

Review: Cyber Insight – Illuminating Cyber Security for all

Ayush Kore, Kushal Hirudkar, Palak Jaiswal, Shravani Ambulkar, Shaarav Kamdi, Shalini Kumari GH
Raisoni College of Engineering and Management, Nagpur, India

Abstract- With the advent of the “e-” revolution starting in 2000, the issue of cyber security, cyber-attacks and cyber threats which included domains, but not e-business, e-government, e-commerce etc. only occurred because for the issue of cybersecurity in e-learning is under-explored, the aim of this paper is to present methods that focus on monitoring cybersecurity issues related to e-learning processes on. In addition, this article aims to present some good examples of cybersecurity management strategies in e-learning and cybersecurity trends in this area.[2] This paper will present possibilities for increasing information security and cyber-security awareness in education and e-learning that will inspire future cybersecurity professionals to navigate their career path.[3]

Index Terms- cyber security; cyber-attack; e-learning; skills; programming.

I. INTRODUCTION

E-learning is the accession of knowledge and chops through electronic means, and it's among the imperative technologies which are being endured by numerous in current times. Due to high technological widgets and tools that have picked up, it has reduced the difficulties and frustrations learners suffer in hunt of knowledge and chops. The days when people had to travel from hence to get knowledge and chops and pay a huge quantum of plutocrat to develop their eventuality are far before. For case, no redundant cost is incurred by the universities, sodalities, or institutions on erecting structure or hiring outfit similar as electronic boards, projectors, etc. The scholars can gain applicable information and chops from the internet in their defined surroundings with smaller amenities. The usage and fashion ability of Internet and computer networks have grown over the times giving stakeholders more and more possibilities to get an education, get access to digital coffers, information, news, in order to limitlessly improve our professional and particular lives- from any place at our accessible time.(1) This also includes graces in the development of digital coffers, but at the same time there's a problem it's hard to define if data protection will be carried out without snooping with availability and simplicity in light of the fact that we tend to partake information on different kinds of spots and networks without indeed allowing about being exposed to cyber pitfalls. This technology has given remarkable openings for scholars and the entire stakeholders of thee-learning system. In the forenamed environment, the increased operation of e-Learning systems, the continuing growth of computers and mobile computing bias operation (smartphones, tablets, PDA's) in confluence with internet access, numerous business associations, seminaries, academic

institutions and public spaces have espoused the BYOC – Bring Your Own Computer and of the BYOD – Bring Your Own Device paradigm. innovated by Intel in 2009, BYOD means that scholars and workers can bring their own particular bias and use them to pierce private networks of the association they belong to.(2)

E-learning operation systems use the Internet as a place to acquire all the necessary information and knowledge employed in this internet-grounded literacy system. still, due to these illegal conditioning and security pitfalls, it's ineluctable that nonstop security pitfalls, pitfalls, and attacks be within an e-learning environment. further to the point, the internet has actually come the origin of cyber-attacks. Hacking and internet fraud less are using different ways to steal particular information and sequestration.

For that matter, the core rudiments of any e-learning system are participating ideas, information via electronic means. Data must be secured and defended to maintain its confidentiality, integrity, and vacuity. This paper aims at compactly assaying the conversations in the affiliated literature, furnishing a summary review of the security aspects of thee-learning operation system, and also to ascertain the security challenges in an eLearning operation system. It anatomized indispensable mechanisms in examining the cyber threat involved in an eLearning operation system, by a veritably detailed literature review using academic databases, including Google Scholar. The end of this paper is to harmonize all that information so that directors, scholars, and preceptors come to know the threat involved in an e-learning operation system. And, thereby, have implanted some security measures to evolve a secured and defended terrain fore-learners from cyber-attacks.(1)

II. LITERATURE SURVEY

1. The Benefit of the E-Learning operation System

This changed because the world has now come to be a global will, making education shift from the traditional class- room-grounded experience to an online base. People acquire knowledge and chops without inescapably being in the classroom. New course models are now available, combining face- to- face with e-learning. Both coetaneous and asynchronous form of literacy is now available for the campaigners of knowledge and chops. These benefits, thus, aren't only helpful for the scholars but rather help the scholars and the entire stakeholders of the e-learning system. The benefits of e-learning are bandied below;

The benefit of e-learning to the scholars. E-learning has been the easiest means to acquire knowledge and skill. Due to its flexible nature, it has come the medium of education among public workers. It can be derived that e-learning has prodded life-long literacy. Through e-learning, the learner is given the occasion to have access to accoutrements and information anywhere at any time. Whereas in an e-learning terrain, information is been accessed online and there's no time-bound in reaching the asked accoutrements , thus, the learner in his comfort zone has access to knowledge at any paying time. E-learning has helped scholars economically in the sense that, scholars don't need important plutocrat in buying of reading accoutrements . rather, applicable information can be penetrated online. Situations where preceptors have to travel to the longer distance in seeking knowledge are over. eLearning saves plutocrat and time. Using new ICT widgets in our technological terrain helps pupil get further understanding of affiliated generalities. Knowledge is now at the doorsteps of scholars. scholars can pierce knowledge any-time, anywhere, and at any place. similar gain can not be quantified. Thee-learning terrain avails the learner with important- required chops in ICT. The more the pupil engages with the ICT tool, the more professed hebe-comes.

What advantage the e-learning operation system offers to the association. With the revolution of e-learning, institu- tions don't need to put on a lot of structures to accommodate thousands of scholars, since learners can have access to information online in both coetaneous and asynchronous form. Economically, institutions, associations, and companies are making a huge quantum of plutocrat through online courses.

2. Cybersecurity in the E-Learning Management System

The security deficiency of e-learning systems currently used to support online learning. Series of online course management systems were designed to improve collaborative learning, then, suddenly, the security aspect was left in the cold. This may pave way for insecurity issues that may blemish managerial activities since students would try to

access information belonging to their colleagues, Tutors and administrators handling the students' academic records would manipulate them, etc. Given such circumstances, Moneo et al. proposed a system based on PKI models that offer preliminary security properties and services within online collaborative learning environments, ensuring data and information availability, integrity, authenticity, and confidentiality.

PKI consists of the hardware, software, and procedures that are necessary for the management, storage, and revocation of digital certificates and public keys. The PKIs provide the basis that allows technologies, like digital signature and encryption, across large user populations. Therefore, it provides elements required to make an online transfer of information both secure and trusted. Moreover, PKIs enable the formation of a secure data transfer between users and devices with authenticity, confidentiality, and integrity of operation intact.

In their attempt to preserve the availability, integrity, confidentiality, and authenticity of the e-learning management system, Mohd Alwi and Fan proposed a model developed by Microsoft in designing web applications to analyze security threats in the electronic learning systems termed "IWAS". This model provides five steps in the analysis of security threats in an e-learning environment, and they are been listed as bellow;

- Identify security objectives
- Application overview
- Decompose application
- Identification of threats [1]

3. Benefits of using BYOD and e-Learning System

In the recent past, BYOD in organizations or academic institutions has become common with various benefits. In this regard, these organizations have to enact policies – accessible, comprehensible, and open for feedback.

The users have to secure and protect their devices with passwords and other authentication methods and have to be trained concerning vulnerabilities and cyber threats.

Specific cases such as universities benefit the student's use of the internet as a source of information, whereby they are allowed digital resources (electronic journals, digital libraries, on line courses, shared information by other students and teachers) from anywhere at any time. The above type of learning can be tailored for every student according to his free time, style of learning, his level of knowledge, and also can be suitable for students to provide feedback. In order to have good results in the process of education, it is necessary to have interaction and cooperation. Implement BYOD in universities has a great impact on their economy: Infrastructure and costs-the universities can provide a smaller number of computers/tablets/smart devices for students who cannot afford these devices, Time-the student knows to use

their own devices-and hence the learning process becomes more interactive and attractive.

Some of the main problems in using BYOD, as a student-centered vector for personalized learning in universities and schools, include lack of control: teachers have no idea if the student is interested in the topic or uses the device in his or her personal interest other than learning, which might be distracting for the process of learning.

The phenomena of cyberbullying and disclosure of private and confidential information on the web or social media, compatibility of devices, configurations, and software applications, computer/mobile devices skills and not less important, affordability of the device. Other implicit cost includes the discovery of IT experts to provide this kind of learning and the related infrastructure behind and to ensure security, to know the risks and solutions in countering a potential threat or mitigating the effects of a cyber breach/attack. Using those solutions, learning institutions may better track and know more about the devices, the software and applications the web sites, the downloads, etc. the students and staff use in this environment. A much-debated topic in the domain, technology in education is used at a large scale as we use technology in almost every aspect of life and digital resources are in an extra ordinary growth, as their availability. "Combined with the right pedagogical skills, used with responsibility, eLearning is an effective instrument.". From the private sector standpoint, BYOD means that the workers' own devices-their laptops, tablets, smartphones, etc- can now be connected to the company network and resources in all of their work activities. From home or office or anywhere, they could log into work at any time, and they could store data belonging to the company on them, thus saving a lot of the costs associated with the IT infrastructure of creating a collaborative flexible productive environment.

To reduce the risk, the company needs to be in possession of an effective Information Security Management System as well as a BYOD use policy on using such a system with secure passwords, have appropriate training sessions to present the policy, risks resulting from inappropriate use, data loss, etc. should be accessible and comprehensible to ensure the protection of company data and assets.

Even though it is a trend, there are companies and academic organizations which are reticent considering the threats of using BYOD are more expensive than the benefits of using it. They use their own infrastructure, deciding which devices are used, which software is installed, which websites are accessed and which information can be downloaded and shared, using an IT service to ensure these policies.

Employees now expect they can utilize their mobile devices for business purposes or other purposes in their lives, whether

company-owned or owned by the employee. Similarly, many employees believe that a company should be flexible and provide its employees with an opportunity to use a device for either the employee's business or individual purpose for better productivity in the workplace. From literature, there are studies, methodologies, and guidelines for

BYOD by known organizations that provide recommendations on the management of BYOD, for example, "Whiter House Guidelines" on BYOD or "National Institute of Standards and Technology Guidelines" on BYOD.

To the same extent, there are similar studies by private companies and all have the purpose of making BYOD a suitable instrument while implementing security and privacy policies, regulating the authorization levels for users and staff, securing network and web access.

4. Cyber Security in BYOD and e-Learning System

Cyber security represents the set of rules enacted for the protection of cyberspace. As e-Learning has undertaken spectacular development in the last years and its usage has been traced with uprising trends from various studies, which maintain this growth trend, interest concerning the issue of security of e-Learning systems, both in research and education, takes on the utmost importance.

Using BYOD, besides the advantages it bears huge risks considering the fact that devices are owned by users and not organizations companies, universities. Devices can provide weaknesses, compromised, and going through networks can result in cybersecurity breaches and affect data susceptible to protection and/or privacy.

Generally, eLearning systems tend to favor a collaborative flexible, sharing environment and more pedagogical rather than security-oriented which might result in a negative effect on learning activities as well as human life.

BYOD has expanded its boundary of acceptance through the tablets and smartphones; apart from the laptops and iPads, it provides more flexibility and mobility. Students and employees are accessing educational material, interacting with colleagues and tutors, reading content, recording courses, copying notes, and work-related material through a company or university network using a browser. Along with these advantages, with information sharing and dissemination and a wide range of users and applications, BYOD involves a certain number of risks and vulnerabilities: security threats, thefts of personal data or identity, data modification, piracy, cyber bullying, etc.

Among these cyber security threats, the most accentuated from the point of view of the specialized literature are those concerning:

- authentication – theft of credentials, unauthorized access, espionage, insecure communication, etc.
- data loss/ leakage – due to loss or stolen devices or poor security and encryption, unauthorized collection of data, confidentiality attacks, incidental disclosures of data, etc.;
- installation of malicious software (viruses, spam, phishing scam, malware, Trojans, spyware, etc.), use of untrusted applications, technical failures and errors, etc.;
- malicious software cyber-attacks (viruses, worms, macros, denial of service, Cross Site Scripting, IP spoofing, Rootkits, SQL Injection, etc.), sabotage, etc.;
- delicts relating to intellectual property (piracy, copyright, infringement), etc.;
- use of untrusted/unsecure networks, network congestion, etc.;

The figure of security breach is on a constant rise, whether it's learning institutions, private or public companies, or governmental institutions. All such breaches are costly to each institution and thus each organization is to be answerable for its data protection.

There are measures to mitigate such risks and threats such as: implementing Security management; security policies, procedures, and processes; improved authentication tools; access control; permissions for users in different layers according to their status; automatic back-up procedures; encryption for important or sensitive data; antivirus, anti-spam, and firewall software, and beyond all that - user awareness training.

As we have seen above, this is a national and European regulatory framework that realizes protection and data integrity solely depends on the organization and each user of BYOD. As mentioned earlier above, it means not just having anti-virus software installed or firewalls in organizations but insisting on implementing security policies and procedures, holding campaigns, and training for awareness and acceptance of BYOD security policies by the users.[2]

5. Building Digital Trust

Higher Education is a very different environment to what it was some years ago and is now offering significant student engagement via online learning systems. Students have an ever-increasing understanding of information systems (IS) and information technology (IT) issues, so overall learning strategies devised by course providers must be intrinsically linked with IS/IT strategies to meet student needs now and in the future. Digital natives and digital immigrants will expect their e-Learning system to be highly user-friendly, secure, and protective of personal information. This may involve the safe management of a student's bank details relating to fee payments for courses and other items. Universities in the UK possess vast intellectual property with research and other

academic material which would prove an easy target for cyber-criminals. Researchers will expect their sensitive work and commercially important information to be stored securely, without any risk of theft or misuse. A cyber security risk assessment needs to be done by institutions and they need to determine best arrangements for technology, people, and processes.[4]

6. Common Application Vulnerabilities

Paper In Common Security Vulnerabilities in e-commerce Systems With the enormous growth of online transactions have also gained their equal amount in growing numbers as well as types of attacks on the security of systems of online payment. Some of such attacks exploited vulnerabilities that have been published in reusable third-party components utilized by websites, such as shopping cart software. Other attacks use general weaknesses inherent to any web application, such as SQL injection or cross-site scripting. An exploitation of such a vulnerability can lead to several types of result. Disclosure vulnerabilities of information and path will probably act as the first steps to further exploitation. The website could end up crippled by SQL injection or price manipulation attacks and compromised confidentiality, with the worst-case scenario being its complete shutdown.[5]

7. Research in Security of E-Learning

The e-learning environment must avoid all four kinds of threat: fabrication, modification, interruption and interception. To-date, very few researches have been conducted towards securing the e-learning environment. The main categories of researches in security include policy, identity (access management) and intellectual property.

Most researchers indicate that, in order to avoid all attacks upon the e-learning environment, access control has to be essential. One of the ways to do this is via authentication and authorization process. Jalal, 2008 recommends an authentication process so as to identify a legal user process; this will overcome the illegal usage of application. A system which is too heavily secured will be difficult to be accessed by the user. Balancing accessibility and security Saxena uses the single sign on authentication and authorization services to all authorized web applications and web resources for getting an equal balance. Graf gives a possible approach in which protection of intellectual property is achieved via extension of control by the copyright holder onto the whole lifetime of the digital data. CI-PRESS This is a method he suggests in order to control access to material. The other technical aspect by which Yong discusses how to secure e-learning is through the design of digital identity and privacy preservation.

This can be considered as insufficient because the attack can come not only from the outsiders but also from the insider. There is a great need for the management to supervise the proper handling of information security issues in order to

check for the vulnerabilities that could make the system a failure. As such, information security management is crucial when striving to guarantee the success of the secured e-learning implementation.[6]

III. METHODOLOGY

This Methodology will help you to guide walkthrough to the website by block diagrams.



Fig 1: Front page Interface

This front page will content of two main components i.e., Navbar & Hero section as can see in fig 1.

The Navbar, or navigation bar, is a crucial component of a website that helps users navigate through different sections or pages. A navbar is a user interface element that contains links to the main sections of a website. It typically appears at the top of the web page but can also be found on the sides or bottom, depending on the design. The Navbar will content of some buttons like, Home, Road Maps, Tools, Sign-up/Sign-in.

The Home button, in fig 2., in a navbar is essential for enhancing user navigation and experience. It serves as a gateway back to the homepage, facilitating easy access to the central content of the website while reinforcing brand identity and encouraging exploration. A well-placed and designed Home button is a key component of effective website navigation. The primary function of the Home button is to provide users with a quick way to return to the homepage of the website. This is particularly useful for users who have navigated deep into the site and want to start over or access the main content.

The Road Map, in fig 2., is a strategic plan that outlines the structure, design, and functionality of a website. It serves as a blueprint for both the development and design teams, guiding them in creating a cohesive and user-friendly online experience. A website roadmap is a comprehensive plan that guides the design, development, and maintenance of a website. It encompasses goals, audience analysis, site structure, content strategy, design elements, functionality,

time- lines, budgets, testing, and maintenance plans. Having a well-defined roadmap is crucial for the successful execution of a website project, ensuring that it meets user needs and business objectives effectively.

Website Sign-in and Sign-up are essential features for many online platforms, allowing users to create accounts and access personalized services. It processes are crucial components of many websites, enabling users to create accounts and access personalized features securely. The processes involve filling out registration forms, verifying email addresses, entering credentials, and possibly using additional security measures like two-factor authentication. These features enhance user experience, security, and engagement while providing valuable data for website owners.

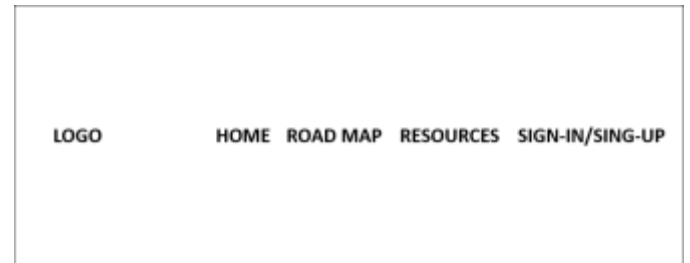


Fig 2: Website Navbar or Navigation Bar

The Resources will content of main three Features Cyber Security Theory, Cyber Security Tools and Programming Languages.

Cyber Security Theory will Cover some theory topics, like Computer Network, Secure Programming, Operating System and many more. These all topics will guide you through what exactly cyber security is and how can you prevent yourself from being attacked by any hacker.

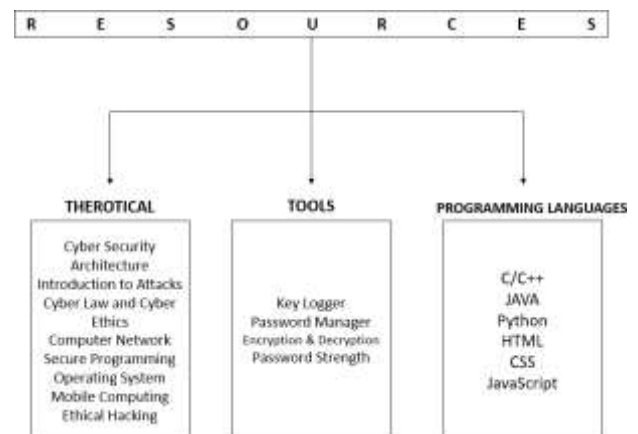


Fig 3: Main Features of Resources

This can also be done by some live tools, this will demonstrate how can anyone get attacked by hacker and how

can you prevent from it by using website tools, like Key Logger, Password Manager, Encryption & Decryption, Password Strength.

And To Study some basic programming languages it will content of languages, like C/C++, Python, Java, HTML, CSS and JavaScript.



Fig 4: User Admin Interface

The Admin Interface will be only access by admins or those who will have username and password. If the credentials are correct then user can manage Student list, Create Course, Delete/Edit Course, Delete Student Profile, as given in Fig 4.

The User have to create his/her account to access all the resources. After sign-in they can use all tools, like Theory, Tools, programming languages. User can also practice by playing quiz or can also read some news about cyber security, how vast cybercrime is increasing globally.

IV. RESULT

The results indicate that the platform successfully enhances users' understanding of cybersecurity principles and practices. Feedback from participants highlights improved awareness of cyber threats and best practices for online safety. The interactive learning modules and practical exercises were particularly effective in reinforcing theoretical knowledge, allowing users to apply what they learned in realistic scenarios.



Fig 5: Front page Interface

The frontend view of the cybersecurity e-learning platform is user-friendly and visually pleasing, designed for intuitive navigation by all users with diverse skill sets.

At the head of the page, there is a clean and direct navigation bar displaying some of the important links like Home, Courses, About Us, Resources, and Sign-in/Sign-up as well that can be observed in Fig 5. On full display on the top-left side are the logos of the platform as well. This actually reiterates brand identity.

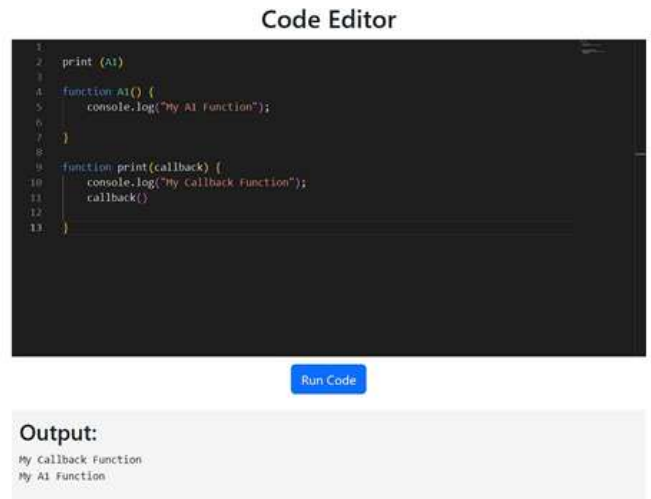


Fig 6: Online Compiler

This is online compiler, which can be directly accessed from a webpage. This allows the user to write, compile, and run code from the comfort of their browser. Such a platform greatly aids the learning process when acquiring a programming language, since using it requires testing code snippets without any need to have software installed on the local machine.

The code editor forms the core component of the online compiler. This is where users typically write their code; it would have some basic support for syntax highlighting, auto-completion, and error detection that will help the user in coding more efficiently.

Once one has written code, he or she may click on the "Run Code" button to compile and execute the code. Such an action will consequently trigger the compiler to process the code so as to generate a reported output, as indicated above in Fig 6 blue button.

Below or to the side of this code editor, one generally finds an output console in which the results of the executed code are shown. It is very useful for debugging and for knowing how the code works.

The compiler will print out error messages in the output console, therefore giving users an idea where exactly the problem lies so that they can solve the problem.

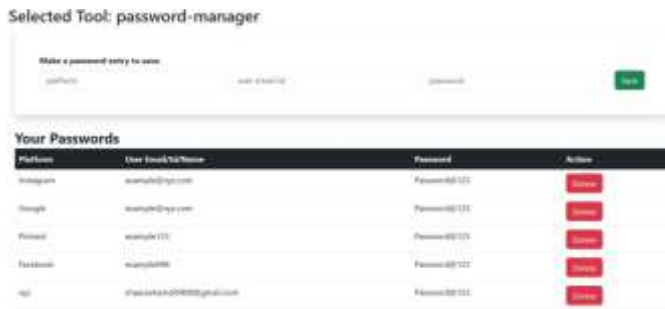


Fig 7: Password Manager

A password manager for a website is a utility program to save, monitor, and even generate passwords for web account access. This way, security is automatically enhanced because users will be able to create nonrelated, complex passwords for every website without having to memorize them all.

This one usually has a clean and intuitive user interface, typically in fig. 7. A dashboard that would present all the lists of the saved passwords, possibly ordered by website or application. It is very easy to conduct searches for specific entries.

The manager allows saving passwords safely. An entry usually contains the website name, a login name, a password, and sometimes an additional note regarding it. All passwords are encoded for safe protection against unauthorized access.

Some password managers have a security audit feature that analyzes stored passwords for weaknesses, including reuse or just too weak. This helps users to improve their overall password security.



Fig 8: Admin Interface to Create Course

Fig 8 Creating courses on a webpage: this is an admin panel. It is a kind of back end interface that the administrator or teacher might interact with to develop and modify virtual courses.

Traditionally, the admin panel starts with a dashboard showing an overview of all courses, statistics such as the number of people enrolled in students, completion rates of courses, and recent activity. The dashboard helps admins speedily determine their overall statuses about their courses. Usually, a well-noted area is for course creation. This enables admins to input all of the most important information, which includes the course title, description, and category.

Admins can upload different types of content as needed for a course.

Modules and Lessons: This functionality should allow an individual to create modules, which could include several lessons. In this particular case, each lesson could be assigned with text, pictures, video links, or even quizzes.

V. CONCLUSION

Building an e-learning cybersecurity platform would be a great leap forward in the cause to better the awareness and knowledge of cybersecurity in the field.

This platform may be one of the really valuable sources offered to individuals and organizations through which they can improve their understanding and skills concerning cybersecurity. There are full-blown courses, interactive modules, and news on the latest emerging threats. All this makes the platform empower users to protect their assets and themselves in the digital world.

The addition of practical work and real-world case studies can enrich the learning experience so that users not only acquire some theoretical concepts, but also learn how to apply them. Moreover, including industry specialist certifications for developing content will boost the authenticity and appeal of this platform.

The ultimate success of this e-learning cybersecurity platform will be an attractive appeal to its users, combined with creating an environment of ongoing adaptation to the development of this world of security threats. This e-learning cybersecurity platform, following this approach, would turn out to be a safe and essential point in forming the digital surroundings for all users.

REFERENCES

1. Habib Ibrahim, Songül Karabatak, Abdullahi Abba Abdullahi: A Study on Cybersecurity Challenges in E-learning and Database Management System, Published in 2020
2. M. Anghel, G.C. Pereteanu: CYBER SECURITY APPROACHES IN E-LEARNING, Published in 2020

3. Milos Tisma, Jasmina Andric: Importance of cyber security awareness and e-learning motivation for cyber security in reshaping the education, Published in 2021
4. I.Bandara, F.Ioras, K.Maher: CYBER SECURITY CONCERNS IN E-LEARNING EDUCATION, Published in 2016
5. Chee Chern Lim and Jesse S Jin: A Study on Applying Software Security to Information Systems: E-Learning Portals, Published in 2006
6. Najwa Hayaati Mohd Alwi, Ip-Shing Fan: E-Learning and Information Security Management, Published in 2010
7. Abdullah M. Alnajim , Shabana Habib, Muhammad Islam, Hazim Saleh AlRawashdeh and Muhammad Wasim: Exploring Cybersecurity Education and Training Techniques: A Comprehensive Review of Traditional, Virtual Reality, and Augmented Reality Approaches, Published in 2023
8. Mary Jane C. Samonte, Kevin Nicholas U. Banganay, Karen E. Fernandez and Jameela Nadine D. Jamena: CyLearn: An Assistive Web-Based e-Learning System for Cybersecurity Skills Course, Published in 2023
9. Dat Tang, Cuong Pham and Ken-ichi Chinen, Razvan Beuran: Interactive Cybersecurity Defense Training Inspired by Web-based Learning Theory, Published in 2017
10. Regner Sabillon, Jordi Serra-Ruiz, Victor Cavaller, Jeimy J. Cano M: An Effective Cybersecurity Training Model to Support an Organizational Awareness Program: The Cybersecurity Awareness TRaining Model (CA- TRAM). A Case Study in Canada, Published in 2019
11. Anna Georgiadou, Spiros Mouzakis, Kanaris Bounas , and Dimitrios Askounis: A Cyber-Security Culture Framework for Assessing Organization Readiness, Published in 2022