made it easy for the student, the teacher, and the educational material to meet in one place, and this is considered one of the most important types and patterns of education that we live in these days[1]. However, the risks of cybersecurity through the use of these platforms have increased and their ways and impact have diversified, just as the impact of various threats on the environment of multiple platforms has remained a question that haunts all educational institutions, especially during the recent COVID 19 pandemic, in which the demand for using educational platforms increased, and then after the COVID 19 pandemic era, they became These institutions are unwilling to continue using these platforms because of their great influence and advantages that have made education an attractive sector for, all immediate indications indicate that we are in the era of synchronous digital education, but we must address the cybersecurity problems that threaten its continuity and ensure the safety of its workers and beneficiaries from students, teachers, assistant administrative staff, and an educational environment in order to ensure the safety of these platforms for more than a two billion learners and professors around the world [2], [3].

II. METHODOLOGY

This paper deals with the different risks that threaten the security of electronic platforms from malicious programs, such as denial of service attacks, spam messages, phishing techniques, scams, and cross-border attacks, by analysing and providing tips and advice based on Kaspersky DDOS intelligence system tools to combat denial-of-service attacks.

III. OBJECTIVES OF THE STUDY

Previously, many serious scientific pieces of research were conducted regarding the importance of cybersecurity in the education sector, especially, but only a few of them focused on the policies and standards that must be applied in the online classroom security issues so that these institutions can overcome the danger of many threats and risks. Hence, this study focuses on policies, standards, and measures. And the instructions to be followed in the various education institutions. In this study, the risks and challenges were discussed, as well as the importance of imposing policies and standards to protect the e-learning activities.

IV. ONLINE LEARNING THREATS

Various threats are exposed to e-learning platforms today, as I mentioned earlier, most of the studies in this field agree that these platforms are very important and must be protected from these risks, and that the education sector represented by these platforms is witnessing escalating and innovative attacks. Below we mention the most important of these platforms [5].

A. Moodle: It is considered one of the most popular education management platforms (LMS). It is used by teachers to manage educational content, design tasks, activities, courses, and tests, with the feature of building a question bank.

B. Blackboard: It's another popular (LMS) provides an integrated learning environment where teachers can create activities, courses and tests, also provides video conferences, meetings and virtual classrooms.

C. Zoom: A commonly used collaboration tool, as its importance emerged during the COVID19 pandemic, as many teachers were able to create courses, conferences, meetings, and virtual classes.

D. Google Classroom: A web service designed spatially for digital education , as its importance emerged during the COVID19 pandemic, as many teachers were able to create courses, conferences, meetings, and virtual classes.

E. Coursera: It's the famous educational platforms, as it provides integrated digital education that includes distance education and virtual classes in various scientific courses

F. edX: The platform provides many open courses around the world.

G. Google Meet: Provides a video communication, conferencing service, which is similar to Zoom, through which lessons and meetings can be done.

V. DISCUSSION AND RESULTS

A. Distributed Denial of Service (DDoS)

By using Kaspersky DDOS intelligence system, the system intercepts and analyses commands and network traffic received by bots and command servers and controls the system proactively and not interactively, which means that it does not affect even infecting a device or executing an order. Each unique target represents a specific IP address that is being attacked. This paper discusses and reviews the percentage of DoS attack attacks that affected educational resources out of the total number of attacks of this type by Kaspersky DDOS intelligence system in the period from Q1 2019 to Q1 2020 Key Findings The number of DOS attacks affecting educational resources increased by 550% in January 2020 compared to January 2019[6], [7].

We find that for each of the months from February to June, the number of DDoS attacks affecting educational resources out of the total number of attacks was 350-500% greater in 2020 than in the corresponding month of 2019. From January to June 2020, the total number of users in the education sector who encountered various threats hidden under the guise of e-learning platforms reached 168,550, an increase of 20.5% compared to the same period in 2019. It also notes that from January to June 2020, the most used main platform was the Zoom platform, where 5% of users faced various challenges, as the second most used platform was Moodle.

The threat programs that were encountered in the year 2020 were malicious programs, downloading files, advertising programs, and unwanted mail messages. The various technologies, especially the security system under study, succeeded in confronting them with a rate of more than 98% of the total recorded infection attempts, along with Trojan horses and computer worms. As for threats Distributed under the guise of educational platforms for virtual classes, in 2020 the highest infection rate was recorded in Russia, as the number of hacking attempts reached (59 attempts per 1000 users). Followed by Germany (39 infection attempts 1000 users) [8], [9].

B. Phishing Risks

Phishing Risks with regard to e-learning platforms and video conferencing applications, phishing, which is one of the oldest and most famous forms of electronic crimes, operates in these platforms to a small extent in proportion to increasing awareness and awareness in the education sector. In the matter of securing these platforms, care must be taken. Due to the increase in the number of domains registered and linked to the Zoom platform, it has been registered 2449 domains 32 from it is harmful,320 suspicious domains Suspicious domains covered all educational platforms such as Microsoft teams and google meet, users who access phishing pages are often tricked into clicking on URLs that download malware, Or they may be tricked into entering or verifying login data, which puts this information at the service of cybercriminals [10].

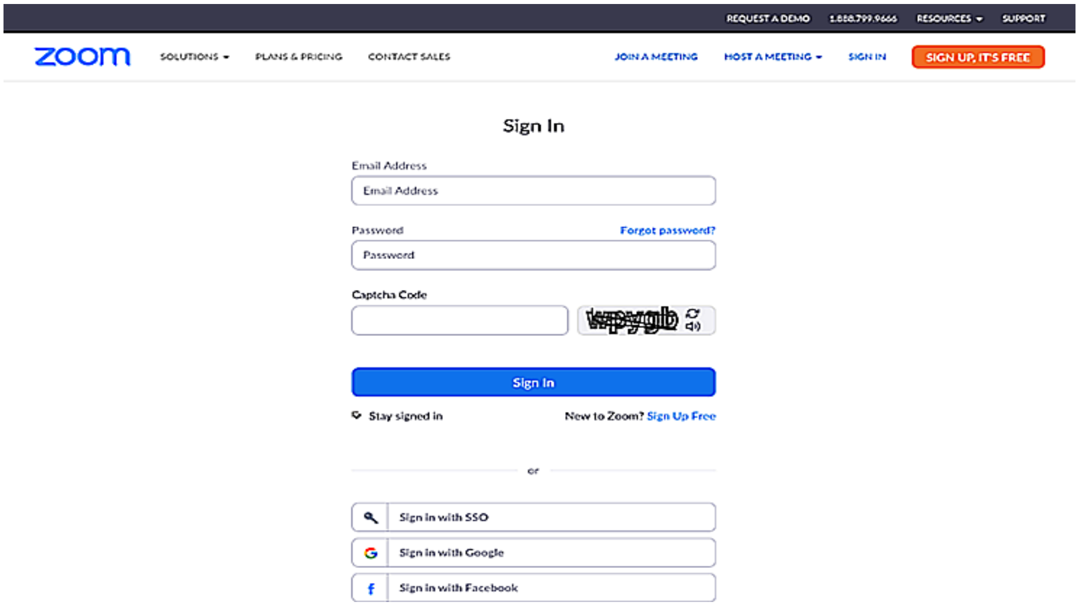
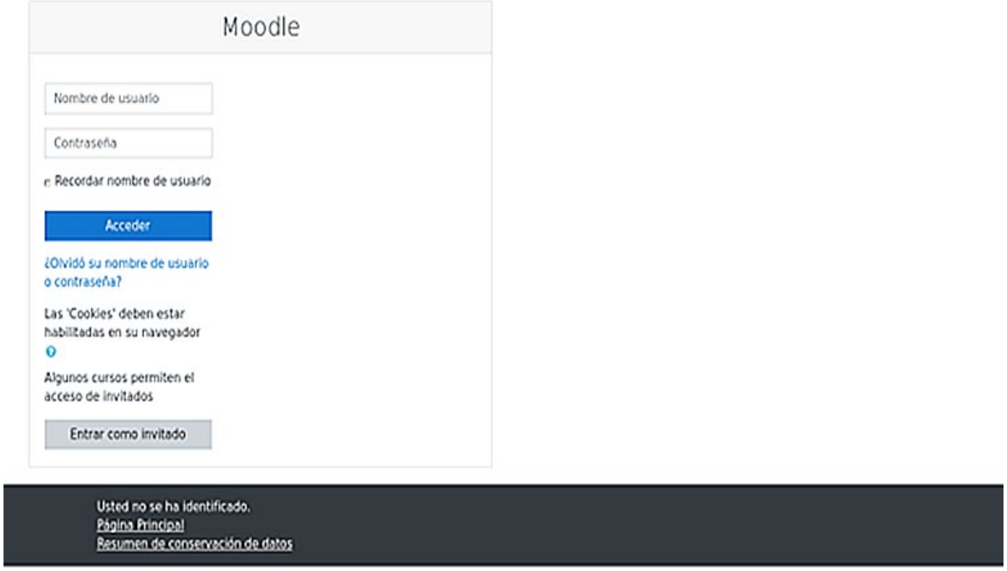


Fig. 1 Fake login page for Zoom



Moodle

Nombre de usuario

Contraseña

Recordar nombre de usuario

Acceder

¿Olvidó su nombre de usuario o contraseña?

Las 'Cookies' deben estar habilitadas en su navegador

Algunos cursos permiten el acceso de invitados

Entrar como invitado

Usted no se ha identificado.
Página Principal
Resumen de conservación de datos

Fig. 2 Fake login page for Moodle

Criminals may keep the data of students and professors for a long time and may use this data to attack others or harm the victims or threaten the integrity of the institution's data or change the settings of the network devices used to manage the educational process. This information may also be used in email attacks or requesting money and all more Information about future victims

Most universities have their own platforms where their dogs and professors can log in to access important resources related to the educational process and various academic services. In the previous year, an attacker created a fake page that seemed to belong to a real university and set up fraud nets for students and caused severe damage to the reputation of that university and damage to student data .Aside from the fake pages that are on the rise, in the previous year alone, cybercriminals managed to send over 300 million messages booby-trapped or containing malicious content to students, telling them that they had missed an important meeting, lecture, class, or workshop and that it was time to activate. Of course, if students respond to these messages, they may be exposed to many risks, the least of which may be losing their ability to use these accounts again, or they may be asked to pay a ransom to restore their accounts [11].

C. The Cyber Threats of Online Learning Platforms

One of the common methods is the distribution of disguised electronic attacks in the form of applications for video meetings, platforms for training courses, registration for courses, or even for different universities, and here we find that most of the threats appear to be legitimate programs or applications 7% of students' time is usually wasted in such fake applications, even if It did not affect their files, as it affects their time and academic achievement, in this way, these student users end up unintentionally on pages that do not belong to their scientific institutions, and then they are exposed to a flood of malicious programs and advertisements, and they enter into a maze that wastes their effort, time and focus. There are other deception methods that use e-mail etc. [12].

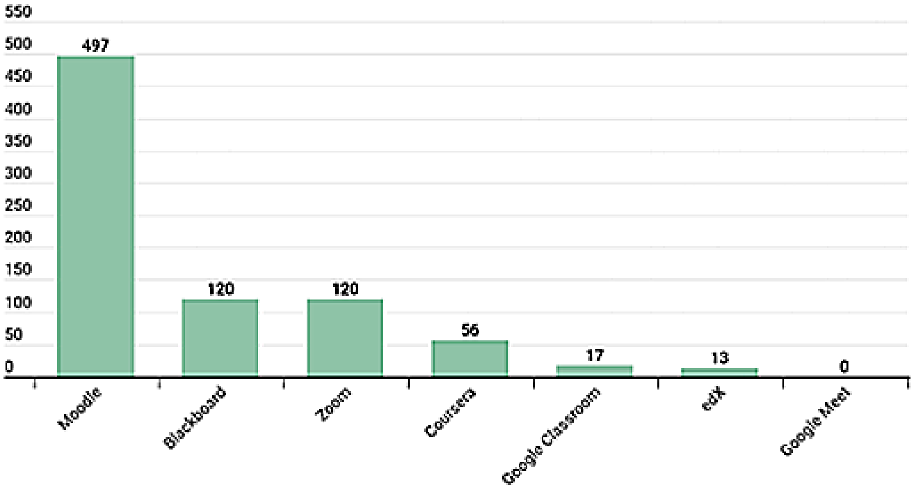


Fig. 3 The number of unique users that encountered various threats disguised as popular online learning/video conferencing platforms, January-June 2019

Hence, we find that the institutions that were attacked in the first quarter of the year 2019, a unit of 820 institutions, and that the technologies used to protect them failed by 31%, due to the lack of activation of a security policy that can deal with this type of attack.

Most of the attacks focused in the first half of the year 2020 on the Moodle platform, and then Blackboard and Zoom came in the second and third places, respectively, with neglect and failure to follow the necessary measures. The number jumped at the end of the year to 168,550 attacks on various platforms and using various types of attacks and tricks, which means an increase from the beginning year by 21%.

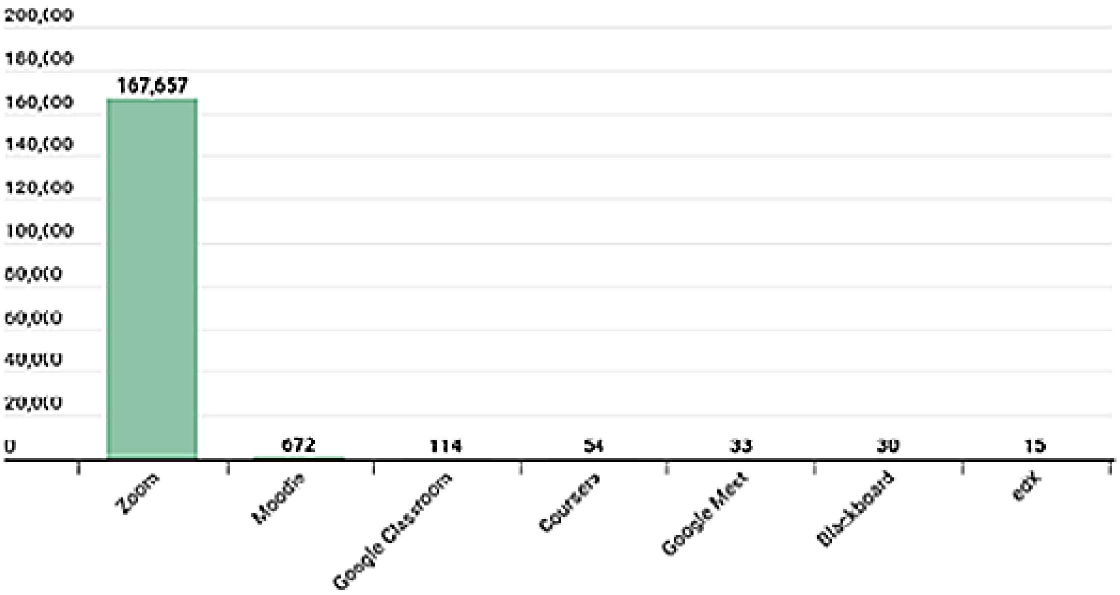


Fig. 4 The number of unique users that encountered various threats disguised as popular online learning/ video conferencing platforms, January-June 2020

Zoom was the most popular platform among other platforms as a lure far and away, as 99.5% of users encountered various threats disguised under its name. It was on the Zoom platform in the year 2019, as the company announced in April of the year 2020 that it had 300 million participants in meetings per day, given the privacy of that period, Covid 19, and given its energy popularity, it is logical that it would be exposed to all these attacks, which exposes its employees to great risks, in addition to millions looking forward To the system to the platform, and I am writing this paper at the beginning of the year 2023, the number of users of the Zoom platform has exceeded 300 million users, which has increased the company's responsibility in securing and protecting the privacy of all this number of users.

By far the most common threats distributed under the guise of legitimate video conferencing/online learning platforms were not-a-virus (99%). Not-a-virus files are typically divided into two categories: riskware and adware. Adware bombards users with unwanted ads, while riskware consists of various files – from browser bars and download managers to remote administration tools – that may carry out various actions on your computer without your consent.

About 1% of the infection attempts were about different families of Trojan horses, and this method is considered old, and the other part was malicious files that allow cybercriminals to carry out a number of malicious activities on the victim's device, such as file deletion, stealing passwords, bank card numbers, hiding data, and other activities This is in addition to other attacks that use backdoors to hide the nature of their work and then withdraw when they store what they want. Backdoors are dangerous in that they enable hackers to exploit various vulnerabilities on the organization's device or network [13].

In April of the year 2020, some digital hackers were able to penetrate the website of a large Turkish university by forcing it to disconnect from the Internet for more than forty minutes after it was subjected to a distributed denial-of-service attack. There are many examples of this type of attack in different countries of the world, which negatively affects the reputation and performance of educational institutions of a larger trend that began after schools were forced to transition to emergency remote learning: the rise of DDoS attacks against the education sector.

In general, the total number of DDoS attacks increased globally by 80% for Q1 2020 when compared to Q1 2019. And a large portion of that increase can be attributed to the growing number of attacks against distance e-learning services.

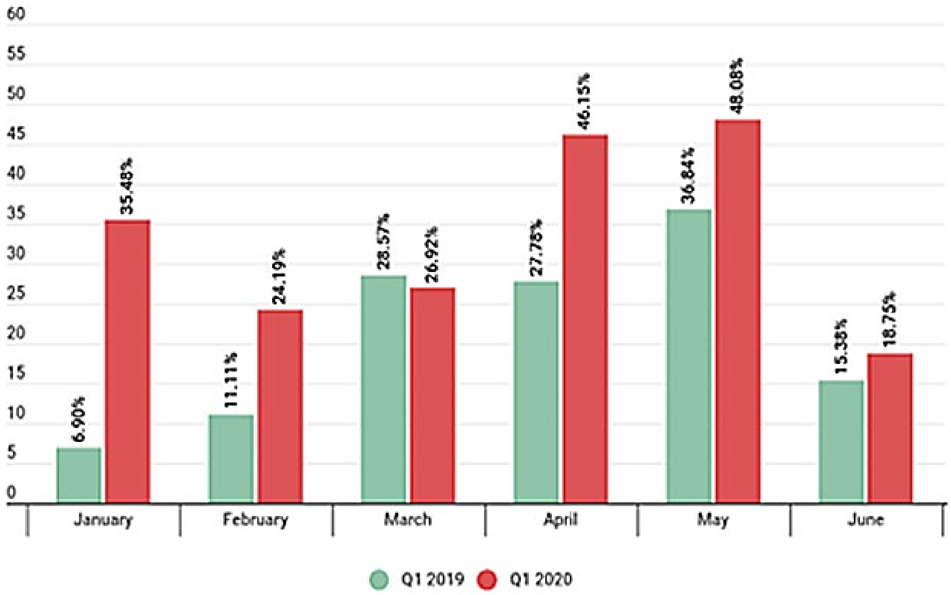


Fig. 5 Percent of the total number of DDoS attacks that affected educational resources: Q1 2019 vs Q1 2020

When compared to Q1 2019, the percentage of DDoS attacks affecting educational resources out of all DDoS attacks increased steadily for each month of Q2 2020 (with the exception of March). When looking at the total number of DDoS attacks that occurred between January and June 2020, the number of DDoS attacks affecting educational resources increased by at least 350% when compared to the corresponding month in 2019 [14].

V. CONCLUSION

As we are witnessing the beginnings of the year 2023, I do not agree with the opinion of many who believe that education via the Internet is an immediate response to the harmful conditions that swept the world in previous periods, and he stressed that the future is for this interactive style of education, and we find today that many educational institutions have preserved it and are even studying it In addition, this new pattern must be avoided because it targeted a new group of students who were not able to complete their education in previous stages, or between them and the traditional education difficulties. The cybersecurity risks continue to grow in popularity, cybercriminals will attempt to exploit this fact for their own gain. That means educational organizations will continue to face a growing number of cyber risks – into this fall and beyond. Fortunately, engaging and secure online academic experiences are possible. Educational institutions just need to review their cybersecurity programs and adopt appropriate measures to better secure their online learning environments and resources.

The security problems in e-learning platforms did not start with the COVID19, and it will not end with its end. There are other problems faced by educational institutions, which are weaknesses in availability and accessibility policies, internal problems related to infrastructure, protection system, such as adjusting firewalls settings, and external problems related to domain names system and hosting, where all these problems must be addressed by following strong and flexible security policies that understands accidents at the time of their occurrence and even predicts them. This paper has contributed to all of this and spread the necessary awareness to confront the various challenges of cybersecurity.

ACKNOWLEDGMENT

I would like to thank Kaspersky security for the very important report that has been issued during COVID-19 crises. It was vital to support this paper, the university of Nizwa for providing a good research environment, and my students and colleagues.

REFERENCES

[1] A. V. Herrera, M. Ron, and C. Rabadão, "National cyber-security policies oriented to BYOD (bring your own device): Systematic review," *in Proc. 2017 12th Iberian Conference on Information Systems and Technologies (CISTI),* pp. 1-4, 2017.

[2] F. Mishna *et al.,* "Interventions to prevent and reduce cyber abuse of youth: A systematic review," *Research on Social Work Practice,* Vol. 21, No. 1, pp. 5-14, 2011.

[3] H. F. Lokman, N. Nasri, and F. Khalid, "The effectiveness of using the Twitter application in teaching pedagogy: A meta-synthesis study," *International Journal of Academic Research in Progressive Education and Development,* Vol. 8, No. 2, pp. 205-212, 2019.

[4] Oxford University Press, *Oxford Online Dictionary,* Oxford: Oxford University Press, 2014, [Online]. Available: http://www.oxforddictionaries.com/definition/english/Cybersecurity.

[5] DHS, *A glossary of common cybersecurity terminology,* National Initiative for Cybersecurity Careers and Studies: Department of Homeland Security, 2014. [Online]. Available: http://niccs.uscert.gov/glossary.

[6] H. Ho. Park, "A Study on Cyber Crime Deterrence Recognition: The Influence of Recognition of Punishment for Cyber Crime on Intention to Report Crime," *Korean Criminal Psychology Research,* Vol. 16, pp. 85-98, 2020, DOI: https://doi.org/10.25277/KCPR.2020.16.4.85.

[7] A. Goswami, "Impact of Cyber Security in Different Application of E-Governance," *Journal of Advances and Scholarly Researches in Allied Education,* Vol. 15, pp. 65-70, 2018, DOI: https://doi.org/10.29070/15/57309.

[8] M. Rademaker, "Assessing Cyber Security 2015," *Information & Security: An International Journal,* Vol. 34, pp. 93-104, 2016, DOI: https://doi.org/10.11610/isij.3407.

[9] A. Robins, "The Ongoing Challenges of Computer Science Education Research," *Computer Science Education,* Vol. 25, pp. 115-119, 2015, DOI: https://doi.org/10.1080/08993408.2015.1034350.

[10] S. Hart, M. Andrea, P. Federica and S. Vladimiro, "Risk: A Serious Game for Cyber Security Awareness and Education," *Computers & Security,* Vol. 95, Article ID: 101827, 2020, DOI: https://doi.org/10.1016/j.cose.2020.101827.

[11] S. Negi and M. Sunita, "Effectiveness of Cyber Bullying Sensitization Program (CBSP) to Reduce Cyber Bullying Behavior among Middle School Children," *International Journal of Cyber Research and Education,* Vol. 1, Article No. 5, 2019, DOI: https://doi.org/10.4018/IJCRE.2019010105.

[12] W. Trappe and J. Straub, "Journal of Cybersecurity and Privacy: A New Open Access Journal," *Journal of Cybersecurity and Privacy,* Vol. 1, pp. 1-3, 2021, DOI: https://doi.org/10.3390/cybersecurity1010001.

[13] M. Keith, "Cyber Security Education, Qualifications and Training," *In: Holloway, R., Ed., Engineering & Technology Reference, Institution of Engineering and Technology,* London, pp. 1-11, 2015, DOI: https://doi.org/10.1049/etr.2014.0029.

[14] *Digital Education: The Cyberrisks of the Online Classroom,* Securelist.