JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

# Educational Game on CyberSecurity

[1]Prof Shraddha Rokade,[2]Diksha Ingle,[3]Priya Wadile ,[4]Pooja Zepale
[1]Assistant Professor, [2] Student ,
[3] Student,[4] Student.
Department of Computer Engineering,
Usha Mittal Institute of Technology, Santacruz(w), India

***Abstract:*** A Web-based application called the Cyber Warriors is developedto educate, promote and help raise awareness of the best practices for cyber security. Ren'Py, Python, and Figma were used to build the game, which aims to be entertaining, interactive, and educa-tional. The game's aims and events test the player's knowledge of cyber security concepts like malware, phishing attacks, and strong passwords. Users are given various tasks, each designed to be enter-taining and educational. Ren'Py is an interactive storytelling enginedesigned for creating visual novels and life simulation games forcomputers and mobile devices. Using Ren'Py, a well-known designtool that enables rapid prototyping and iteration, the game inter-faces were developed. Python is a flexible and potent programminglanguage that is used to construct the game and get performancefeedback. Users can compare their performance with others using the leaderboard in the game. The Cyber Warriors is an entertainingand useful tool to educate students on cyber security best practices.It combines the strengths of Python for developing the backend and game logic and for constructing engaging user interfaces and visually appealing features. Through this combination, users canlearn about cyber security in a way that is interactive, informative and memorable.

***IndexTerms* –** Cyber Safety , Internet Security, awareness, Cyber-Attacks(cyberbully,stocking,harassment)

## I. INTRODUCTION

Children nowadays play a lot of online games and browse the inter-net for several hours every day. On the internet, they meet several opportunities as well as risks; but without relevant knowledge, itis difficult for them to assess the associated risks or threats of using the internet and digital systems. Sometimes they do not evenrealize the danger of the risks. Children may potentially expose themselves at risk unintentionally in various ways or sometimes. may leak personal or confidential information even without knowing. They can also fall victim to cyber security threats like socialengineering, cyberbullying, hacking, viruses, damaging malware, cyberstalking, etc. through search engines, online advertisements and social networking websites such as Facebook, Twitter and lots of other websites[5].

We created a Cyber Warriors that is created using Ren'Py and interactive Python to meet this demand. This web-based application was created especially for kids and is meant to be interesting, interactive and educational. It gives students a chance to learn about cyber security in a way that is interesting and memorable breaches. The game includes several challenges and scenarios that test the student's understanding and awareness of cyber security concepts like malware, phishing attacks and strong passwords. Students can learn the importance of secure passwords, how to identify and avoid phishing emails and how to protect against malware through those activities. Overall, the Cyber Warrior is an innovative and effective approach to educate students about cyber guidelines and to enhance student awareness of them. We have developed an interactive experience that is exciting and memorable for kids to learn about cyber security by combining the capabilities of Ren'Py and Python.

## II. EXISTING SYSTEM

Related work for Cyber Warriors for students consists of: Here are some reasons why work is relevant for cyber security awareness:

- CyberPatriot, NetSmartz Workshop, "Be Online Awesome"and "WebME" are a few mobile applications and games that have been created to teach students about cyber security.
- The effectiveness of various cyber security education methods and approaches, such as video games and multimedia applications has been examined in studies and research publications.
- Guidelines and best practices for creating efficient cyber security education programs, with suggestions for curriculum design, instructional strategies, and evaluation measures .
- Technical research articles on the development of programs and technologies, like Ren'Py and Python, that are utilized in the Cyber Warriors Game .

- Papers discussing the ethical issues related to the development and use of the technologies for cyber security education, such as privacy, security and informed consent.
- Papers on the benefits and effectiveness of cybersecurity education in various settings, such as at educational institutions organizations or governments.

## III. METHODOLOGY

The methodology of our Cyber Warrior Game for Students can bebroken down into the following steps :

- Identify the Game's Intended Audience: In this situation, thegame's target audience is students. Decide on their average age, level of education, and any other relevant details thatcan help with game design.[4]
- Establish Learning Objectives: Especially the game's learning objectives should correspond to the needs and aims of the intended audience. For instance, the game might try to teach pupils about things like phishing, malware, and cyber-bullying.[4]
- Design the Game Interface: Ren'Py is used to create a game's user interface and experience. The layout, colors, typography, and graphics that will be utilized in the games or organizations must be designed.
- Define the game mechanics: That will be used in the gameto engage and motivate students. Create Game Mechanics. To encourage learning, the game could, for instance, use gamification strategies like points, badges, and leaderboards. Develop the Game Backend: To build the game's logic and functionality, developers must use Python to develop the game's backend. The game's rules, certificate, and feedbackmechanics have to be implemented.
- Design the Game Frontend: Build the user interface, animations and interactions for the game's frontend using the Ren'Py. At this level, the backend logic and game mechanicsare integrated into the user interface.
- Test and Debug the Game: Test and debug the game to makesure it runs smoothly and is error-free. In this step, usability tests are carried out and input frame stakeholders, includingstudents, are gathered.
- Deploy the Game: After the game has been tested and fixed,release it on the platform that better serves the target audience. In our case, This is a Web Application which is accessible from anywhere and on any computational mobile and desktop device.
- Analyze the effectiveness of the game by gathering information on user happiness, learning outcomes, and user engagement. Use this information to finetune and enhance the game for future versions
- By using this process, game developers can produce a successful cyber security awareness game that enthuses kids and instructs them on critical cyber security principles and best practices.

## IV. TECHNOLOGIES

While creating the CYBER WARRIORS game we have used technolo-gies to fulfill our motto of cyber warrior game. The technologieswe used are as follows :

- Ren'Py - Ren'Py is an interactive storytelling engine de- signed for creating visual novels and life simulation games for computers and mobile devices. It enables users to com- bine words, images and sounds to craft engaging narratives. Ren'Py features a user-friendly script language that facilitates the creation of extensive visual novels, while its integration with Python allows for the development of morecomplex simulation games. It is an open-source platform available for commercial use at no cost. We have implemented our game by using the Ren'Py. Now the reason tochoose Ren'Py is because it provides better graphics thanany other. It is the library of Python so here we also comewith our Python language. By using Ren'Py we have createdall 3 levels in our game. Ren'Py helps us publish our game as a website or mobile application. So it was very beneficialfor us as well as for our users.
- Figma - We used figma for the pictorial representation togive our game a realistic look
- Google Slide - We have used Google Slide for the templateof the completion certificate.
- Google Forms– We have used Google Forms as we need totake input from the user as their name, and email ID so we will provide them a certificate with their name.
- Google sheet – To store the data of the Google form and provide them with the certificate via their mail so this tech-nology is used for that
- Autocrat – It is a free add-on that can create PDFs or shareddocuments from spreadsheet data. It uses merge tags to iden-tify which fields to merge, and a template to merge the data into a document.

## V. SYSTEM DESIGN

I. User Interface: There are built-in options for Start, Load, Skip, back, and Quit which allows the user to play the game effortlessly.
II. Game levels: The game levels are based on different cybercrime scenarios that players have to overcome to win.
III. Feedback and Rewards: After completion of the game, the user will get a certificate through the mail by filling out the Google form.
IV. GamePlay: In this game, players are lured into doing unethical things which can lead to hacking of the system by the hacker.

## VI. SYSTEM ARCHITECTURE.

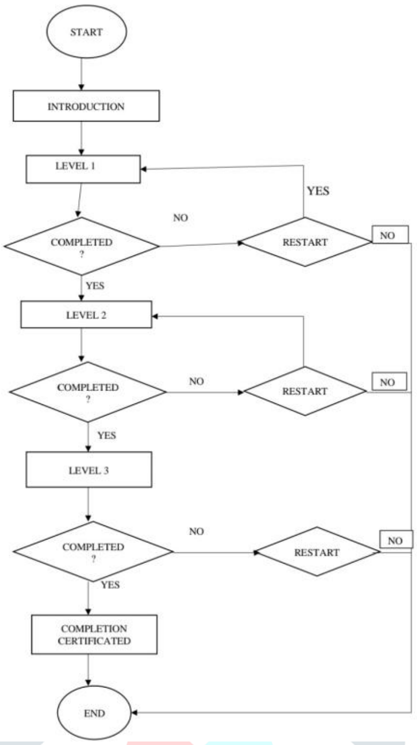


Figure 1: FLOWCHART OF SYSTEM

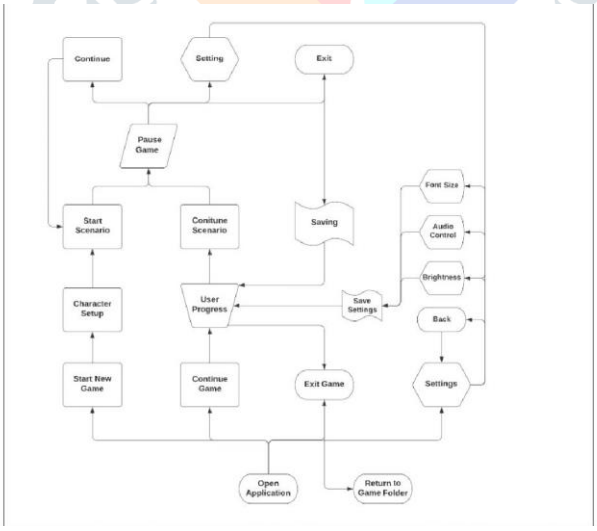


Figure 2 : BLOCK DIAGRAM

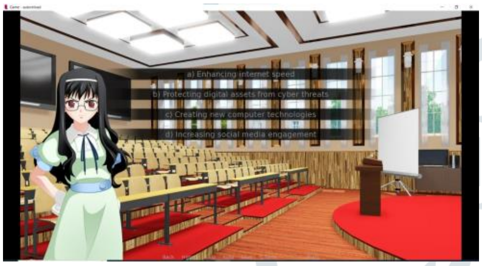
A game built to create awareness amongst teenagers with a fun way of learning. The application will have a character which will guide you through the game. It will start with an introduction tocybersecurity news - of how it's affecting everyone and have them trained through the game through question and answers. It will simulate the whole process of scams that happen through fake mes-sages, emails and calls and how to avoid it is the motive of winning this game. Players can check their scores on the scoreboard. Thiswill create an awareness among teenagers to gain cybersecurity knowledge.

- Level 1 – After choosing the character there will be instruc- tions for the reader with the knowledge of cybersecurity.Like what exactly is cybersecurity? various news of cyber-security fraud Details of the level At this level, they onlyhave to read all the news and definitions of cybersecurityand then they have to pass one MCQ test based on the same.On this basis, they will get marks on the scoreboard. [6] Certainly! Here's a scenario tailored for school-going stu-dents who are new to cybersecurity:
- Scenario: Amy is a high school student who loves spending time online, chatting with friends, playing games, and doingresearch for school projects. One day, while browsing the internet, she comes across a website claiming to offer free downloads of popular games and apps. Excited about the prospect of getting new games without paying, Amy clicks on the download button and installs the software on her computer. However, shortly after installing the software, Amy notices that her computer starts behaving strangely. Pop-up ads appear frequently, her computer slows

down, andshe receives a strange email asking for personal information.Concerned about the security of her computer and her online accounts, Amy seeks advice on how to stay safe online.

- Level 2 - Now in these levels, users enter with lots of knowl-edge of cybersecurity and they will get fraud messages For eg: Congratulations you won an iPhone 14 pro to claim theseyou have to just contact them - Now if the user knows level 1better they will decline it. If they accept it then the visitationmessage comes to their bank account/voice message From that, they will learn what exactly we did. If users accept the message then it will deduct their marks and increase their cybersecurity knowledge. [6]
- Level 3 - Now at this level, users enter with lots of knowledge and experience In these we Give them more tasks Like fraudemail or getting a Job by giving a particular amount. We will provide them with real effects of the environment like com- pany information, payment methods and all. There are somegenuinely true emails. So at this level, users have to decide what is right and wrong depending on that only they will get or lose their marks. After all again with their particular criteria of marks, they will get a certificate of completion.If they are not qualified they have to start again so it will increase their knowledge and the moto of the educational game will be fulfilled. [6]

## VII. IMPLEMENTATION



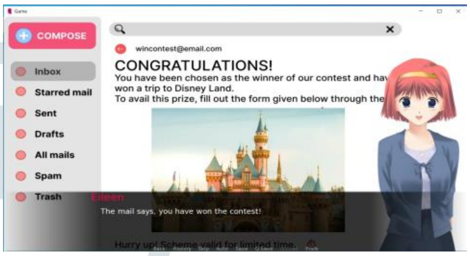
a) Enhancing internet speed

b) Protecting digital assets from cyber threats

c) Creating new computer technologies

d) Increasing social media engagement

LEVEL 1



wincontest@email.com

CONGRATULATIONS!

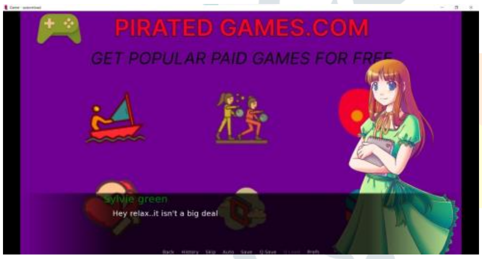
You have been chosen as the winner of our contest and hav
won a trip to Disney Land.
To avail this prize, fill out the form given below through the

Hurry up! Scheme valid for limited time.

Eileen

The mail says, you have won the contest!

LEVEL 2



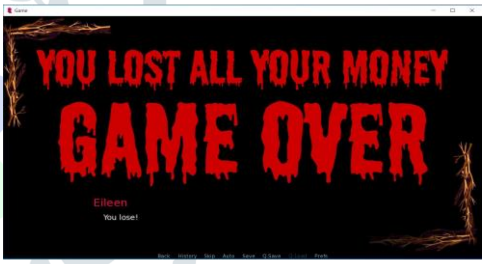
PIRATED GAMES.COM

GET POPULAR PAID GAMES FOR FREE

sylvie green

Hey relax..it isn't a big deal

LEVEL 3



Eileen

You lose!

LOST GAME

## VIII. CONCLUSION

Conclusion Since cyber security threats are getting more complex and common, it is important to inform kids about the dangers and how to stay safe. Lectures and videos, which are common teachingtools for cyber security awareness, can be dull and monotonous. By offering a different and interesting approach to teaching stu-dents about cybersecurity awareness, the Cyber Security Aware-ness Game makes learning enjoyable and memorable. Students canhone their critical thinking skills, strengthen their ability to make decisions and gain a greater understanding of the dangers and con-sequences of cyberattacks by taking part in this game. We have used technologies like Ren’Py, Figma and Python. The proposed project can help the future generation to have prior knowledge of cyber-attacks and cybersecurity on social media. The visual aids and animations would help generate more interest in students in cybersecurity./ This game hence not only attracts young audiences with its cartoonish characters and background but also Multiple decisions are given to the user to be made just like in real life in a single day we make multiple decisions and each decision changes how the day turns out to be. This decision-making ability is naturalto humans and is followed from a very early age hence imple- menting this in the game allows the user to experience the game more immersive and the game in all feels realistic. Whole games allow users to take that first-hand experience of falling into traps and scams of cyber attackers. The best way to learn is to learn through experience and failures. Even though such a sensitive topic is taught without any long theory hence not making the audience bored. Even so, since the game is focused on teens from ages 12-18 attractive characters and backgrounds give it a very friendly feel.

## IX. FUTURE SCOPE

In our future work, we are going to have more designed experi-mentation to discover more attacks and real cases t for different target groups. Furthermore, we are going to gamify some other critical issues that are usually included in cyber security awareness campaigns such as plagiarism. Our target groups will be mainlyschool students, who currently have less information security skills and capabilities, however, they need it soon when there will be realrisks. [2]

## X. ACKNOWKEDEMENT

I would like to thank my guide, Prof. Shraddha Sushant Rokade from the Computer Engineering Department, Usha Mittal Institute of Technology for her support and guidance.

## XI. CONCLUSION

[1] CYBERAWARE: A Mobile Gamebased App For Cyber-security Education And Awareness”; Filippos Giannakas, Georgios Kambourakis And Stefanos Gritzalis

[2] CYBERHERO: A Gamification Framework For Cyber Security Awareness For High Schools Students; Hani Qusa, Jumana Tarazi.

[3] Research Paper On Cybersecurity; Mrs. Ashwini Sheth, Mr Sachin Bhosale, Mr Farish Kurupkar

[4] Application Of The Educational Game To Enhance Stu- dent Learning; Siu Yin Cheung, Kai Yin Ng.

[5] Cyber Security Education for Children through Gamifi- cation: Challenges and Research Perspectives

[6] https://www.Ren’Py.org/doc/html/index.html.