Towards Inclusive Cybersecurity Learning: A Novice-Friendly Capture-the-Flag Onboarding Platform

Lik Ken Chen
Forensics and Cyber Security Research Centre
Asia Pacific University of Technology and Innovation (APU)
Kuala Lumpur, Malaysia
chenlikken@hotmail.com

Mohd Hanis Jenalis
School of Technology
Asia Pacific University of Technology and Innovation (APU)
Kuala Lumpur, Malaysia
mohd.hanis@apu.edu.my

Julia Juremi
Forensics and Cyber Security Research Centre
Asia Pacific University of Technology and Innovation (APU)
Kuala Lumpur, Malaysia
julia.juremi@apu.edu.my

***Abstract* — Cybersecurity has evolved into a global imperative driven by a surge in cyber-attacks and an acute shortage of cybersecurity experts. To address this challenge, gamification, which is the term used for incorporating game-like elements, has become a popular approach in cyber security education to attract, train, and retain cybersecurity talents. Among the methods embraced in this field, Capture-the-Flag (CTF) competitions and models have emerged as a prevalent means for educators to implement gamification and foster practical cybersecurity skills. However, CTFs can sometimes be intimidating and not beginner-friendly. To address this issue, this research aims to propose a beginner-friendly and supportive CTF onboarding platform for novices in cybersecurity. The targeted respondents for this research are Malaysian novice CTF players and cybersecurity educators, with 100 CTF players and 5 educators. An online survey was conducted using a digital questionnaire, and the results show the importance of an introductory platform for novices in the field. However, more work needs to be done in the future to develop a framework for designing and organizing CTFs that are engaging and educational for all levels of learners.**

Keywords— Capture the flag, gamification, cybersecurity, education, beginner-friendly

I. INTRODUCTION

In recent years, with the number of cyber-attacks on the rise, cybersecurity has become a critical global issue (Nor Azlina et al., 2022). The situation becomes even more pressing as there is also a worldwide shortage of cybersecurity professionals with a drastic 3.4 million people workforce gap ((ISC)^2, 2022). Therefore, governments, educational institutions, researchers, and private companies are actively looking into more effective ways to attract, train, and retain talents in the cybersecurity field.

One such approach that has gained popularity in recent times is the integration of gamification into cybersecurity education. Gamification leverages game-like elements to enhance the learning experience, making it not only informative but also fun and engaging at the same time (Poondej & Lerdpornkulrat, 2016). A particularly popular method of gamifying cybersecurity education is the incorporation of Capture-the-Flag (CTF) events and models into curricula and assessments (Kaplan et al., 2022).

CTFs are commonly referred to as cybersecurity competitions where participants will solve a range of cybersecurity-themed tasks (challenges) to "capture" hidden "flags", where the flags are typically represented as strings of characters, numbers, and/or special characters. The participants must locate these flags and submit them on the CTF platform in exchange for points. Depending on the CTF format, individuals or teams will compete to accumulate the highest number of points and the top scorer or team will emerge as the CTF victor (European Union Agency for Cybersecurity, 2021).

Cybersecurity professionals or lecturers often encourage those who are interested in cybersecurity to participate in CTFs so that they can gain exposure, skills and knowledge. It was believed that CTFs offer an interactive way for individuals to effectively acquire and practice a range of cybersecurity skills (Trickel et al., 2017; Nor Azlina Abd Rahman et al., 2023).

However, it might not be a good idea for students or beginners in the field who have plenty of interest but zero or little knowledge and skills to join CTFs without sufficient exposure, training or preparation. Before CTFs were introduced to the education sector, they were initially used as a platform for hackers to demonstrate their skills and compare themselves with their peers (Cowan et al., 2003). Therefore, the style of CTFs can sometimes be too competitive and somewhat humbling for novices.

In this paper, an introductory CTF onboarding platform is proposed to gently introduce CTFs to beginners and build up their confidence to join CTFs.

II. LITERATURE REVIEW

A. Cybersecurity Education

Cybersecurity education refers to education and training in the field of cybersecurity (European Union Agency for Cybersecurity, 2020). Due to the interdisciplinary nature of cybersecurity (Furnell et al., 2022), it encompasses various topics, including but not limited to security testing and audit, web security, cryptography, security policies, and secure coding (McGettrick, 2013). Cybersecurity education is crucial to equip individuals with cybersecurity knowledge and skills so that one, fewer people will be susceptible to cyber threats (Rahman et al., 2020) and two, the global shortfall of cybersecurity professionals can be mitigated (Vykopal & Barták, 2016).

1) Evolution of Cybersecurity Education: The Švábenský et al. (2019) review of cybersecurity education papers reveals the two main approaches for teaching cybersecurity. The first approach is via conventional lecture-based teaching where this method of education focuses on the instructor imparting

knowledge to students and is mainly theory-based with little hands-on and practical elements. Preparation for teaching will take little time and the course materials need only to be prepared once. However, the learners' capabilities and needs can be overlooked. This method of teaching is common in most educational establishments where textbooks and case studies will be used as teaching materials (Mirkovic & Peterson, 2014; Langner et al., 2022).

The second approach is using hands-on exercises. This education method provides practical education using teaching materials like online hacking exercises to expose students to security concepts and vulnerabilities (Votipka et al., 2021). By incorporating hands-on exercises in cybersecurity education, students' comprehension and retention of the topic taught will be enhanced (Kalyanam et al., 2020). It is also believed that students will have a more enjoyable learning experience while allowing them to discover how to apply theoretical security concepts in the real world (McDaniel et al., 2016; Vykopal et al., 2020). Additionally, this approach will allow instructors to choose how much guidance to provide students with so that the students can hone their analysis skills (Weiss et al., 2016).

Nevertheless, the most popular method for cybersecurity education nowadays is a combination of lectures and some laboratory exercises (Workman et al., 2021). However, European Union Agency for Cybersecurity (2020) has reported that the current cybersecurity education and training system has failed to encourage students to get into cybersecurity and equip them with the appropriate skills and knowledge. Crick et al. (2019) also stated that traditional lecturing is not a good method for teaching cybersecurity.

Therefore, cybersecurity education has started moving away from traditional classroom-based learning to more practical approaches, such as hands-on learning, simulations, and particularly gamification (Workman et al., 2021). A good example of the shift can be seen in the work of Tseng et al. (2022) where they developed a board game, named "iMonsters" with a self-evolving algorithm on attack and defense knowledge to teach students sophisticated cybersecurity concepts. Their study revealed that this gamified approach outperformed traditional classroom learning. Kaplan et al. (2022) have also applied gamification into cybersecurity curricula by incorporating jeopardy-style CTF challenges, and they found that the students' engagement and perceived learning improved. Additionally, Wolfenden (2019) confirmed that gamifying cybersecurity can increase student engagement and encourage continuous learning.

To conclude, the integration of hands-on experiences and gamification is quickly becoming the norm in preparing future cybersecurity professionals. This growing trend indirectly highlights the urgent necessity for a CTF onboarding platform, given that CTFs are widely adopted and effective in gamifying cybersecurity education.

B. Capture The Flag (CTF)

According to Raman et al. (2014), there are 3 different formats of CTFs: attack-defence, jeopardy and mixed. In attack-defence CTFs, every participating team is provided with an identical machine that is designed to have a few vulnerable services. To get points, the teams need to exploit the vulnerabilities in other teams' machines, gain access to their services to extract the flag and submit it. They also need to patch the vulnerabilities of their own machine's services to avoid losing points. In Jeopardy-style CTFs, a variety of cybersecurity-related tasks (challenges) are provided. When players successfully solve the challenges, they are rewarded with the flag. The players can then submit the flag for points. Sometimes, there can be a format for the flag, for example, "ABOH23{flag}" (Nor Azlina Abd Rahman et al., 2023).

However, there seem to be new CTF formats as Cole (2022) and Kucek & Leitner (2020) mentioned some other formats of CTFs like King of the Hill (KotH) where players compete to gain access to a neutral resource, normally a server, and points are awarded for the control duration. On the other hand, hack quest CTFs embed challenges in a video game. Lastly, there are also quiz-style CTFs where players answer questions on cybersecurity. In all formats, the participants are ranked based on their points and the player(s)/team(s) with the most points win.

1) CTF and Cybersecurity Education: CTFs have been brought into the education sector to become a part of cybersecurity education for many reasons but in general, the main motive was to introduce, educate and test students on the broad spectrum of cybersecurity knowledge, skills and tools (Burns et al., 2017; McDaniel et al., 2016; Nor Azlina et al., 2022, 2023; Švábenský et al., 2020). Pusey et al. (2014) even added that the purpose of having CTF competitions was to foster competent cybersecurity practitioners. Bertrand et al. (2020) also stated that CTF competitions are the starting point for attracting and retaining young talents in the cybersecurity workforce.

The benefits of CTFs can be seen in Carlisle et al. (2015) where CTFs help motivate students to carry out self-directed learning and go all out for knowledge. Leune & Petrilli (2017) and Zack et al. (2022) also found that CTF sessions increase students' confidence, student engagement and practical skill development. According to Sener (2016), CTFs have multiple roles in cybersecurity education including motivating students, providing comprehensive learning experience with both theoretical and practical aspects, as well as talent identification and development.

However, Chung & Cohen (2014) proved that CTFs are not always beneficial for everyone. They can have often unnecessarily ambiguous or difficult challenges, challenges with inappropriate point values (Vykopal et al., 2020; Votipka et al., 2021), and unstable websites. Also, they are often not beginner-friendly. Ahmad Haziq Ashrofie Hanafi et al. (2021) and Mirkovic & Peterson (2014) confirmed that the number of participants interested in CTFs and cybersecurity education dropped after participating in CTFs. That said, it can be argued that CTFs help participants clarify if they are suited to work in the field of cybersecurity (Sener, 2016). Nonetheless, Feng (2015) stated that the unguided nature of CTFs is not effective for learning as compared to guided learning and Weiss et al. (2016) added that a balance should be struck between guided and independent cybersecurity learning.

In summary, this literature review highlights the evolution of methods for teaching and learning cybersecurity, demonstrating a notable shift towards practical approaches such as hands-on exercises and competitions. These methods are believed to provide students with the opportunity to gain or practice various cybersecurity skills in a more engaging

and entertaining way. That being said, while the practical approach has been shown to be effective, with CTF events being a popular gamification method, it is essential to acknowledge and address certain limitations. One notable concern is the potential intimidation factor which may deter novices and interested individuals from entering the cybersecurity industry or sector. Thus, there is a need for more platforms to gently introduce CTFs and help guide novices in the field towards becoming proficient cybersecurity professionals.

C. Similar Systems

As the proposed system is a CTF platform for introducing CTFs to beginners, two similar systems namely picoGym and SKR CTF will be discussed in this section.

picoGym: picoGym is an online platform for one to practice solving CTF challenges where most of the challenges are from past picoCTF competitions. While its primary target users are high school students, CTF players, hackers and cybersecurity professionals are all welcome to hone their skills on the platform. The challenge repository is updated regularly and there are 7 categories of challenges in total, namely binary exploitation, web exploitation, reverse engineering, cryptography, forensics, general skills and uncategorized. Users can determine the difficulty of the challenges by evaluating the point values of the challenges and the number of solves and likes. A user's progress can be tracked by the number of solves for each category and his/her total score (Carnegie Mellon University, n.d.-a; n.d.-b). Fig 1. shows the user interface of picoGym.

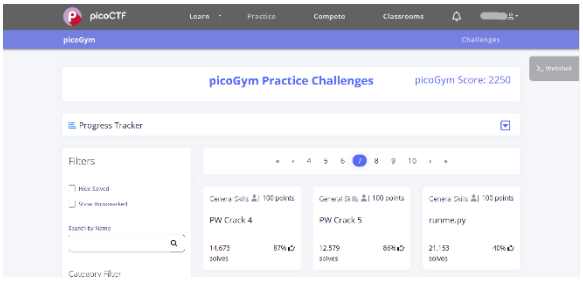

Fig. 1. picoGym Practice Challenges (Carnegie Mellon University, n.d.-b)

1) SKR CTF: SKR CTF is a website developed by a Malaysian CTF team named "SKR", to teach beginners on cybersecurity knowledge and CTFs (SKR, n.d.-a).

There are 12 categories of challenges in total, including tutorial (warm up), web, cryptography, forensics, reverse engineering, binary, linux, steganography, mini game, OSINT, programming, and miscellaneous. The difficulty levels for the challenges are provided and the platform contains a scoreboard, web shell and learning materials (SKR, n.d.-b).

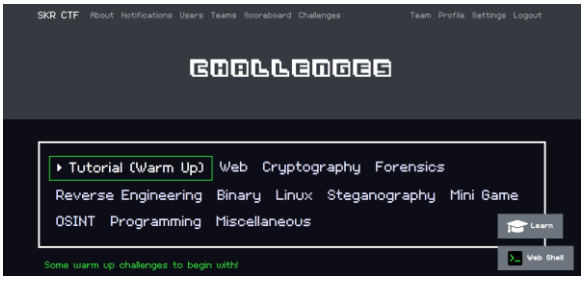

Fig. 2. SKR CTF Challenges (SKR, n.d.-b)

D. Comparison of Similar Systems

TABLE I. FEATURE COMPARISON BETWEEN PICOGYM AND SKR CTF

Features	picoGym	SKR CTF
Learning Path	○	●
Recommended Challenge Solution	○	○
Challenge Rating System	●	●
Challenge Learning Outcome Summary	○	○
Challenge Hints	◘	◘

[a.] Each column indicates whether a platform has implemented the features fully (●), partially (◘), or not at all (○).

Table I shows the features implemented on both platforms. SKR CTF has designed some sort of a learning path for players to solve their challenges by locking the more difficult challenges before the easier challenges are solved but picoGym does not have a learning path. picoGym has a challenge rating system where a player can give a thumbs up or thumbs down reaction to the challenge while SKR CTF allows players to rate challenges by giving a heart reaction. However, some challenges on both platforms have insufficient hints or no hints at all. Furthermore, neither platform provides recommended solutions for the challenges and a summary of the expected learning outcomes from solving the challenges.

Hence, although these two platforms target the novices in the field of cybersecurity and aim to provide a place for them to prepare for CTF competitions, there are still many features that can be implemented for a more beginner-friendly CTF introductory process. So, the CTF platform proposed in this paper will include learning paths, recommended challenge solutions, a challenge rating system, challenge learning outcome summaries and hints for challenges as its features.

III. PROBLEM STATEMENT

CTFs are not exactly beginner-friendly. They have evolved to become more complex and difficult by the year (USENIX, 2014). This has caused many players, particularly novices who were new but interested in cybersecurity to be taken aback by the complexity and difficulty of the challenges (T. Z., Wang, personal communication, January 29, 2023). Novices do not know which tools are needed to solve the challenges or have the pre-requisite knowledge to even understand them (Bertrand et al., 2020; Burns et al., 2017; Thomas et al., 2019). The newcomers felt alienated, frustrated, less engaged, intimidated, overwhelmed, and lost self-confidence as they could not solve most, if not all of the challenges unlike the other more experienced competitors (Chung & Cohen, 2014; Mirkovic et al., 2015; Pusey et al., 2014; Thomas et al., 2019; Tobey et al., 2014; Vykopal & Barták, 2016; Vykopal et al., 2020). This influenced them to

stop playing CTFs and some of them even lost interest in pursuing further cybersecurity education (Ahmad Haziq Ashrofie Hanafi et al., 2021; Mirkovic & Peterson, 2014). S. Alizadeh, a lecturer teaching the Practical CTF Strategies module at Asia Pacific University of Technology & Innovation (APU), explained that he lost interest in CTFs after his friend showed him a very difficult challenge when introducing him to CTFs (personal communication, January 18, 2023).

Not only that, the points allocated for the CTF challenges which are often used by players as a metric for measuring challenge difficulty, are often inappropriately allocated (Chung & Cohen, 2014; Vykopal et al., 2020; Votipka et al., 2021). Moreover, CTF players are so focused on capturing the flag and increasing their points that their focus has shifted from learning about cybersecurity to competing (S. Alizadeh, personal communication, January 30, 2023).

Additionally, there are very limited writeups, also commonly known as the CTF players' solutions to the CTF challenges, published online which makes it harder for the CTF community to learn (Švábenský et al., 2020). It is also common for CTF challenges to provide vague or confusing descriptions and hints, or not have hints at all (Chung & Cohen, 2014; Cole, 2022). Sometimes, even when hints are provided, they are not useful for the players, making them hesitant to exchange points for hints (Votipka et al., 2021; Vykopal & Barták, 2016; Vykopal et al., 2020). Hints directing participants to the relevant learning materials are even rarer as self-learning and exploration is the norm in CTFs (Weiss et al., 2016). However, Kirschner et al. (2006) and Feng (2015) confirmed that this method of minimal guidance learning which is common in CTFs is not an effective way of learning as compared to strong instructional guidance and this can be applied to both novices and also veterans in the field.

This situation worsens particularly in Malaysia as most Malaysian students only start learning about computing when they reach college or university levels (Khoo, 2019). Moreover, the teachers in schools have insufficient knowledge of computational thinking skills and lack proper guidelines to teach computer science (Puganesri & Saifullizam Puteh, 2019). As a result, Malaysian students miss out on vital foundational knowledge in computing that is usually taught at earlier levels of education in other countries (Seow et al., 2019; Ministry of Education, Singapore, n.d.). This presents a challenge for young talents in Malaysia who are interested in cybersecurity as they have to acquire both computing and cybersecurity-related knowledge while trying to keep pace with their international counterparts. Not only that, but Malaysian university students will also need to take up certain subjects like the General Education Subjects (GES), more commonly known as Mata Pelajaran Umum (MPU) amongst Malaysians which further increases their burden (Curtin University Malaysia, 2023).

With that said, there has not been extensive research conducted on the aforementioned topic, particularly in the context of Malaysia. These issues have not garnered significant attention, as many cybersecurity novices in Malaysia remain hesitant to participate in CTF competitions (S. Alizadeh, personal communication, January 30, 2023). In conclusion, all the challenges identified in existing CTFs can be resolved by introducing a beginner-friendly CTF onboarding platform.

IV. Research Aims

This research aims to propose a beginner-friendly and supportive Jeopardy-style CTF onboarding platform to help novices in cybersecurity participate in Jeopardy-style CTFs confidently.

V. Research Objectives

i) To develop a user-friendly platform for learning about Jeopardy-style CTFs using clear, simple language and illustrations.

ii) To create a clear and organised learning journey for novice players by separating the easier challenges from the more complex ones.

iii) To design CTF challenges that effectively educate players on the various aspects of cybersecurity by providing clear descriptions and informative hints.

iv) To enable players to evaluate challenges through the implementation of a challenge rating system.

VI. Research Questions

i) How to develop a user-friendly platform for learning about Jeopardy-style CTF competitions using clear, simple language and illustrations?

ii) How to create a clear and organised learning journey for novice players by separating the easier challenges from the more complex ones?

iii) How to design CTF challenges that effectively educate players on the various aspects of cybersecurity by providing clear descriptions and informative hints?

iv) How to enable players to evaluate challenges through the implementation of a challenge rating system?

VII. Research Significance

The results of this study can bring significant benefits to cybersecurity professionals, educators, governments, cybersecurity companies, students, and CTF players. Governments and companies in the field of cybersecurity will attract, inspire and retain more young talents to join the cybersecurity workforce. Educators will be able to use the proposed system in their classes to facilitate teaching and learning processes, providing an interactive and engaging learning experience for their students. Besides that, as CTF challenges are simulations of real-world security vulnerabilities and problems, educators will have more relevant teaching materials and easily demonstrate the security concepts taught in classes. Students could learn cybersecurity concepts and CTF strategies at their own pace through a gamified approach and apply what they have learnt in a practical setting while thinking critically and creatively in the process, encouraging active learning. Cybersecurity professionals and CTF players will also have a place to practice and reinforce their knowledge and skills in cybersecurity.

VIII. Methodology

The targeted respondents of this research are Malaysian novice CTF players and cybersecurity educators. The sample size of CTF players will be 100 while for educators, only 5 will be chosen as the sample. Judgement sampling will be used

as the sampling method in this research. This is because the targeted population is quite specific and limited. Using this sampling method, the representative sample will be assembled by the Forensics and Cyber Security Research Center (FSeC) of Asia Pacific University of Technology & Innovation, Malaysia. An online survey will be conducted by distributing a digital questionnaire containing 3 sections with 4-point Likert scale and multiple-choice questions to the respondents.

IX. Overview of the Proposed System

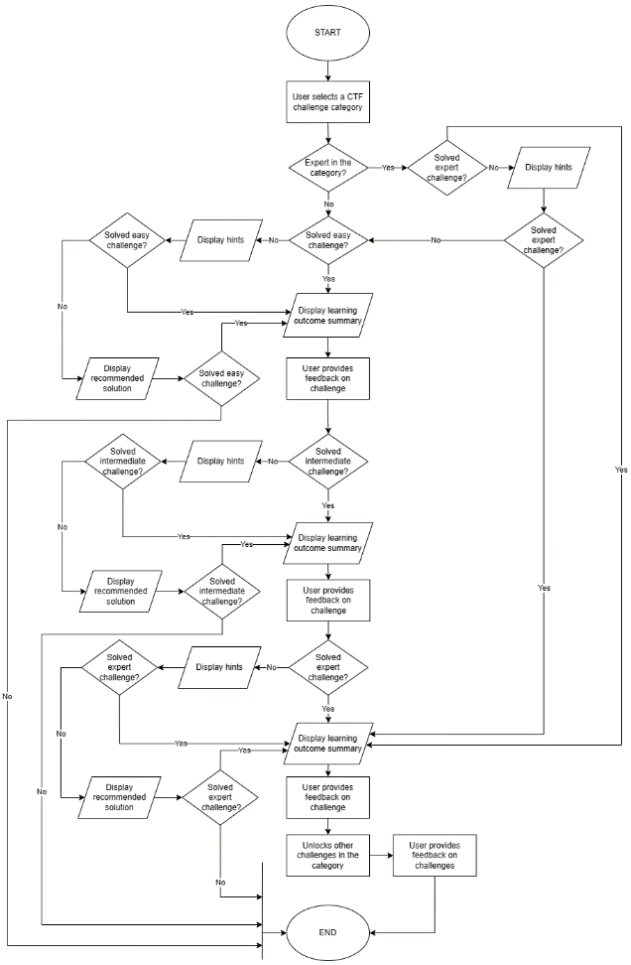

Fig. 3. Flow Chart of Proposed System

This section discusses the overview of the proposed CTF platform. The flow of the proposed system is shown in figure 3. First, a user picks a CTF challenge category to solve challenges on. If the user thinks that he or she is an expert in the category, the user can solve the expert-level challenge using only hints as the supporting materials and if it is solved successfully, the learning outcome summary for the challenge will be displayed and the rest of the challenges in that category will be unlocked directly. On the other hand, if the user fails to solve the challenge with only hints or the user is not an expert in the category, they will need to solve the easy, intermediate and expert-level challenges sequentially to unlock the other challenges in the category. Hints and recommended solutions will be provided to help them. After solving any challenge, users will be prompted to provide feedback on the challenge. However, if the user fails to solve the challenge with both hints and the recommended solution provided, they will not be able to proceed to the next level or unlock the rest of the challenges.

X. Conclusion

In conclusion, this research aims to address the challenges faced by individuals new to the field of CTFs by providing an introductory platform that guides them through their learning journey. This platform offers a unique approach compared to traditional CTFs, which can often be overwhelming and challenging for beginners. By providing recommended solutions, more hints and using easy language, novices will have a better understanding and experience of CTFs. However, while this research is a step in the right direction, more work needs to be done to address the root cause of the problem which is the underlying challenges in CTFs in the education sector. Future research can focus on developing a framework for designing and organising CTFs in a way that is more engaging and educational for all levels of learners.

Acknowledgement

Special appreciation goes to Maxis Broadband Sdn. Bhd. for the kind sponsorship that supported the academic endeavours contributing to this research paper. Last but not least, we sincerely thank Asia Pacific University of Technology & Innovation and its Forensics and Cyber Security Research Centre for this publication opportunity.

References

(ISC)^2. (2022). *(ISC)2 CYBERSECURITY WORKFORCE STUDY*. Retrieved February 3, 2023, from https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx

Ahmad Haziq Ashrofie Hanafi, Haikal Rokman, Ahmad Dahaqin Ibrahim, Zul-Azri Ibrahim, Md Nabil Ahmad Zawawi & Fiza Abdul Rahim. (2021). A CTF-based approach in cyber security education for secondary school students. *Electronic Journal of Computer Science and Information Technology, 7*(1), 1-8. https://doi.org/10.52650/ejcsit.v7i1.107

Bertrand, J. I., Martakis, A., Liu, H., Zhong, C., & Yao, J. (2020). Exploring participants' views of cybersecurity competitions through the lens of social media. *2020 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA)*, 155-162. https://doi.org/10.1109/cogsima49017.2020.9216073

Burns, T. J., Rios, S. C., Jordan, T. K., Gu, Q., & Underwood, T. (2017). Analysis and exercises for engaging beginners in online CTF competitions for security education. *USENIX Security Symposium*. https://www.usenix.org/system/files/conference/ase17/ase17_paper_burns.pdf

Carlisle, M., Chiaramonte, M., & Caswell, D. (2015). Using CTFs for an undergraduate cyber education. *2015 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 15)*. https://www.usenix.org/system/files/conference/3gse15/3gse15-carlisle.pdf

Carnegie Mellon University. (n.d.-a). *What is picoCTF?* Retrieved February 4, 2023, from https://picoctf.org/

Carnegie Mellon University. (n.d.-b). *picoGym Practice Challenges*. Retrieved February 4, 2023, from https://play.picoctf.org/practice?page=7

Chung, K. C., & Cohen, J. (2014). Learning obstacles in the capture the flag model. *Genetics Selection Evolution*. https://www.usenix.org/system/files/conference/3gse14/3gse14-chung.pdf

Cole, S. V. (2022). Impact of capture the flag (CTF)-style vs. traditional exercises in an introductory computer security class. *Proceedings of the 27th ACM Conference on Innovation and Technology in Computer Science Education Vol. 1*, 470-476. https://doi.org/10.1145/3502718.3524806

Cowan, C., Arnold, S., Beattie, S., Wright, C., & Viega, J. (2003). Defcon Capture the Flag: Defending vulnerable code from intense attack. *Proceedings DARPA Information Survivability Conference and Exposition*. https://doi.org/10.1109/discex.2003.1194878

Crick, T., Davenport, J.H., Irons, A., & Prickett, T. (2019). A UK case study on cybersecurity education and accreditation. *2019 IEEE Frontiers in Education Conference (FIE)*, 1-9. 10.1109/FIE43999.2019.9028407

Curtin University Malaysia. (2023, 18 September). *MoHE Compulsory Subjects*. https://humanities.curtin.edu.my/departments/mpu/mohe/

European Union Agency for Cybersecurity. (2020). *Cybersecurity skills development in the EU*. https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union

European Union Agency for Cybersecurity. (2021). *Capture-The-Flag competitions: All you ever wanted to know!* https://www.enisa.europa.eu/news/enisa-news/capture-the-flag-competitions-all-you-ever-wanted-to-know

Feng, W. (2015). A scaffolded, metamorphic CTF for reverse engineering. *2015 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 15)*. https://www.usenix.org/system/files/conference/3gse15/3gse15-feng.pdf

Furnell, S., Langner, G., Tokola, T., Andriessen, J., Quirchmayr, G., & Luciano, C. (2022). Collaborative cybersecurity learning: Establishing educator and learner expectations and requirements. *Information Security Education-Adapting to the Fourth Industrial Revolution: 15th IFIP WG 11.8 World Conference, WISE 2022, Copenhagen, Denmark, June 13–15, 2022, Proceedings*. 46-59. https://doi.org/10.1007/978-3-031-08172-9_4

Kalyanam, R., Yang, B., Willis, C., Lambert, M., & Kirkpatrick, C. (2020). CHEESE: Cyber human ecosystem of engaged security education. *2020 IEEE Frontiers in Education Conference (FIE)*, 1-7. https://doi.org/10.1109/fie44824.2020.9273931

Kaplan, Z., Zhang, N., & Cole, S.V. (2022). A Capture The Flag (CTF) platform and exercises for an intro to computer security class. *Proceedings of the 27th ACM Conference on Innovation and Technology in Computer Science Education Vol. 2*, 597-598. https://doi.org/10.1145/3502717.3532153

Khoo, L. J. (2019). Design and develop a cybersecurity education framework using Capture The Flag (CTF). *Design, Motivation, and Frameworks in Game-Based Learning*, 123–153. https://doi.org/10.4018/978-1-5225-6026-5.ch005

Kirschner, P. A., Sweller, J., & Clark, R. E. (2006). Why minimal guidance during instruction does not work: An analysis of the failure of constructivist, discovery, problem-based, experiential, and inquiry-based teaching. *Educational Psychologist*, *41*(2), 75–86. https://doi.org/10.1207/s15326985ep4102_1

Kucek, S., & Leitner, M. (2020). An empirical survey of functions and configurations of open-source capture the flag (CTF) environments. *Journal of Network and Computer Applications*, *151*, 102470. https://doi.org/10.1016/j.jnca.2019.102470

Langner, G., Skopik, F., Furnell, S., & Quirchmayr, G. (2022). A tailored model for cyber security education utilizing a cyber range. *ICISSP*, 365-377. https://www.skopik.at/ait/2022_icissp.pdf

Leune, K., & Petrilli, S.J. (2017). Using Capture-the-Flag to enhance the effectiveness of cybersecurity education. *Proceedings of the 18th Annual Conference on Information Technology Education (SIGITE '17)*, 47-52. https://doi.org/10.1145/3125659.3125686

McDaniel, L., Talvi, E., & Hay, B. (2016). Capture the Flag as cyber security introduction. *Proceedings of the 2016 49th Hawaii International Conference on System Sciences (HICSS)*, 5479-5486. https://doi.org/10.1109/HICSS.2016.677

McGettrick, A. (2013). Toward effective cybersecurity education. *IEEE Security & Privacy*, *11*(6), 66–68. https://doi.org/10.1109/MSP.2013.155

Ministry of Education, Singapore. (n.d.). *Strengthening Digital Literacy*. Retrieved February 3, 2023, from https://www.moe.gov.sg/microsites/cos2020/refreshing-our-curriculum/strengthen-digital-literacy.html

Mirkovic, J., & Peterson, P. A. (2014). Class Capture-the-Flag exercises. *Genetics Selection Evolution*. https://www.deter-project.org/sites/info.deterlab.net/files/files/class%20capture-the-flag%20exercises_mirkovic_peterson_usc%20isi_august_2014.pdf

Mirkovic, J., Tabor, A., Woo, S. S., & Pusey, P. (2015). Engaging novices in cybersecurity competitions: A vision and lessons learned at ACM Tapia 2015. *2015 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 15)*. https://www.usenix.org/system/files/conference/3gse15/3gse15-mirkovic.pdf

Nor Azlina Abd Rahman, Ibiwani Alisa Hussain, Noris Ismail, Jojo, H. & Khan, Y. (2022). Millennial psychology towards hacking activities. *Journal of Applied Technology and Innovation*. *6*(2). 22. https://jati.sites.apiit.edu.my/files/2022/03/Volume6_Issue2_Paper5_2022.pdf

Nor Azlina Abd Rahman, Chen, L. K., & Yeo, J. Q. (2023). *BATTLE OF HACKERS CTF: A guide to gamified learning - Beginner level*.

Poondej, C., & Lerdpornkulrat, T. (2016). The development of gamified learning activities to increase student engagement in learning. *Australian Educational Computing*, *31(2)*. http://journal.acce.edu.au/index.php/AEC/article/download/110/pdf

Puganesri, K. & Saifullizam Puteh. Computer Science education in Malaysia schools: The challenges of enhancing computational thinking skills. (2019). *International Journal of Engineering and Advanced Technology*, *8*(6S3), 441–444. https://doi.org/10.35940/ijeat.f1080.0986s319

Pusey, P., Tobey, D. H., & Soule, R. (2014). An argument for game balance: Improving student engagement by matching difficulty level with learner readiness. *Genetics Selection Evolution*. https://www.usenix.org/system/files/conference/3gse14/3gse14-pusey.pdf

Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, *10*(5), 378–382. https://doi.org/10.18178/ijiet.2020.10.5.1393

Raman, R., Sunny, S., Pavithran, V., & Achuthan, K. (2014). Framework for evaluating Capture the Flag (CTF) security competitions. *International Conference for Convergence for Technology-2014*, 1-5. https://doi.org/10.1109/i2ct.2014.7092098

SKR. (n.d.-a). *About Us*. Retrieved February 4, 2023, from https://skrctf.me/about

SKR. (n.d.-b). *Challenges*. Retrieved February 4, 2023, from https://skrctf.me/challenges

Seow, P., Looi, C.-K., How, M.-L., & Wadhwa, B. & Wu, L.-K. (2019). Educational policy and implementation of computational thinking and programming: Case study of Singapore. *Computational Thinking Education*, 345-361. https://library.oapen.org/bitstream/handle/20.500.12657/23182/1/1006971.pdf#page=341

Sener, J. (2016). *The role of student competitions in cybersecurity education* [White paper]. National Cyberwatch Center. https://www.nationalcyberwatch.org/wp-content/uploads/2016/05/Student_Competitions_White_Papers_INTERACTIVE.pdf

Švábenský, V., Vykopal, J., & Čeleda, P. (2019). What are cybersecurity education papers about? A systematic literature review of SIGCSE and ITiCSE conferences. *The 51st ACM Technical Symposium on Computer Science Education (SIGCSE '20)*. http://arxiv.org/pdf/1911.11675

Švábenský, V., Čeleda, P., Vykopal, J., & Brišáková, S. (2020). Cybersecurity knowledge and skills taught in capture the flag challenges. *Computers & Security*, 102. https://doi.org/10.1016/j.cose.2020.102154

Thomas, L. J., Balders, M., Countney, Z., Zhong, C., Yao, J., & Xu, C. (2019). Cybersecurity education: From beginners to advanced players in cybersecurity competitions. *2019 IEEE International Conference on Intelligence and Security Informatics (ISI)*, 149-151. https://doi.org/10.1109/ISI.2019.8823310.

Tobey, D. H., Pusey, P., and Burley, D. L. (2014) Engaging learners in cybersecurity careers: Lessons from the launch of the national cyber league. *ACM Inroads*, *5*(1), 53-56. https://dl.acm.org/doi/pdf/10.1145/2568195.2568213

Trickel, E., Disperati, F., Gustafson, E., Kalantari, F., Mabey, M., Tiwari, N., Safaei, Y., Doupe, A. & Vigna, G. (2017). Shell we play a game? CTF-as-a-service for security education. *ASE@ USENIX Security Symposium*. https://www.usenix.org/system/files/conference/ase17/ase17_paper_trickel.pdf.

Tseng, S.-S., Yang, T.-Y., Shih, W.-C., & Shan, B.-Y. (2022). Building a self-evolving iMonsters board game for cyber-security education. *Interactive Learning Environments*, 1–19. https://doi.org/10.1080/10494820.2022.2120015.

USENIX. (2014, October 10). *3GSE '14 – Learning obstacles in the Capture The Flag model* [Video]. YouTube. https://youtu.be/57oyVmMYhwI

Votipka, D., Zhang, E., & Mazurek, M. L. (2021). HackEd: A pedagogical analysis of online vulnerability discovery exercises. *2021 IEEE Symposium on Security and Privacy (SP)*. https://doi.org/10.1109/sp40001.2021.00092

Vykopal, J., & Barták, M. (2016). On the design of security games: From frustrating to engaging learning. *USENIX Security Symposium*. https://www.usenix.org/system/files/conference/ase16/ase16-paper-vykopal.pdf

Vykopal, J., Švábenský, V., & Chang, E.-C. (2020). Benefits and pitfalls of using Capture the Flag games in university courses. *Proceedings of the*

51st ACM Technical Symposium on Computer Science Education. 752-758. https://doi.org/10.1145/3328778.3366893

Weiss, R., Turbak, F., Mache, J., Nilsen, E. L., & Locasto, M. E. (2016). Finding the balance between guidance and independence in cybersecurity exercises. *USENIX Security Symposium*. https://www.usenix.org/system/files/conference/ase16/ase16-paper-weiss.pdf.

Wolfenden, B. (2019). Gamification as a winning cyber security strategy. *Computer Fraud & Security*, *2019*(5), 9–12. https://doi.org/10.1016/s1361-3723(19)30052-1

Workman, M. D., Luévanos, J. A., & Mai, B. (2021). A study of cybersecurity education using a Present-Test-Practice-Assess model. *IEEE Transactions on Education*, *65*(1), 1–6. https://doi.org/10.1109/te.2021.3086025

Zack, K., Ning Z., & Cole, S. V. (2022). A Capture The Flag (CTF) platform and exercises for an intro to computer security class. *Proceedings of the 27th ACM Conference on Innovation and Technology in Computer Science Education Vol. 2 (ITiCSE 2022)*, 597-598. https://doi.org/10.1145/3502717.3532153.