Article

Avoidance of Cybersecurity Threats with the Deployment of a Web-Based Blockchain-Enabled Cybersecurity Awareness System

Abdul Razaque ^{1,*}, Abrar Al Ajlan ², Noussaiba Melaoune ³, Munif Alotaibi ⁴ , Bandar Alotaibi ^{5,6} ,
Issabekov Dias ¹ , Ammar Oad ^{7,*} , Salim Hariri ⁸ and Chenglin Zhao ⁷

- ¹ Department of Computer Engineering and Cybersecurity, International Information Technology University, Almaty 050000, Kazakhstan; diassss178@gmail.com
- ² Self-Development Skills Department, Common First Year Deanship, King Saud University, Riyadh 12211, Saudi Arabia; aalajlan1@ksu.edu.sa
- ³ Department of Computer Science and Information Technology, Mohammed V University in Rabat, Rabat 10170, Morocco; noussaiba.melaouene@um5s.net.ma
- ⁴ Department of Computer Science, Shaqra University, Shaqra 11961, Saudi Arabia; munif@su.edu.sa
- ⁵ Department of Information Technology, University of Tabuk, Tabuk 47731, Saudi Arabia; b-alotaibi@ut.edu.sa
- ⁶ Sensor Networks and Cellular Systems (SNCS) Research Center, University of Tabuk, Tabuk 47731, Saudi Arabia
- ⁷ Faculty of Information Engineering, Shaoyang University, Shaoyang 422000, China; iecsyu@hnsyu.edu.cn
- ⁸ Department of Electronics and Computer Engineering, University of Arizona, Tucson, AZ 85721, USA; hariri@email.arizona.edu
- * Correspondence: a.razaque@iitu.edu.kz (A.R.); ammar.oad@hnsyu.edu.cn (A.O.)

Citation: Razaque, A.; Al Ajlan, A.; Melaoune, N.; Alotaibi, M.; Alotaibi, B.; Dias, I.; Oad, A.; Hariri, S.; Zhao, C. Avoidance of Cybersecurity Threats with the Deployment of a Web-Based Blockchain-Enabled Cybersecurity Awareness System. *Appl. Sci.* **2021**, *11*, 7880. <https://doi.org/10.3390/app11177880>

Academic Editor: Tiago M. Fernández-Caramés

Received: 3 July 2021

Accepted: 22 August 2021

Published: 26 August 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Abstract: Modern information technology (IT) is well developed, and almost everyone uses the features of IT and services within the Internet. However, people are being affected due to cybersecurity threats. People can adhere to the recommended cybersecurity guidelines, rules, adopted standards, and cybercrime preventive measures to largely mitigate these threats. The ignorance of or lack of cybersecurity knowledge also causes a critical problem regarding confidentiality and privacy. It is not possible to fully avoid cybercrimes that often lead to sufficient business losses and spread forbidden themes (disgust, extremism, child porn, etc.). Therefore, to reduce the risk of cybercrimes, a web-based Blockchain-enabled cybersecurity awareness program (WBCA) process is introduced in this paper. The proposed WBCA trains users to improve their security skills. The proposed program helps with understanding the common behaviors of cybercriminals and improves user knowledge of cybersecurity hygiene, best cybersecurity practices, modern cybersecurity vulnerabilities, and trends. Furthermore, the proposed WBCA uses Blockchain technology to protect the program from potential threats. The proposed program is validated and tested using real-world cybersecurity topics with real users and cybersecurity experts. We anticipate that the proposed program can be extended to other domains, such as national or corporate courses, to increase the cybersecurity awareness level of users. A CentOS-based virtual private server is deployed for testing the proposed WBCA to determine its effectiveness. Finally, WBCA is also compared with other state-of-the-art web-based programs designed for cybersecurity awareness.

Keywords: information security; cybercrime; cyber awareness; cybersecurity basics; cybersecurity hygiene; blockchain technology

1. Introduction

With the spread of digitalization and the Internet of Things, information security is increasingly enmeshed in many aspects of our society [1]. Digital information not only offers advantages but also creates security threats. In handling these threats, cybersecurity is of paramount significance because it provides defensive methods to detect the potential

intimidations [2]. However, the majority of the defensive methods are not very effective. Additionally, individuals have tunnel vision regarding information security basics, and they do not know much about other ways to consider and improve cybersecurity awareness. Despite the level of spending, public awareness, and readiness in certain fields, most users do not yet think of computer security as anything but a nuisance [3]. Cybercriminals try to access personal and private information that poses a threat to privacy and confidentiality [4]. Cybercrime can be regarded as computer-mediated activities that are either illegal or considered illicit by certain parties, and these activities can be conducted through global networks [5]. Therefore, the main question is whether it is possible to avoid any cybercrime by knowing the basics of cybersecurity in the mainstream. As modern technologies are used everywhere globally and by almost everyone on the Internet, this issue affects all of them. Cybercrime is switching its battleground from desktops to other platforms, including mobile phones, tablet computers, and VoIPs [6]. This includes stealing, such as by capturing everything people type, including passwords, bank accounts, and credit card numbers [7]. Cyber fraud, stealing, phishing, and other malicious behaviors will enrich the terminology of cybercrime in the years ahead [8]. It is not sufficient to only follow the recommended cybersecurity standards, rules, and anti-cybercrime actions to avoid cybercrimes. There are obvious risks caused by this problem, such as large business losses and the dispersion of prohibited themes, such as cultural and racial hate, violence, child porn, and cyberterrorism. Currently, cybercrime has emerged as the biggest threat to the computer information technology (IT) industry that has taken shape [9]. Security is being employed in different organizations to protect their assets, but it does not fully provide safeguards [10]. As an increasing number of users and businesses use emerging technologies, awareness is becoming one of the most predominant issues [11]. Some cybercriminals are interested in gaining financial access, whereas others seek to get consumer information or intellectual property, harm an organization's reputation, or release a political declaration through "hacktivism" [12]. The question is whether the fight against cybercriminals can be won or lost. The answer is to depend on individuals' current cybersecurity knowledge about protecting against cybercrimes so that businesses can be more resistant to cybersecurity attacks. Even if law enforcement reduces the rate of cybercrimes, the issue is to avoid them entirely [13]. A lack of structural stability and continuity within an organization may interrupt efforts to efficiently address the issue of online crime [14]. The government has also made considerable efforts to educate consumers regarding the risks of identity crime, especially the forms that occur online [15,16]. Individuals can also be protected from cybercriminals with the advantages of existing laws [17]. However, this disintermediation of the news process runs counter to the construction of the imagery surrounding cybercrime, which originated in the days before the Internet when the mass media was organized more centrally [16]. It is predicted that a 25% increase in identity theft until 2027 will cause a \$40.62 billion loss [18]. Figure 1 shows the effect of cybercrime that leads to payment fraud. As mentioned, cybersecurity awareness plays a vital role in fighting against cybercriminals. Thus, in realizing cybersecurity awareness, the following should be considered: (a) determining the various security topics and programs available for cybersecurity training, (b) investigating common mistakes in human behavior, and (c) determining the methods by which cybercriminals act. We are working to address these problems and use these solutions to protect individuals from cybercrimes.

Figure 1. Statistics of payment fraud.

The human factor is one of the major weak points in the information security of any organization. Increasing cybersecurity awareness among people is very important. However, existing methods face several challenging difficulties, such as depending on content that is outdated, not being attractive to people, people forgetting what they learned, being time-consuming, not being consistent, and facing potential security threats. Thus, effective cybersecurity awareness requires more than simply telling the person about what he or she needs to do and not do [19].

Moreover, there is a need for robust and efficient solutions, such as the advanced system model that can assess and increase the users' cybersecurity awareness levels. The system should be secured. Thus, we propose a blockchain-enabled approach that consists of several program modules to increase the cybersecurity awareness levels of users.

1.1. Research Problem

The very extensive and difficult problem at hand is a lack of knowledge regarding information security basics, and its significance will become increasingly relevant as new technologies are developed. For instance, in the future, people will use modern technologies, and in parallel, the need for full protection of these technologies will grow. All global businesses, including large corporations and companies, will bring innovations to life. However, this is insufficient. Moreover, if the world needs good specialists for the development of these technologies (and there are very few), there will be an even greater need for cybersecurity specialists (especially those who protect the masses in such ways).

1.2. Research Importance

It is very important not only to know the basics of cybersecurity, but also to see the whole picture of cybercrime so as not to become another victim of cybercriminals. The point is that most types of cybercrime require an organization with execution as well as profitability [20]. In other words, knowledge is light, and ignorance is darkness. This problem also concerns information security. The varying attack types in existence illustrate how it is difficult to put any single exact, meaningful label on the size of the problem [21].

1.3. Possible Research Solutions

To reduce the risk of cybercrimes, the possible solutions to this problem are as follows:

- The study of common mistakes individuals make, which lead to them becoming the victims of cybercriminals, and taking advantage of these experiences;
- The development of a web-based program that will test for the common behaviors of cybercriminals;

- Monitoring the impact of cybercrime and giving a new view of cybercrimes by using the advantages of much cybersecurity information;
- The creation of more cybersecurity seminars and training programs about the cyber-crime world and cybersecurity hygiene;
- The analysis and usage of advice from cybersecurity professionals and modern cybersecurity trends to prevent cybercrimes.

However, the most feasible solution from an efficiency perspective is to train users with the developed web-based program, which tests their cyber awareness levels. This should be implemented as a Linux-based web server, which holds a program that determines the cybersecurity awareness of the users. Additionally, there should be deployed Blockchain technology to protect the program from potential threats.

1.4. Research Contributions and Assessment

The contributions of this work, which are motivated by the above challenges, are summarized as follows:

- The developed web-based program helps many people test and improve their cybersecurity awareness levels.
- The developed web-based program is guaranteed to determine the cybersecurity bottlenecks of the tested users.
- The program results can be analyzed to train the tested users on advanced cybersecurity topics to preserve their high cybersecurity awareness.
- Blockchain technology is used to protect the WBCA program from any potential malicious threats. As a result, only legitimate users can successfully be entertained.

The WBCA program is designed and developed on the Java platform to assess these contributions. It is tested on the CentOS-based virtual private server in Almaty, Kazakhstan. The proposed WBCA program consists of four modules to test the users' knowledge: (a) an initial knowledge check, (b) a lower cybersecurity awareness module, (c) an advanced knowledge-check module, and (d) a high cybersecurity awareness module. Furthermore, the WBCA program is secured using blockchain technology because the features of blockchain technology only allow legitimate users to access the program and block illegitimate users when they try to access the program.

1.5. Research Structure

The remainder of the paper is organized as follows. Section 2 presents the features of the existing literature. Section 3 presents the state-of-the-art system model. Section 4 presents the proposed cybersecurity awareness process. Section 5 presents the experimental results and provides the discussion of the results. Finally, the conclusion of the paper is presented in Section 6.

2. Related Work

In this section, the main characteristics of current approaches are deliberately discussed. The existing approaches can be categorized into general detection/prevention approaches and approaches based on emerging technologies, such as blockchain and artificial intelligence. The following Section 2.1 surveys the general detection/prevention approaches, whereas the approaches that utilize emerging technologies are surveyed in Section 2.2.

2.1. General Detection/Prevention Approaches

Nowadays, individuals employ various cybersecurity techniques to ensure that they are protected in cyberspace. One effective piece of technology utilized to mitigate cybercrimes is the point-of-sale device [22]. It protects individuals against malicious codes that trace Internet movements and enable attackers to obtain everything they type, including credit card information, bank account numbers, and passwords. Although this approach

can protect individuals from malicious software, this advantage can only be applied locally on personal computers. Moreover, the software is not free; individuals must pay to use it.

A solution called “law enforcement strike back” was proposed by Dreyfuss [23]. This solution recommends that law enforcement officials utilize “electronic sanctions” to act in response to cybercrime activities, such as spreading different types of malware, worms, viruses, hacking techniques, and denial-of-service attempts. Despite the advantages that this proposed method has to offer to decrease the cybercrime rate, there is still a small issue regarding the details that this solution provides. The author did not cover certain cybersecurity issues and actions to precisely prevent/mitigate cybercrimes.

Eskandari et al. [24] proposed an effective web browser-based method to protect users against malicious code. This solution is a decent attempt to provide security at the browser level. For instance, this technique can block malicious ActiveX code, Java, and JavaScript activities. Furthermore, there is a built-in capability to enable predefined selection of low, medium low, medium, or high security levels. Furthermore, most malicious web attacks can be detected through monitoring all the browsing activities. Nevertheless, this method does not address the technology utilized to recognize these attacks. Moreover, it cannot identify zero-day attacks, which creates a vulnerability for web browsers.

Pessim and Marcio [21] concentrated on scaling the types of varying cyberattacks. The main aim of this study was to expand the scale of issues linked to both the community and the cybercrimes. However, this kind of solution comes with a price, as scaling causes difficulty in resolving issues. Burlison et al. [25] introduced a theoretical resolution known as “the development of user education and victim support”. Their solution involves technical staff who are responsible for deleting malicious phishing information after observing the suspicious activities. This support does not accurately measure the entire affected rate.

Cascavilla et al. [26] introduced a method to mitigate the risk of being targeted. This method combats cybercrimes utilizing various businesses’ countermeasures. The authors introduced some prevention rules and corporate-level rules to combat cybercrimes. This approach enforces specific business countermeasures that might only be customizable to certain organizations or regions; thus, it lacks a worldwide scale.

Tsakalidis and Kostas [27] believe that profitability and organizations are the major factors behind the presence of cybercrime. Therefore, they think concentrating on these aspects would effectively prevent cybercrime. Other potential aspects that motivate cybercrimes were not discussed.

Newhouse et al. [20] recommended sticking to the suggestions provided in the NIST cybersecurity framework to mitigate cybercrimes. This framework assists companies and government institutions in recognizing, coordinating, and assessing cybersecurity risks. The NIST recommends that organizations should realize that with the revolution in information security and technological innovation, people must continue to keep up to date on developments, and key online security measures must also be made, implemented, maintained, and continuously developed. This framework is decent because it can help deploy cybersecurity management schemes to protect against or mitigate cybersecurity violation attempts. The main issue with this framework is the lack of providing technical methods to avoid cybercrimes.

George and Dorothy [12] suggested a solution to diminish “hacktivism”. The authors believe the motivations of cybercriminals can be summarized as financial gain, obtaining consumer information or intellectual property, destruction of an institution’s reputation, or using “hacktivism” to express a political statement. However, other local factors were not considered by the authors.

Senarak [28] analyzed cybercrime evolution. The author found that cybercrime will cause organizations to open an increasing number of jobs in the upcoming five years. It is a valuable idea to gather information to help researchers/industries to develop effective solutions to prevent these cybercrimes. However, the authors did not provide practical ways to prevent these attacks.

Individual awareness regarding various malicious behaviors is of paramount importance. Cybercrime behaviors, such as phishing, scamming, and malicious activities, will enhance the cybercrime concept in the years to come [29]. However, not all malicious behaviors have been covered in this article.

2.2. Approaches Based on Emerging Technologies

The authors of [30] proposed a deep learning-based solution to detect cybersecurity threats. The authors proved the effectiveness of their approach using experimental analysis. The proposed solution achieved promising results. However, similar approaches must be tested in real environments to prove their effectiveness.

The BLOCKchain-Based Platform for Healthcare Information Exchange (BlocHIE) was introduced in [31]. The security requirements (privacy and authentication in particular) were evaluated by analyzing healthcare data extracted from different sources. Based on the evaluation, the authors implemented a pair of loosely coupled blockchains to process heterogeneous healthcare data. The privacy and authentication requirements were further fulfilled by integrating on-chain verification and off-chain storage. To enhance the system fairness among users and the throughput, the authors also proposed two packing algorithms. This platform is a useful solution because it can provide both privacy and authenticity. However, the system throughput and fairness might decrease the effectiveness of the platform.

The fairness-based transaction packing algorithm was introduced in [32]. Based on theoretical analysis, the authors deduced that fairness is somehow associated with the sum of waiting times of chosen transactions. Thus, a mini-heap-based optimal algorithm was presented, and the time complexity of this algorithm was analyzed to prove its effectiveness. The proposed algorithm achieved superior results compared to existing solutions in terms of both transaction response time and fairness.

Jiang et al. [33] proposed a protocol utilizing a bloom filter and a multi-keyword search. The proposed solution is efficient and enhances privacy preservation. To carry out a multi-keyword search process, the bloom filter is used to choose a low-frequency keyword in order to be utilized to filter the database. This procedure would decrease the computational complexity because the algorithm chooses a low-frequency keyword, meaning most of the data will be excluded. Moreover, the authors proposed a technique known as pseudorandom tags to perform each search process in a single round.

3. System Model

This section presents a system scenario for calculating the information security awareness of users on the Internet and in network spaces. First, before we define the system model's components, we should know that cybercrime is a crime committed on the Internet, on networks, or even against stationary computers. The cybersecurity awareness web program is significant software among the growing information security trends. To prove the limitations of the lack of cybersecurity basics, the system model consists of four parts:

- An initial knowledge-check
- A lower cybersecurity awareness module
- An advanced knowledge check
- A high cybersecurity awareness module

The initial knowledge check module checks the information security basics known by the user. The lower cybersecurity awareness module is responsible for identifying the low awareness of the user and giving appropriate feedback for the user's bottlenecks. The advanced knowledge check module assesses the advanced information security basics possessed by the user. The high cybersecurity awareness module also identifies the high awareness of the user and gives appropriate feedback for the current user's bottlenecks.

These four parts work consecutively through logical examinations and result retrievals, as shown through the blocks and arrows in the dataflow diagram depicted in Figure 2. First, it is necessary to ensure that the user has good knowledge of information security, and the

program initially checks the current knowledge. If the user does not have this knowledge, then the situation is classified as “poor awareness” and the result is provided as “low cybersecurity awareness”. The next step is to check if the tested user has good knowledge. If the result is positive, the aggregation concludes that the user has excellent information security awareness (high cybersecurity awareness). Therefore, using this system model, we can determine the user’s cybersecurity awareness level. The system model realizes the need for increasing the cybersecurity awareness of users. If this model is implemented in the real world, the risks of cybercrimes can be minimized as users become more aware of information security basics. The use of a cybersecurity awareness web program not only ensures a high cybersecurity awareness level while testing users but also improves cybersecurity training efficiency.

Figure 2. The process of defining the cybersecurity awareness of the user.

4. Proposed Blockchain-Enabled Cybersecurity Awareness Process

This section shows the mechanism of how user knowledge is calculated in the field of information security in detail. The proposed WBCA consists of following processes.

- Counter Sorting Process
- Cybersecurity Awareness Assessment Process
- Blockchain-Enabled Susceptibility Detection Process

4.1. Counter Sorting Process

The proposed main components are used to calculate accurate results from the user’s replies, sort them, and arrange them so that the efficiency for each topic can be viewed. Each step defines the degree of aptitude that the user shows during testing on the web server. For this algorithm, we used the counting sort algorithm as a baseline sorting method to check the input entries of each user to assess their knowledge of cybersecurity. The counter sort approach is an efficient process for sorting an array of elements, each with a non-negative integer key mapped to the elements by some alphabet-to-numeric conversion scheme. It is a stable sorting technique that is used to sort objects according to keys that

are small numbers. It counts the number of keys whose key values match. This sorting method is effective when the difference between different keys is not large; otherwise, it can increase the complexity of the space. Thus, its time complexity is given by

$$T_c = O(n + r) \quad (1)$$

where T_c is the time complexity, $O(n + r)$ is the time function for measuring performance, n is the number of elements, and r is an element's degree.

At the same time, its spatial complexity is identical:

$$S_c = O(n + r) \quad (2)$$

where S_c is the space complexity.

The sorting process maps M the following input/output pairs:

$$M_{(I)} = \sum_{i=0}^{n-1} i \{A_{[0]} + A_{[n+1]} + \dots + A_{[n-1]}\} \quad (3)$$

where A is an array to be summed, and $M_{(I)}$ is the input mapping.

The process outputs a sorted permutation of A , called B , such that

$$M_{(O)} = \sum_{i=0}^{n+1} i \{B_{[0]} + B_{[n-1]} + \dots + B_{[n+1]}\} \quad (4)$$

where B is a sorted permutation of array A , and $M_{(O)}$ is the output mapping.

4.2. Cybersecurity Awareness Assessment Process

It comprises of a function with variables, and the function itself is based on the checking process for defining cybersecurity awareness. The function gives a positive output if and only if the following condition is true: The current cybersecurity knowledge is related to the good knowledge given by

$$F(x) = \forall x (x \in G_k \wedge x \notin B_k) \quad (5)$$

where x is the current cybersecurity knowledge, G_k is the good cybersecurity knowledge, and B_k is the bad cybersecurity knowledge.

In Algorithm 1, the process of defining cybersecurity awareness is shown.

Algorithm 1 Cybersecurity awareness assessment process

Input: C_K, B_K, G_K in

Output: G_k or B_K out

- 1: **Initialization:** $\{C_K$: Current knowledge; B_K : Bad knowledge; G_K : Good knowledge; A_l : Low cybersecurity awareness; A_h : High cybersecurity awareness;
 - 2: **Check** $C_K \in B_K$
 - 3: **if** $C_K \in B_K$ **then**
 - 4: **Show** A_l
 - 5: **Check** $C_K \in G_K$
 - 6: **end if**
 - 7: **if** $C_K \in G_K$ **then**
 - 8: **Show** A_h
 - 9: **end if**
 - 10: **if** $C_K \notin B_K$ and $C_K \notin G_K$ **then**
 - 11: **Show** A_l
 - 12: **end if**
-

In Algorithm 1, the cybersecurity awareness definition process is explained. In step 1, the variables are initialized to determine the process. At the beginning of the algorithm, the input and output processes are given to evaluating cybersecurity knowledge, respectively. Step 2 makes an initial check to see if the current cybersecurity knowledge is bad. Consequently, in step 4, the program shows the result as low knowledge. Next, steps 5–7 check if the current cybersecurity knowledge is good. Therefore, in steps 8–10, if the current cybersecurity knowledge is good, then the program outputs “high knowledge”. Finally, in step 11, the program determines whether the current information security basics are defined as neither good nor bad; it generally outputs this result as low knowledge by default. Using the results, it can be concluded that if the program outputs bad knowledge, it shows that the tested user has low cybersecurity awareness. Otherwise, the user has high cybersecurity awareness.

Let us define the cybercrime rate C_r of the user that can be calculated as it relates to current knowledge:

$$C_r = C_k \times 100\% \quad (6)$$

Next, the overall cybercrime risk is used to assess the user’s risk of being the victim of a cybercrime, which can be calculated by

$$R_c = \frac{C_r + G_k}{B_k} \quad (7)$$

where R_c is the overall cybercrime risk of the user.

On the other hand, the cybercrime delta between good cybersecurity knowledge and bad cybersecurity knowledge is shown in the following equation:

$$C_d = \frac{1}{G_k - B_k} \quad (8)$$

To calculate the inverse proportion of Equation (6), which is necessary to find the correct current knowledge, the equation is

$$\text{However, } C_k = \frac{C_r}{100\%} \quad (9)$$

Consequently, Equation (9) is simplified in this way, which is helpful for using only the current knowledge dependency:

$$R_c = \frac{C_k(G_k + 1)}{B_k \times 100\%} \quad (10)$$

Based on the essential steps explained in the Algorithm 2, it is necessary to use the modulus ponens of the cybersecurity awareness level. Therefore, the formula is as follows:

$$S_r = G_k \times 100\% \quad (11)$$

where S_r denotes a successful result of the program’s test.

In other words, if the results are positive, then the user has high cybersecurity awareness:

$$F(S_r) = \forall x((x \in G_k) \wedge (x \in S_r)) \quad (12)$$

Theorem 1. Suppose first that the user obtains good results from a web-based program. Consequently, the user has a good cybersecurity awareness G_k . Therefore, if the user has high cybersecurity awareness, then the risk of being the victim of cybercrimes is low R_l .

Proof. First, let us define the second instance of the theorem; thus, the following formula defines the high cybersecurity awareness as being inversely proportional to the risk of being a victim:

$$G_k = \frac{1}{R_l} \quad (13)$$

Consequently, we have two separate instances as follows. This is helpful for defining the bounds of the estimated program results:

$$(G_k + S_r)^u = \sum_{k=0}^n \binom{k}{u} \left(\frac{1}{R_l}\right)^k G_k^{u-k} \quad (14)$$

where u is the upper bound and k is the lower bound. Now, let us use the relative formula of good results and the sine equation for the first and second instances, which in turn should be used to check further graph data:

$$S_r = \frac{1}{R_l} \times \pi \quad (15)$$

$$\sin(S_r) = 2\pi \times \sin\frac{1}{2}(R_l) \quad (16)$$

As a result, Equation (15) squared together with the first instance is inversely proportional to low cybercrime risk (π is constant and removed from the formula), and the following equation is helpful for estimating the program results twice:

$$S_r^2 = \frac{1}{R_l^2} \quad (17)$$

Consequently, combining the equations of S_r and the sine of S_r make the sine-based view of the estimated results more accurate:

$$\sin\left(\frac{1}{R_l} \times \pi\right) = 2\pi \times \sin\frac{1}{2}(R_l) \quad (18)$$

Therefore, it is mathematically proven that if the user has good program results, then the risk of being the victim of cybercrimes is lower. $\square$

Corollary 1. *If the user has bad results from the web-based program, then their risk of being the victim of cybercrimes is high.*

Good cybersecurity basics are now substituted by poor cybersecurity basics. Therefore, we have the corresponding cosine version of the equation:

$$\cos\left(\frac{1}{R_l} \times \pi\right) = 2\pi \times \cos\frac{1}{2}(R_l) \quad (19)$$

Theorem 2. *If the user has high cybersecurity awareness H_s , then the user has a low chance of being the victim of cybercrimes L_c . However, the user has a high chance of being a victim of cybercrimes. Therefore, the user's cybersecurity awareness is low.*

Proof. First, the given instances of this theorem are shown below, which demonstrate that if there is any current knowledge, it belongs to the high awareness category:

$$F(L_c) = \forall C_k (C_k \in H_s) \quad (20)$$

where H_s is the user's high cybersecurity awareness and L_c denotes a low chance of being the victim of cybercrimes.

Next, assuming that the user has high cybersecurity awareness, let us integrate this assumption with Equation (20):

$$\int_0^{L_c} H_s^2 dH_s = \frac{L_c^3}{3} \quad (21)$$

Now let us use the conjunction of Equation (15) with the negation of H_s , which describes an integral part of high awareness between low chances and ordinary chances:

$$A(H_s) = \int_c^{L_c} (H_s) dH_s \quad (22)$$

Next, let us define the mean of the low risk and low chance situations through the integration of the function of H_s :

$$A(H_s) = \int_0^{R_l+L_c} f(H_s) dH_s = \frac{(R_l + L_c)^2}{2} \quad (23)$$

Finally, the conditional equations of the negation of H_s and its cosine function are obtained, so we have the functional result of the integral parts:

$$f(H_s) = \frac{A(H_s + L_c) - A(x)}{x} \quad (24)$$

As a result, the user has a high chance of being the victim of cybercrimes, and the user has low cybersecurity awareness. The theorem is proven. $\square$

Property 1. *Cyber awareness Nondualism—the cyber awareness score result is always a positive or negative number.*

For instance, if the final score of the web program shows bad cybersecurity knowledge, the output is a negative number. Otherwise, the program gives a positive number instead.

$$F(R_p) = \exists x((x \in G_k) \wedge (x \in B_k)) \quad (25)$$

where R_p is the web program result.

In conclusion, we observe that the results of the proposed WBCA deduce only two results: good cybersecurity knowledge or bad cybersecurity knowledge.

4.3. Blockchain-Enabled Susceptibility Detection Process

The Blockchain activates the distributed ledger by replacing the existing centralized ledger structure. It provides security using hash encryption and a public key cryptographic algorithm. Our proposed WBCA is deployed on the cloud. Therefore, it is a possibility that it is exposed due to the vulnerability of the cloud and have threats launched on the WBCA server by the attacker. The attacker can generate similar cybersecurity tasks using the same digital signature because double occurrence is possible. The attacker can make it realty if it has a robust hashing capability and generated a longer private chain as compared to public key cryptography to perform such events. The probability of the susceptibility detection P_{sd} is given by

$$P_{sd} = \left(\frac{x}{y}, 1\right)^{\max(y+1, 0)} \begin{cases} 1 & \text{if } \gamma < 0, x > y \\ \left(\frac{x}{y}\right)^{y+1} & \text{if } \gamma \geq 0, x \leq y \end{cases}$$

where x, y are hash parameters of the legitimate user and attacker, respectively. γ is the number of the blocks used by the WBCA program that provides an edge over the attacker.

If γ turns positive, then the proposed WBCA program is capable of sending the blocks and overtaking the illegitimate users. The Blockchain-enabled susceptibility detection model for WBCA is shown in Figure 3. The WBCA server can transmit the data using

Blockchain-enabled technology to restrict the potential threats encountered by the attacker. The Blockchain susceptibility detection process is explained in Algorithm 2.

Figure 3. Blockchain-enabled susceptibility detection model for WBCA.

Algorithm 2 Blockchain susceptibility detection process of defining the user's vulnerability

Input: C_U, I_U, R_U in

Output: C_p or C_r out

- 1: **Initialization:** $\{C_U$: Current user; C_p : Cybercrime prone; C_r : Cybercrime resistant; I_U : Insecure user; R_U : Reliable user; $\}$
 - 2: **Check** $C_U \in I_U$
 - 3: **if** $C_U \in I_U$ **then**
 - 4: **Show** C_p
 - 5: **end if**
 - 6: **if** $C_U \in R_U$ **then**
 - 7: **Show** C_r
 - 8: **end if**
 - 9: **if** $C_U \notin R_U$ **then**
 - 10: **Show** C_p
 - 11: **end if**
-

Algorithm 2 shows the process of defining the user's cybercrime proneness. In step 1, the variables are initialized to determine the process. The input and output processes are given at the beginning of the algorithm, respectively. Steps 2–3 check if the current user is insecure or reliable. If he/she is insecure, then in steps 4–5, the program outputs that the user is cybercrime prone. Next, step 6 checks if the user is reliable, then in steps 7–8, the web program outputs that the user is cybercrime resistant. Finally, in steps 10–11, if the current user is defined neither as insecure nor reliable, the program outputs the result as an insecure user by default.

Corollary 2. *If the user has a high chance of being a victim of attacker, then the user has low cybersecurity protection measures. The given chances tend to the maximum. Therefore, the cybersecurity protection is low.*

Now, we have an integral function to assess the integral of low chances between high chances and ordinary chances:

$$B(L_s) = \int_c^{H_c} L_s dL_s \quad (26)$$

where H_c is a high chance of being a cybercrime victim and L_s represents low cybersecurity awareness. Therefore, the conditional function is the same as for the conditional equation, which again shows the functional result of the integral parts:

$$f(L_s) = \frac{B(L_s + H_c) - B(x)}{x} \quad (27)$$

Property 2. *Cyber awareness Non-idealism—the user’s cybersecurity threat detection capability level always tends toward an idealistic result but never reaches it. For example, suppose that the user has 100% cybersecurity threat detection capability. However, as cutting-edge technologies are developed, the person must always observe the new cybersecurity trends.*

$$F(C_{td}) = \nexists x (x \in (C_a \times 100\%)) \quad (28)$$

where C_{td} is the cybersecurity threat detection capability level.

Based on the Properties 1 and 2, a hypothesis is introduced.

Hypothesis 1. *If $C_{td} + R_p = S$, where S is the overall security level; x, y , and z are natural numbers; and x, y , and $z > 2$; then C_{td}, R_p , and S possess the common security criteria.*

Proof. To prove the hypothesis, let us introduce the entropy dependency of the input variables:

$$H(S^z) = H(C_a^x) + H(R_p^y) \quad (29)$$

where $H(S^z)$ is the entropy of the security level, $H(C_a^x)$ is the entropy of the cybersecurity threat detection capability level, and $H(R_p^y)$ is the entropy of the web program result. $\square$

This equation helps us obtain the hypothetical entropy results of the given variables.

As $H(S)$ is the logarithm of S and other entropies are the logarithms of their variables, Equation (29) gives the logarithmic form of these entropies:

$$\log_2 S^z = \log_2 C_a^x + \log_2 R_p^y \quad (30)$$

Now let us write the same equation in a shorter form:

$$\log_2 S^z = \log_2 C_a^x \times R_p^y \quad (31)$$

This gives the simplified form of Equation (31). Consequently, let us simplify the equation; we see that using this simplest form, the overall security level consists of two factors: the cybersecurity threat detection capability level and the program results given by

$$S^z = C_a^x \times R_p^y \quad (32)$$

Next, we have a system that gives the two dependency forms of the overall security level. From these systems, providing that x, y , and $z > 2$, we have a trivial solution, and the system S^z has only a single state:

$$\begin{cases} S^z = C_a^x \times R_p^y \\ S^z = C_a^x + R_p^y \end{cases} \quad (33)$$

Now, let us introduce the common security criteria for the calculations to define the mean factor of the cybercrime rate of Blockchain-enabled susceptibility given by

$$D = C_a^x \times R_p^y + S^z \quad (34)$$

where D denotes the common security criteria.

In addition to system (34), this formula achieves the summary of the overall security level plus its two independent factors.

Therefore, the common security criterion of S^z is $D_{S^z} = D_{C_a^x} + 1$, i.e., the criteria coefficients of C_a^x, S^z also differ by 1:

$$\begin{cases} R_p^y \times D_{S^z} = S^z \\ R_p^y \times D_{C_a^x} = C_a^x \end{cases} \quad (35)$$

where $D_{S^z}^y$ denotes the common security criteria of S^z and $D_{C_a}^y$ represents the common security criteria of C_a^x .

Now, we have proven the hypothesis, as this system finally shows that for each set of C_a , R_p , and S , the common security criteria of Blockchain technology is achieved.

Corollary 3. For $D = 0$, the above equation has several solutions.

For example, as they are natural numbers, the various solutions can be shown in the following equation:

$$D_{C_a^x}^y = a_1((D_{S^z} + 1)^y - R_p^y) + 1 \quad (36)$$

That is, for $D = 0$, the equation indeed derives various solutions from the cybersecurity criterion for each set of C_a , R_p , and S , so they have common security criteria.

Property 3. *Cyber awareness integrity—The user's overall security level consists of the user's susceptibility detection level and the positive or negative results obtained from the Blockchain technology. This property can be written as*

$$D_{C_a^x}^y = a_1((D_{S^z} + 1)^y - R_p^y) + 1 \quad (37)$$

Therefore, the overall security level is the sum of the cybersecurity susceptibility detection level and the performance of the proposed WBCA program.

5. Experimental Results

This section demonstrates the experimental results regarding the experimental setup, performance metrics, and finally result discussion.

5.1. Experimental Setup

The proposed WBCA uses a web server installed on a CentOS-based Linux distribution. To achieve the stated goals, a CentOS-based virtual private server is deployed and tested in Almaty, Kazakhstan, where the program consistency, quality ratio, user response time, solution efficiency, and threat avoidance capacity are monitored and calculated during testing process. The proposed WBCA is compared with the existing the state-of-the-art methods: Framework competence development and assessment(FCDA) [34], Integration of self-determination and flow (ISF) [35], modified total interpretive structural model (M-TISM) [36], Cybersecurity knowledge and skills(CKS) [37], and Cyber security awareness (CSA) [38].

These data are also calculated for the three most popular cybersecurity threats (email phishing, weak passwords, and virus). The minimal characteristics for the server hardware are Linux CentOS 7 x64 as the operating system, an Intel(R) Core (TM) i3-6100H with a frequency of 2.3 GHz and a cache size of 8192 kilobytes as the two-core processor, 4096 MB of random access memory, and a minimum of 50 gigabytes of hard disk space for collecting data. The required program component is Java SDK version 1.8.271u, and a monitor with a screen resolution of at least 920×1080 is used to conduct the proper experiments. These necessary characteristics for the web server are summarized in Table 1.

Table 1. Components of the web server.

Components	Version/The Name of the System
Personal computer	x64
Operating system	Linux CentOS 7
Java version	1.8.271u
Recommended screen resolution	920 × 1080
Processor	Intel(R) Core (TM) i3-6100H
Maker	Intel Xeon
RAM	4096 MB
Video memory	16 MB
Hard drive	50 GB (/dev/sda1)
CPU	2.300 GHz
Cache size	8192 KB

5.2. Performance Metrics

We determine the performance of the proposed WBCA and compared with the state-of-the-art contending programs. Therefore, the following parameters are used for conducting the experiments:

- Consistency
- Quality Ratio
- User Response Time
- Solution Efficiency
- Threat Avoidance Capacity

5.2.1. Consistency

The program consistency refers to the guarantee that the program follows the required rules to provide the stable outcomes. The user's basic cybersecurity awareness consistency is calculated using the following equation:

$$C = \frac{C_a}{T_a} \times 100\% \quad (38)$$

where C is the cybersecurity awareness consistency, C_a is the number of correct answers, and T_a is the total number of answers.

The data in Figure 4 demonstrate the correlation between the number of answered questions using the proposed WBCA and its comparison with other programs. The result demonstrates the consistency and versus the time users take to solve the test questions. The calculated data used to define the cybersecurity awareness consistency levels of the tested users are depicted in Figure 4a, which illustrates the best cybersecurity topic (with 85% knowledge) demonstrates that our proposed WBCA produces 99.76% consistency; whereas the contending programs show 97.4–98.75% consistency. The CKS yields 97.4% consistency that is less than other contending programs.

Figure 4. (a) Cybersecurity topic consistency using proposed WBCA and contending programs (M-TISM, ISF, FDCA, CSA, and CKS). (b) The quality ratios of the advanced cybersecurity topics using proposed WBCA and contending programs (M-TISM, ISF, FDCA, CSA, and CKS). (c) The correlation between the number of users and the time consumed when solving basic cybersecurity tasks with the proposed WBCA and contending programs (M-TISM, ISF, FDCA, CSA, and CKS).

5.2.2. Quality Ratio

Quality ratio refers to a quantitative factor that controls how efficiently the program uses its parameters to produce high performance. The users who pass the tests on the basic cybersecurity topics are further tested on advanced cybersecurity themes. However, in these calculations, we use the following equation of the quality ratio:

$$Q = \frac{N_t}{T} \times 100\% \quad (39)$$

where Q is the quality ratio, N_t is the total number of steps used to solve advanced tasks, and T is the total time required to solve these tasks.

This ratio shows the final cybersecurity awareness levels of the tested users. Consequently, we analyze the correlation between the time and the quality ratio. The result demonstrates in Figure 4b that the proposed WBCA has a 99.97% quality ratio, whereas the contending programs have a 98.08–99.38% quality ratio. M-TISM has a lower quality ratio. The main reason for not completing tasks is that the contending programs are affected due to malicious threats compared to the proposed WBCA program.

5.2.3. User Response Time

It refers to an important measurement indicator that demonstrates how much time the user gets for the task completion. It is the time that is required to complete the given cybersecurity tasks. Two different experiments are conducted. In the first experiment, time is measured for the basic cybersecurity tasks. In the second experiment, time is measured for the advanced tasks. Therefore, the basic task is calculated as

$$C_{bt} = \frac{n_u}{t_w} \times 100\% \quad (40)$$

where C_{bt} is the correlation between the number of users and time wasted when solving basic cybersecurity tasks, n_u is the number of users, and t_w is the time wasted when solving basic cybersecurity tasks.

Based on the result, we determine that a maximum of 90 users complete their basic cybersecurity tasks in 29.58 min with the proposed WBCA program, whereas M-TISM, ISF, FDCA, CSA, and CKS help the users to complete their tasks in 39.58, 37.31, 35.01, 32.41, and 49.59 min, respectively. In the second experiment, the proposed WBCA program takes 33.01 min to help the 90 users to complete their advanced cybersecurity tasks, while the

contending programs M-TISM, ISF, FDCA, CSA, and CKS support the users to finish their advanced cybersecurity tasks in 42.05, 45.01, 51.09, 39.03, and 57.23, respectively.

5.2.4. Solution Efficiency

Two experiments have been conducted to determine the solution efficiency. In the first experiment, the solution efficiency of the basic cybersecurity tasks is determined. In the second experiment, the solution efficiency of the advanced cybersecurity tasks is identified. The solution efficiency of the basic tasks is calculated as

$$S_{eb} = \frac{t_b}{n_b} \times 100\% \quad (41)$$

where S_{eb} is the solution efficiency of the basic tasks, n_b is the number of basic cybersecurity tasks, and t_b is the wasted time to solve these basic cybersecurity tasks.

Figure 4c shows the solution efficiency of the proposed WBCA and contending state-of-the-art programs. The results demonstrate that the solution efficiency of the proposed WBCA is found to be 100%, while the solution efficiency of the contending program is 98.06–99.65%. Based on the result, we conclude that the proposed WBCA program is working efficiently. On the other hand, the contending programs reduce the solution efficiency. The CKS program is highly affected as compared to other contending programs. When we conduct the second experiment with the advanced cybersecurity tasks, the performance of the proposed WBCA is slightly reduced despite the fact that it gets 99.34%, which is much higher than contending programs depicted in Figure 5a. Based on the results, we observed that the contending programs show a lower solution efficiency of 95.48–98.12%. The CKS is again producing lower solution efficiency.

Figure 5. (a) The correlation between the number of users and the time consumed when solving advanced cybersecurity tasks with the proposed WBCA and contending programs (M-TISM, ISF, FDCA, CSA, and CKS). (b) The solution efficiency of the proposed WBCA and contending programs (M-TISM, ISF, FDCA, CSA, and CKS) using the basic cybersecurity tasks. (c) The solution efficiency of the proposed WBCA and contending programs (M-TISM, ISF, FDCA, CSA, and CKS) using the advanced cybersecurity tasks.

Therefore, the solution efficiency of the advanced tasks is calculated as

$$S_{ea} = \frac{t_a}{n_a} \times 100\% \quad (42)$$

where S_{ea} is the solution efficiency of the advanced tasks, n_a is the number of advanced cybersecurity tasks, and t_a is the time wasted when solving these advanced cybersecurity tasks.

5.2.5. Threat Avoidance Capacity

The program can eliminate the malicious activities and exposures that negatively affect the performance of the program. Here, different scenarios are generated to determine the threat avoidance effectiveness of the proposed WBCA and competing programs. In Figure 6a, a maximum of 900 different types of threats (Denial of Service, Man-in-the-Middle, Malware, Phishing, and spam) have been generated. The result demonstrates that the proposed WBCA has a 99.32% threat avoidance capacity, whereas the contending programs have 95.52–97.72% threat avoidance capacity. ISF shows the lower 95.52% threat avoidance capacity as compared to other contending programs.

When the number of threats is maximized up to 1800, the threat avoidance capacity of the proposed WBCA is not highly affected. Despite the increase in the number of threats, the proposed WBCA shows 99.11% threat avoidance capacity. On the other hand, the contending programs are highly affected by maximizing the number of threats. The contending programs show the threat avoidance capacity of 93.81–95.04% depicted in Figure 6b. The main reason for getting the higher threat avoidance capacity is to use Blockchain technology that greatly reduces the potential threats.

Figure 6. (a) Threat avoidance capacity of the proposed WBCA and contending programs (M-TISM, ISF, FCDA, CSA, and CKS) with maximum 900 threats. (b) Threat avoidance capacity of the proposed WBCA and contending programs (M-TISM, ISF, FCDA, CSA, and CKS) with maximum 1800 threats.

5.3. Result Discussion

The proposed WBCA program consists of several program modules. The first module is responsible for defining the primary cybersecurity awareness outcome. The second module is responsible for deriving the result of the initial check, which ensures the information security knowledge of the user. As the simple counting sort algorithm is used for verification, the program does not require significant resources, and the user does not need a powerful technique to use it. Moreover, the proposed WBCA program uses Blockchain technology to avoid any potential threat. The proposed WBCA shows higher performance than competing programs (M-TISM, ISF, FCDA, CSA, and CKS) from the perspective of consistency, quality ratio, user response time, solution efficiency, and threat avoidance capacity shown in Table 2. The proposed WBCA makes it possible to easily determine what level of information security awareness a person has. Regardless of the result, the program hints at the shortcomings of the user in terms of the testing errors and gives recommendations for studying the relevant information security topics. Additionally, a big plus for the user is that the program is free, has an open license, and will always be available for download and further use. If there are sudden problems while using this program, the user can always leave feedback through the developer's email. However, it is worth noting a couple of disadvantages regarding this program. This program only checks the basic information security awareness level of the user. At the moment, the program is not

intended for advanced information security awareness testing. However, this drawback is insignificant, and in the future, people can always add an extended database of advanced questions to it. In the end, we can say that an effective program has been created to identify the current level of information security awareness possessed by any individual.

Table 2. Comparative Analysis of the proposed WBCA and contending programs: (M-TISM, ISF, FDCA, CSA, and CKS).

Programs	Consistency	Quality Ratio	User Response Time in Minutes (Basic Task)	User Response Time in Minutes (Advanced Task)	Efficiency (Basic Task)	Efficiency (Advanced Task)	Threat Avoidance (900 Threats)	Threat Avoidance (1800 Threats)
M-TISM	98.0%	98.08%	39.58	42.05	99.26%	97.01%	96.06%	95.04%
ISF	98.75%	98.61%	37.31	45.01	99.65%	98.12%	95.52%	98.17%
FDCA	98.17%	99.38%	37.31	51.09	98.88%	97.85%	97.72%	93.81%
CSA	98.37%	98.39%	32.41	39.03	98.52%	96.11%	96.92%	96.16%
CKS	97.4%	98.78%	49.59	57.23	98.06%	95.48%	96.92%	95.54%
WBCA	99.76%	99.97%	29.58	33.01	100 %	99.34%	99.32%	99.11%

6. Conclusions

This paper introduces a novel WBCA program for promoting high cybersecurity awareness among users. The proposed WBCA works via three modules. The user is tested on common cybersecurity questions and tasks, such as email phishing and weak password policies, and then the program checks if the user has good basic knowledge by making tests regarding advanced cybersecurity topics. The advantage of the proposed WBCA program is the strong check for current cybersecurity trends in the usual process of user behavior. This helps to determine if the person is sufficiently cybercrime resistant. The effectiveness of the proposed WBCA is tested on different metrics (consistency, quality ratio, user response time, solution efficiency, and threat avoidance capacity) and compared to the state-of-the-art programs. The comparative analysis with several topics regarding typical cybercriminal attacks on the users is performed. The proposed WBCA shows higher consistency, quality ratio, user response time, solution efficiency, and threat avoidance capacity than the contending programs (M-TISM, ISF, FDCA, CSA, and CKS). Based on the results, it is proved that WBCA is a good choice for testing if the current information security basics are sufficient to ensure that the person will minimize the risk of being a cybercrime victim. In the future, we will conduct advanced information security awareness testing. Additionally, we will also add an extended database of advanced questions to it.

Author Contributions: A.R., conceptualization, writing, idea proposal, methodology, validation, and results; A.A.A., data curation, software development, submission, and preparation; N.M., conceptualization, investigation; M.A. and B.A., review, editing, and visualization. I.D., A.O., S.H. and C.Z., review, resources, and editing. All authors have read and agreed to this version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The study did not report any data

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

References

- Mittal, A.; Gupta, M.P.; Chaturvedi, M.; Chansarkar, S.R.; Gupta, S. Cybersecurity Enhancement through Blockchain Training (CEBT)—A serious game approach. *Int. J. Inf. Manag. Data Insights* **2021**, *1*, 100001.
- Razaque, A.; Amsaad, F.; Khan, M.J.; Hariri, S.; Chen, S.; Siting, C.; Ji, X. Survey: Cybersecurity vulnerabilities, attacks and solutions in the medical domain. *IEEE Access* **2019**, *7*, 168774–168797. [\[CrossRef\]](#)
- Kaur, J.; Ram Kumar, K.R. The Recent Trends in CyberSecurity: A Review. *J. King Saud Univ.-Comput. Inf. Sci.* **2021**, in press.
- Oad, A.; Razaque, A.; Tolemyssov, A.; Alotaibi, M.; Alotaibi, B.; Zhao, C. Blockchain-Enabled Transaction Scanning Method for Money Laundering Detection. *Electronics* **2021**, *10*, 1766. [\[CrossRef\]](#)
- Palmieri, M.; Shortl, N.; McGarry, P. Personality and online deviance: The role of reinforcement sensitivity theory in cybercrime. *Comput. Hum. Behav.* **2021**, *120*, 106745. [\[CrossRef\]](#)

6. Borkovich, D.J.; Skovira, R.J. Cybersecurity Intertia and Social Engineering: Who'S Worse, Employees or Hackers? *Issues Inf. Syst.* **2019**, *20*, 139–150.
7. Frank, M.L.; Grenier, J.H.; Pyzoha, J.S. Board liability for cyberattacks: The effects of a prior attack and implementing the AICPA's cybersecurity framework. *J. Account. Public Policy* **2021**, 106860. [\[CrossRef\]](#)
8. Button, M.; Whittaker, J. Exploring the voluntary response to cyber-fraud: From vigilantism to responsabilisation. *Int. J. Law Crime Justice* **2021**, *66*, 100482. [\[CrossRef\]](#)
9. Almiani, M.; AbuGhazleh, A.; Al-Rahayfeh, A.; Atiewi, S.; Razaque, A. Deep recurrent neural network for IoT intrusion detection system. *Simul. Model. Pract. Theory* **2020**, *101*, 102031. [\[CrossRef\]](#)
10. Aberbach, J.D.; Christensen, T. Academic autonomy and freedom under pressure: Severely limited, or alive and kicking? *Public Organ. Rev.* **2018**, *18*, 487–506. [\[CrossRef\]](#)
11. Rahim, N.H.A.; Hamid, S.; Kiah, M.L.M.; Shamshirband, S.; Furnell, S. A systematic review of approaches to assessing cybersecurity awareness. *Kybernetes* **2015**, *44*, 606–622. [\[CrossRef\]](#)
12. George, J.J.; Leidner, D.E. From clicktivism to hacktivism: Understanding digital activism. *Inf. Organ.* **2019**, *29*, 100249. [\[CrossRef\]](#)
13. Delcher, P. Are we losing the fight against cybercrime? *Comput. Fraud. Secur.* **2021**, *2021*, 18–19. [\[CrossRef\]](#)
14. Yar, M.; Steinmetz, K.F. *Cybercrime and Society*; SAGE: London, UK, 2019.
15. Lane, B.R.; Salmon, P.M.; Desmond, D.; Cherney, A.; Carley, A.; Hulme, A.; Stanton, N.A. Out of control? Using STAMP to model the control and feedback mechanisms surrounding identity crime in darknet marketplaces. *Appl. Ergon.* **2020**, *89*, 103223. [\[CrossRef\]](#)
16. Umanailo, M.C.B.; Fachruddin, I.; Mayasari, D.; Kurniawan, R.; Agustin, D.N.; Ganefwati, R.; Daulay, P.; Meifilina, A.; Alamin, T.; Fitriana, R.; et al. Cybercrime Case as Impact Development of Communication Technology That Troubling Society. *Int. J. Sci. Technol. Res.* **2021**, *8*, 1224–1228.
17. Bello, M.; Griffiths, M. Routine activity theory and cybercrime investigation in Nigeria: How capable are law enforcement agencies? In *Rethinking Cybercrime*; Springer: Cham, Switzerland, 2021; pp. 213–235.
18. Shuftipro. Available online: <https://shuftipro.com/blog/how-age-verification-protects-the-e-commerce-industry-from-potential-risks/> (accessed on 3 July 2021).
19. Bada, M.; Sasse, A.M.; Nurse, J.R. Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv* **2019**, arXiv:1901.02672.
20. Newhouse, W.; Keith, S.; Scribner, B.; Witte, G. National initiative for cybersecurity education (NICE) cybersecurity workforce framework. *NIST Spec. Publ.* **2017**, *800*. [\[CrossRef\]](#)
21. Pessim, P.S.P.; Lacerda, M.J. State-feedback control for cyber-physical LPV systems under DoS attacks. *IEEE Control Syst. Lett.* **2020**, *5*, 1043–1048. [\[CrossRef\]](#)
22. Talukder, M.A.I.; Shahriar, H.; Haddad, H. Point-of-sale device attacks and mitigation approaches for cyber-physical systems. In *Cybersecurity and Privacy in Cyber-Physical Systems*; CRC Press: Boca Raton, FL, USA, 2019; pp. 367–391.
23. Dreyfuss, R.C. TRIPS-Round II: Should Users Strike Back? In *The Regulation of Services and Intellectual Property*; Routledge: London, UK, 2017; pp. 397–411.
24. Eskandari, S.; Leoutsarakos, A.; Mursch, T.; Clark, J. A first look at browser-based cryptojacking. In Proceedings of the 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), London, UK, 23–27 April 2018; pp. 58–66.
25. Burlison, J.D.; Scott, S.D.; Browne, E.K.; Thompson, S.G.; Hoffman, J.M. The second victim experience and support tool (SVEST): Validation of an organizational resource for assessing second victim effects and the quality of support resources. *J. Patient Saf.* **2017**, *13*, 93. [\[CrossRef\]](#)
26. Cascavilla, G.; Tamburri, D.A.; Heuvel, W.-J.V.D. Cybercrime Threat Intelligence: A Systematic Multi-Vocal Literature Review. *Comput. Secur.* **2021**, *105*, 102258. [\[CrossRef\]](#)
27. Tsakalidis, G.; Vergidis, K. A systematic approach toward description and classification of cybercrime incidents. *IEEE Trans. Syst. Man Cybern. Syst.* **2017**, *49*, 710–729. [\[CrossRef\]](#)
28. Senarak, C. Port cybersecurity and threat: A structural model for prevention and policy development. *Asian J. Shipp. Logist.* **2021**, *37*, 20–36. [\[CrossRef\]](#)
29. Gallo, L.; Maiello, A.; Botta, A.; Ventre, G. 2 Years in the anti-phishing group of a large company. *Comput. Secur.* **2021**, *105*, 102259. [\[CrossRef\]](#)
30. D'Hooge, L.; Wauters, T.; Volckaert, B.; De Turck, F. In-depth comparative evaluation of supervised machine learning approaches for detection of cybersecurity threats. In Proceedings of the 4th International Conference on Internet of Things, Big Data and Security (IoTBDs), Crete, Greece, 2–4 May 2019; pp. 125–136.
31. Jiang, S.; Cao, J.; Wu, H.; Yang, Y.; Ma, M.D.; He, J. Blochie: A blockchain-based platform for healthcare information exchange. In Proceedings of the IEEE International Conference on Smart Computing (SMARTCOMP), Taormina, Italy, 18–20 June 2018; pp. 49–56.
32. Jiang, S.; Cao, J.; Wu, H.; Yang, Y. Fairness-based packing of industrial IoT data in permissioned blockchains. *IEEE Trans. Ind. Inform.* **2021**, *17*, 7639–7649. [\[CrossRef\]](#)
33. Jiang, S.; Cao, J.; McCann, J.A.; Yang, Y.; Liu, Y.; Wang, X.; Deng, Y. Privacy-preserving and efficient multi-keyword search over encrypted data on blockchain. In Proceedings of the IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019; pp. 405–410.

-
34. Brilingaitė, A.; Bukauskas, L.; Juozapavičius, A. A framework for competence development and assessment in hybrid cybersecurity exercises. *Comput. Secur.* **2020**, *88*, 101607. [[CrossRef](#)]
 35. Kam, H.-J.; Menard, P.; Ormond, D.; Crossler, R.E. Cultivating cybersecurity learning: An integration of self-determination and flow. *Comput. Secur.* **2021**, *96*, 101875. [[CrossRef](#)]
 36. Rajan, R.; Rana, N.P.; Parameswar, N.; Dhir, S.; Dwivedi, Y.K. Developing a modified total interpretive structural model (M-TISM) for organizational strategic cybersecurity management. *Technol. Forecast. Soc. Chang.* **2021**, *170*, 120872. [[CrossRef](#)]
 37. Švábenský, V.; Čeleda, P.; Vykopal, J.; Brišáková, S. Cybersecurity knowledge and skills taught in capture the flag challenges. *Comput. Secur.* **2021**, *102*, 102154. [[CrossRef](#)]
 38. Hart, S.; Margheri, A.; Paci, F.; Sassone, V. Riskio: A serious game for cyber security awareness and education. *Comput. Secur.* **2020**, *95*, 101827. [[CrossRef](#)]