The Privacy Universe - A Game-Based Learning Platform for Data Protection, Privacy and Ethics

Christensen, Michael; Britze, Daniel; Vejlin, Jacob; Sørensen, Lene Tolstrup; Pedersen, Jens Myrup

Published in:
2023 IEEE Global Engineering Education Conference (EDUCON)

DOI (link to publication from Publisher):
10.1109/EDUCON54358.2023.10125160

Publication date:
2023

Document Version
Accepted author manuscript, peer reviewed version

The Privacy Universe – a game-based learning platform for data protection, privacy and ethics

1st Michael Christensen
Aalborg University
Copenhagen, Denmark
mchr@es.aau.dk

2th Daniel Britze
Aalborg University
Copenhagen, Denmark
dbritz@student.aau.dk

3th Jacob Vejlin
Aalborg University
Copenhagen, Denmark
jvje17@student.aau.dk

4rd Lene Tolstrup Sørensen
Aalborg University
Copenhagen, Denmark
ls@es.aau.dk

5nd Jens Myrup Pedersen
Aalborg University
Copenhagen, Denmark
jens@es.aau.dk

***Abstract*—Recruiting and educating cybersecurity professionals continues to be a challenge. It is not hard for people with a preexisting interest to learn more, but in order to fill the gap of missing professionals within the field it is necessary to reach a broader audience and make more people interested in cybersecurity. One element in achieving this, is to show that cybersecurity is not only a technical discipline. Privacy Universe is a platform built within the Haaukins training platform, which a focus on privacy, data protection, ethics and social media usage, targeting less technical students. It enables students to learn about cybersecurity and privacy with hands-on training in a closed and secure environment. This paper presents the platform as well as a survey of 50 students of which 80% who have replied that their learning outcome is 4 or 5 on a scale from 1-5, 5 being the highest. In addition to this, a majority also found that their interest within cybersecurity increased based on their experience with Privacy Universe. This indicates that Privacy Universe is a beneficial addition to the already existing platforms to make cybersecurity interesting for a broader audience, in a field where those competences are much needed.**

***Index Terms*—Cybersecurity, Active Learning, Privacy, Training Platform, Game-based Learning, Education, Learning, Social Media**

I. Introduction

Cyber attacks have been on the rise for the past many years, resulting in increased damages and costs to organisations across the globe [10]. This is seen with a 2021 report from the Federal Bureau of Investigation's Internet Crime Report which analyzes incidents reported to the FBI. The report shows that $6.9 billion were lost by victims due to cyberattacks, noting this number is based on reported incidents with many incidents never being reported to the FBI [11]. These attacks range from small scale attacks disrupting parts of a business, to major attacks such as ransomware disrupting significant parts or entire organisations' business. In order to combat this, additional cybersecurity professionals are required. However, this is difficult due to a shortage in cybersecurity professionals and education of such [9]. Organisations in all sectors and areas of the industry and public sector are searching for professionals that can help securing their systems, however often with limited luck. It is estimated that 2,720,000 job openings currently exist around the world for cybersecurity professionals [12]. While this, according to The International Information System Security Certification Consortium, is down from 3,120,000, it is expected that 3,500,000 job openings will exist in 2025 indicating the demand for cybersecurity professionals will increase [13]. Universities have started to create educations or add cybersecurity into their educations as part of closing this gap, and multiple learning platforms have been created and designed to cater to cybersecurity students who want to educate themselves in the practical aspects of the domain. Alongside, platforms such as Hack the box [4], PicoCTF [5] and Haaukins [6] all offer a practical element to learning cybersecurity. Multiple more platforms similar to those exist, all allowing students to attempt solving different challenges related to cybersecurity.

Many of these platforms, however, address the technical and offensive side of cybersecurity. This includes challenges that require the students to hack their way into a system, decrypt secret information, and reverse engineer computer programs. These challenges are often technical and cater to technical people with some experience or interest in computers and programming. While it is important to educate these students, it is also necessary to attract the less technical students. While this is a significant challenge [1], it is a challenge that must be addressed in order to fill the competence gap.

Game-based learning is teaching students using gaming principles to encourage and engage in the field that they are learning. This has for long been an integral part of cybersecurity training, but many of the game elements have a more technical focus and will therefore motivate the same types of more technical students [2].

This paper presents an educational game-based platform that has a focus on data protection, privacy, and ethical behavior online, referred to as the Privacy Universe. The Privacy Universe is built using an existing security learning platform, Haaukins, which is a capture the flag (CTF) platform [3]. Capture the flag is a game model utilizing flags: Flags are

small pieces of text that can be found by solving challenges, and each flag then translates into points. It is a model well known both in the gaming and cybersecurity communities.

The overall purpose of this paper is to determine if it is possible to use the Privacy Universe to engage students in cybersecurity, even if they have little or no previous experience within cybersecurity and CTF, and to clarify to what extend it will increase their interest in and knowledge about cybersecurity. Using Privacy Universe as a platform for a less technical audience with focus on social media and privacy, a survey will be done on students in the target audience. We hope that the results can be useful when it comes to attracting a wider audience to cybersecurity, and eventually lead to more people choosing a career and education within the field.

The paper is organized as follows. Section II describes game-based learning and why it is used, including some of the commonly used platforms based on game-based learning. Section III describes the Haaukins platform and why Privacy Universe is added here. Section IV elaborates on the design of the Privacy Universe and how it can be used for learning purposes. In section V a survey and feedback from users that have used the platform are presented, based on user tests with surveys to assess its learning potential. Section VI concludes the paper.

II. Active learning

Many platforms, including Hack the box [4], PicoCTF [5] and Haaukins [6] utilize game-based learning. Game-based learning is an active learning technique based on the principle of borrowing elements from gaming for education [14]. This includes simulating real world scenarios training the students in practical ways, allowing students to engage in learning using elements that will be playful and dynamic. Compared to passive learning with students following along in a class, listening to a teacher, this engages students actively in solving practical challenges. Solving problems which could occur in the real world is motivating for the students, and prepares them for work and further development of their skills and knowledge within the cybersecurity domain. Cybersecurity both have theoretical and practical parts, and similar to many other computer science and math domains, facilitating learning of the practical parts can be difficult. The cybersecurity domain also includes both offensive (i.e. attacking) and defensive (i.e. defending) elements, where the former requires the student to gain experience with attacking systems - often with the perspective of training the students to ”think like a hacker”. This can be challenging due to legal concerns, thus having closed and secure training platforms which allows for this are crucial. Similarly, defending requires a student to hand systems being attacked, which also have to happen in a secure and known environment to prevent harm to any other systems. The elements of game-based learning can include, but are not limited to, gaining points for solving challenges, and presenting these in a competition way such as public scoreboards [14].

All three platforms mentioned offer points and a scoreboards in which the users can see and compete with other users in terms of who is ranking highest, adding a competitive element to the platforms. By competing, the users are also learning new traits within cybersecurity which can be used later. The platforms also offer a jeopardy style setup which divides challenges into categories and give varied points based on difficulty, just as with jeopardy.

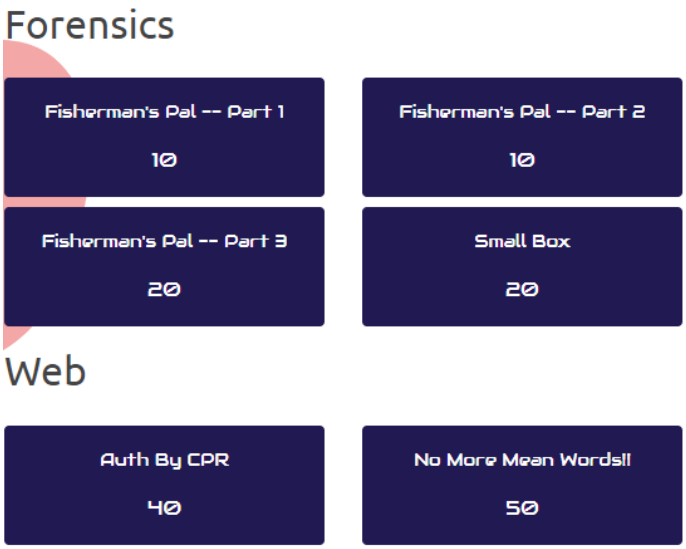

Fig. 1. Haaukins challenge site

Figure 1 shows an example of the Haaukins platform in which it is possible to see how the jeopardy style setup looks. Each challenge has a number showing the amount of points the user receives for solving it, while also indicating the difficulty of each challenge: A low number of points indicates an easy challenge, whereas a higher number of points indicates a harder challenge.

Game-based learning has proven to be effective for learning due to its introduction of practical elements in what are often theoretical fields, along with the competitive elements.

III. The Haaukins platform

The Haaukins platform is an open source project developed at Aalborg University [16] in collaboration with a number of other Danish universities. The platform is based on giving students access to a virtualized environment with no internet connection, thus isolated from the surroundings. This enables students to use any commands, software and techniques within hacking, without risking to cause harm to any real systems. Within this environment, Haaukins provides virtual machines that users can use, in particular each user gets access to a computer with the Kali Linux operative system, which contains many cybersecurity tools. This machine is connected to a number of docker containers where each contains a system with one or more vulnerabilities that can be exploited by the user. The term vulnerability should be understood in a broad sense here, it can also be e.g. a website where the students

simply have to find information hidden on the website, or a puzzle that the students need to solve. A user can connect to the platform through their browser, limiting the technical requirements from the user, and making it accessible for all.

Haaukins allows for *events* to be set up for different use cases. An event is a series of challenges meant for a specific group of users, usually provided for a limited timeframe - this could be for a class, or for an extra-curricular event such as "hacking afternoon". An event can be reached at a specific web address from which the students can access the challenges set up for the specific event, along with an event-speficic scoreboard. This allows a teacher to set up an event for his or her class and not share it with anyone else, thus controlling which challenges should be included and also control the learning outcome for a specific class. All events are separate from another and each user is isolated in their own virtual environment, thus, no one can see each other in the environment. Connecting through the browser is set up to be simple and gives a user interface to a virtual machine using the Kali Linux operating system as shown in figure 2.

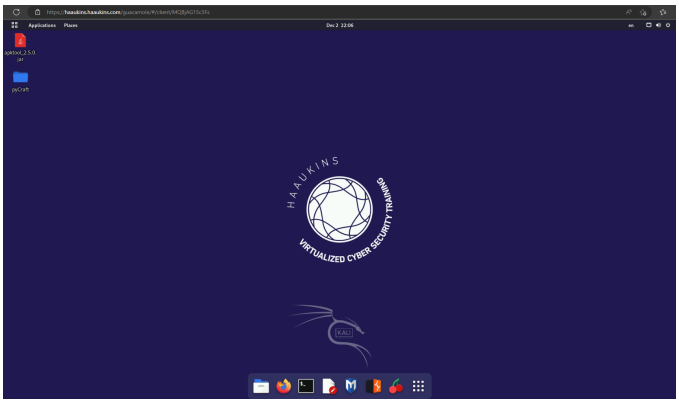

Fig. 2. Kali Linux Virtual Machine on Haaukins

A connection through the browser requires the student to create a user account and then connect to a Kali Linux virtual machine hosted by Haaukins.

Having only two steps from entering the website to being shown a virtualized environment makes it simple for new users to be introduced to the platform.

All challenges are split into categories indicating what the main purpose of the challenge is. If it is *Web Exploitation* the user will have to attack a website, *Cryptography* would be to figure out how to decrypt something, and so on. Selecting a challenge will show a short description introducing the user to the task. It will help the user to get started, and provides the user with all the knowledge required to solve the challenge. It can also include hints on what skills are needed, or pointers to useful resources.

This setup, including both the interface to the users and the closed and secure virtual labs, makes Haaukins a good choice for implementing the Privacy Universe. At the same time, it allows for creating events that include both more technical challenges and challenges based on the Privacy Universe. Also, since Haaukins is open source and since the development team behind Privacy Universe already have been developing challenges for Haaukins, it is chosen as the platform behind the Privacy Universe.

IV. Privacy Universe

Privacy Universe is a subset of Haaukins challenges that promote education on subjects with regards to data protection, privacy, social engineering and information gathering. The project was started in September 2021 and is created as part of the CyberSkills project funded by The Danish Industry Foundation [17], which is a project to increase the interest and competencies with respect to cybersecurity amongst the youth in Denmark.

The main idea behind Privacy Universe is to create a universe in which students can train in security and privacy related topics. Using social media to give a relatable environment for the students, they are taught about usage of these platforms as well as understanding the importance of cybersecurity in their own online lives. Having such social media platforms, based on fictional data and fictional users, allows users to have a safe experience on the platform and still learn about the risks online. Using the data found on the platforms, they will for example be able to log in to the fake users accounts or find private information about them.

In this section we'll cover a technological overview of how we build these educational services, a presentation of the design of the platforms and philosophies behind it, and a discussion about data generation.

A. Technology overview

The Privacy Universe consists of four systems with integrated educational challenges, with the ability to expand the universe later. Each of the services correspond to a simulation of a distinctive social media platform, as seen in table I. They are build to provide a rather deep simulation of the platforms, rather than just being nice looking mock-ups, since this makes it possible to provide a large set of realistic challenges.

Platform	Privacy Universe
Facebook	FriendSpace
Instagram	PhotoSpace
LinkedIn	JobSpace
TikTok	Peacock

TABLE I
Overview of the different spaces in the Privacy Universe

The simulated platforms are build as modern web applications utilizing four primary technologies: **React.js**, **Express.js**, **MongoDB** and **Docker**.

a) React.js: is a modern framework for building Progressive Web Applications. Originally developed by engineers at Facebook (now Meta), it has become one of the major JavaScript frontend frameworks. React's component based structure with natural inheritance between objects makes it a reliable and maintainable choice for a dynamically evolving software project like Privacy Universe.

b) Express.js: is used to build a saleable and reliable HTTP REST API to handle all interconnections between the frontend system and backend resources. Express.js is a popular JavaScript framework for constructing simplistic REST APIs and is used in Privacy Universe exactly for this simplicity and to restrict code base to only JavaScript. In the systems it is responsible for handling incoming requests, fetching data, authentication and much more.

c) MongoDB: is a modern NoSQL database system that provides functionality to store document based data structures. It is integrated with the REST API as a middleware module and facilitates smooth and quick data fetching. All the Privacy Universe systems are in need of both raw data storage (text, numbers, dates etc.) as well as file storage (.png, .pdf, .txt etc.) and the MongoDB document based structure allows us to centralize this in a single database.

d) Docker: binds the whole system together by defining the deployment configuration for each sub-service and the interfaces between them in one central Dockerfile. This is crucial for the systems integration with the Haaukins virtual lab where challenges must be deployed through a single Dockerfile.

Conclusively, these technologies and their integration constitute a modern web architecture fit for local deployment in the virtual lab.

B. Design

To engage the users, both the look and the feel of the websites must be similar to the social media platforms in the real world. Achieving this goal requires that the websites in Privacy Universe both resemble and feel like real social media platforms, which creates a sense of familiarity, heightening engagement. Firstly, making a website within Privacy Universe resemble its respective counterpart is done by taking inspiration of real websites through noting the different modules in a website. Each module is then examined within both its design and functionality. Creating this sense of familiarity through the design is done by taking the modules and making novel, but similar designs to be used within Privacy Universe as seen in figure 3 and 4.

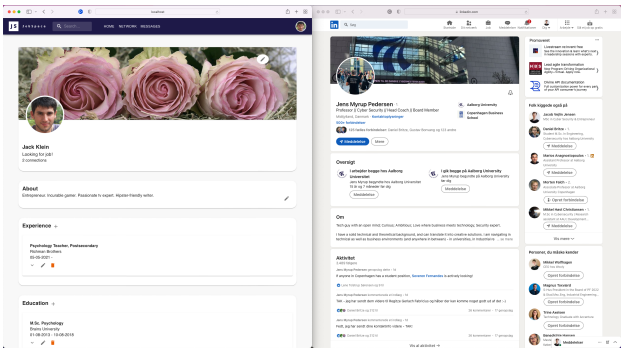

Fig. 3. Profile tab in JobSpace vs LinkedIn

With the visuals of the Privacy Universe websites similar to their real counterparts, the next step is to create a similar feeling when navigating the websites. This is achieved by taking the functionality of the different modules into consideration. If clicking on your profile picture on LinkedIn takes you to your profile, then JobSpace should do the same. Through this analogous functionality, the Privacy Universe websites behave in a way users know and expect. Notably, this recreation also includes smaller elements such as creating an on hover effect, so that if the user hovers their mouse over a clickable element it becomes clear and makes the website feel truly dynamic.

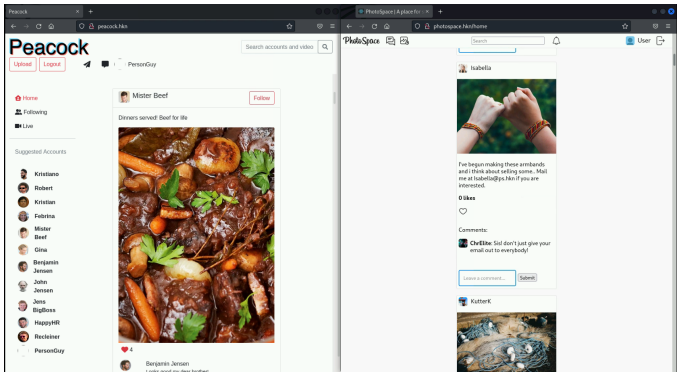

Fig. 4. Main page in Photospace and Peacock

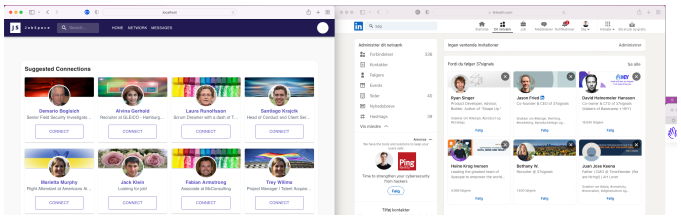

Fig. 5. Functional network tab in JobSpace vs LinkedIn

Finally, the Privacy Universe websites must include believable data, such as users and posts. Creating users requires licenses for the photos, ensuring it can stay on the platform with proper consent. Currently two methods are used: Stock photos and AI generated images [8], the latter of which enables the use of completely non-personal images. The AI generated images are currently limited by only creating one image of a person, where real life counterparts tend to have more than one image of themselves, however due to AI images being a rapidly developing field, this limitation might soon be gone. Generating the posts for the users requires different objects such as: Text, Images, Video, Audio. Depending on whether the user being created are used in a challenge or if it is used to create a larger user base, it may include many items, e.g. text, images etc. or may just be a profile, sometimes with a post or two. This is done to prevent a massive overhead in information as this may not be actively used on the platform anyway. Whilst inspiration is taken from real posts, the text is novel and modified to fit within the different Privacy Universe platforms, creating an internal consistency by for example having a certain amount of employees make posts about the company which the profile works for. Similarly to the profiles

created on Privacy Universe, the images, audio and video are either stock media or AI generated.

C. The Challenges

Each challenge is introduced by a description, as all other Haaukins challenges III. Based on this description the student will have the knowledge required to start the challenge, including which social media to start with, who or what to look for, and so on. When entering the website designated by the challenge description, the student will have to create a user account on that social media. The user can enter any data, and it will not be stored beyond the lifetime of the event. When a user account has been created, the student will find a number of challenges, created by the developers to teach the student about different topics within cybersecurity and privacy. To make the universe alive, there are also a number of pre-created user accounts on the platform, some of which are actively used for the challenges. While in principle the challenges are available for all Haaukins users to use, the source code is not publicly available. The reason for this is that anyone with access to the source code of the challenges will also have the solution, ruining the challenges for students.

Due to the flexibility of the Privacy Universe, it is possible to create a large array of different challenges. An example is a challenge called ”Fisherman’s Pal”. This is a challenge series, meaning that it is three challenges which have to be completed in a certain order for it to make the most sense for the students.

Fisherman’s Pal is created for Photospace and the first challenge in the series has the following description:

We have a suspicion that the notorious hackergroup Fisherman’s Pal has begun to operate again. We have the idea that they might use photospace as a platform to communicate. We need you to find the real name of the hacker they call Elite together with the names of his mother and sister. Good luck.
Flag form: HKN{Name_MothersName_SistersName}
Go to (http://photospace.hkn).

After entering photospace and creating an account, the student sees multiple users. Here it is possible to find a user called Christian as well as his sister. Christian’s profile is set as ”Private”, but the sister’s profile is open, and here we find the mothers name in one of the posts. Having the name, the mothers name and the sisters name, it is possible to create the flag and enter it on Haaukins for points.

Other challenges includes, but are not limited to:

- Find information in images posted to the social media
- Identify hidden information in links
- Find data in cookies
- Find credentials leaked to login to other users account

The list of challenges continue to increase and the goal are to expand beyond social media. This can include finding information on social media, which may give the student access to their business accounts. A challenge like this will teach the student that information posted to social media may be used in the business life too. Small elements like this shows the truth about cybersecurity and how easy it is to compromise an organisation if the employees are not careful. But future challenges can also emphasize the importance of being secure privately, to protect financial information, family and more to avoid information leakage or abuse.

V. Evaluation of the platform

While Privacy Universe is under continuous development of new platforms and challenges, it have been tested by multiple students. This is done through events with students to determine their learning outcome as well as the user experience. While learning is important, user experience is also crucial as this is required for the students to use it for learning purposes. We have created a survey to determine if Privacy Universe supports learning for a less technical group of students, as an addition to some of the platforms mentioned in II. This allows us to determine the potential of using the Privacy Universe, and provides us with inputs for improvement. It is important to note that this is a survey to set a baseline to determine the usefulness of Privacy Universe, however, additional testing and both qualitative and quantitative research could be performed to understand more about the contribution the privacy universe can provide.

A. The Questions

The survey included nine questions, of which six were related to Privacy Universe and the three others were to determine the respondents gender and experience within Capture The Flag events. The nine questions were:

1) How many CTF events have you participated in?
2) What is your gender?
3) What is your experience with CTF events?
4) How was your experience with Privacy Universe?
5) How intuitive did you find Privacy Universe?
6) On a scale from 1-5, how much do you feel you have learned from Privacy Universe?
7) Considering that you have tried Privacy Universe, how likely are you to recommend it to your friends and colleagues?
8) Did Privacy Universe affect your interest in cybersecurity?
9) If Privacy Universe had an effect in your interest within cybersecurity, what effect did it have?

Having reference questions to determine if the audience are experienced with CTFs shows whether it is the correct audience group, namely less technical people with little to no CTF experience. The remainder of the questions are partly to determine if Privacy Universe is usable by the target audience, as well as to determine if it sparks an interest in cybersecurity as this is one of the goals.

Question two and nine were free text, meaning the respondent had to write the answer themselves. The remaining questions were setup as a multiple choice style questionnaire. Question one had 0, 1, 2, 3 and ”4 or more” as options while question 3, 4, 5 and 7 had options such that the respondent

could not answer neutrally meaning that for example question 4 had the options ”Very good”, ”Good”, ”Bad”, ”Very bad”. Studies show that offering a neutral option will lead many respondents to just pick that [15]. On the other hand, not offering this option will force respondents to make a decision, either positively or negatively. Both methods have benefits and drawbacks, however, for this an equal number of possibilities have been chosen.

It is important to note that this survey was conducted on Danish students in the age group of 15-16 years old. While it can be expected that this age group understands English, all questions were translated to Danish to avoid any language barriers. The Danish translations can be found in the Appendix for reference.

B. The Survey Methodology

The survey was conducted with a researcher present with the participants. An event was set up with approximately 50 students present. It started with a presentation by the researcher about privacy and online surveillance to introduce the topic to the students, and to give some prior knowledge as to what to look for. This presentation was followed by a short introduction to Haaukins, how to register, how it works, as well as how to access the virtual machine and Privacy Universe. A challenge description was shown to lead the students to read the description prior to attempting solving challenges.

This was followed by approximately 50 minutes where students could attempt any challenge currently available within the Privacy Universe. A researcher was present at all times to help students who got stuck due to technical reasons, but did not aid with challenges. After the 50 minute session with Privacy Universe, a fast wrap-up of the learnings and challenges was done. Alongside the wrap-up, the survey with the nine questions was handed out for the students to answer.

C. The Results

In addition to helping, the present researcher also observed the students, how they acted and what they said while solving the challenges. These are some of the notes from the researcher:
The students were engaged with the challenges and sat in groups to solve the challenges. Most students started immediately, while others had a few technical problems which were resolved. While walking amongst the students, it was clear that most found it interesting, however, while they did get started, it was not clear if they understood the security issues and purposes of the challenges.

While this is based on the researchers observations, the survey showed positive response too. The event had approximately 50 student, only 43 answered the survey. The reason for this is unknown, other than some simply chose not to answer the survey for personal reasons. With a majority of respondents answering either 0 or 1 to the number of CTF and beginner experience with CTF, and with 1 person for 2 CTF’s and 1 with 3 CTF’s, the anticipated target audience can be determined. Similarly the gender distribution were divided equally amongst men and women.

A majority of respondent had a positive experience with Privacy Universe with 21 responding Very Good and 18 responding Good. In regards to how intuitive the respondents found Privacy Universe, it was quite positive, however the majority answered ”Good” rather than ”Very Good” as shown in figure 6.

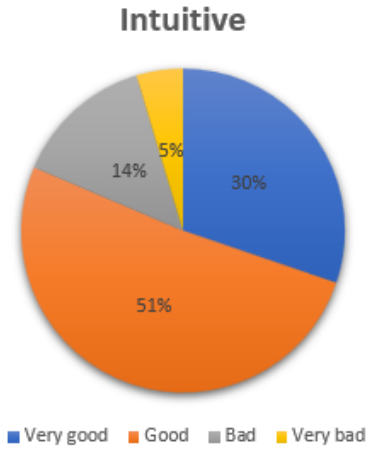

Fig. 6. Results from survey on how intuitive Privacy Universe are

It is important to consider those that did not find it intuitive or did not have a good experience in their first encounter with Privacy Universe. While some may be due to technical issues occurring with the test platform during the day, others seem to be minor error messages that can be ignored - but the students would have to know this and remember after being told.

In terms of whether the students learned anything and would recommend the platform, the results varied more. Figure 7 shows the distribution of how the students determined their learning outcome. 1 being the least learned and 5 the most, it is clear that the majority was in the top half - 80% answered 3 or above. This indicates that Privacy Universe can give a desired learning outcome for the students, but there are still room for improvements.

Finally a majority of the respondents answered that their interest within cybersecurity has increased and that they would recommend the use of the platform to others. This indicates that while some students did encounter technical issues, a majority still had a positive experience and had their interest in cybersecurity grew, which are some of the goals for the platform.

D. Considerations

While the survey were conducted and showed positive results for Privacy Universe, the choice of not using the Likert scale, thus not having a neutral option could have an impact. While it has the benefit of not having the neutral answer, which can be hard to use as it does not tell whether it is positive or negative, it may increase the acquiescence bias, leading

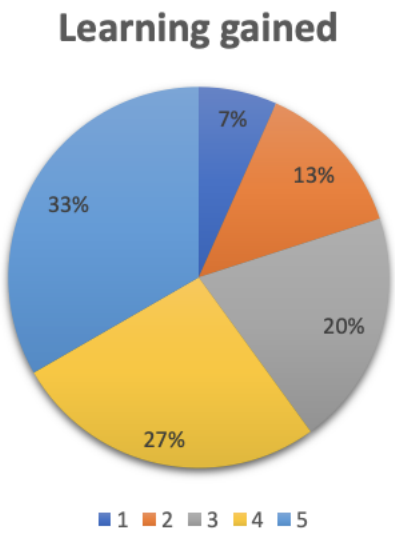

Fig. 7. Percentage of what students learned 1 being low and 5 being high.

to more positive results. A neutral option could be added to serve those who may not have a preference, however it was chosen to leave it out to avoid having answers that were less meaningful.

A common issue with questionnaires is that some respondents may just answer rapidly to continue their day, and this will also be reflected in the results. This may also be the case in this survey as it was conducted on students at the end of their study day. While it may not have an impact as they were given time to fill in the survey, it may be a factor to rapid responses from the students to get home.

VI. Conclusion

This paper presents Privacy Universe, a cybersecurity and privacy platform within the Haaukins training platform. The goal is to determine if this platform can engage with students with little or none technical experience within cybersecurity, and if this creates an interest for the field - thus contributing to attracting a wider set of students to work and study within cybersecurity. The platform introduces websites that imitate social media to create a familiar environment for the students. Creating these social media sites in the Haaukins virtual environment allows the students to work safely without any worries regarding destroying or harming anything. A survey was conducted on a group of 50 students who had used Privacy Universe. The results show that 80% of the surveyed students had a positive learning experience, and the other results were promising in terms of the usability experience by the students. Being a universe that is focused on less technical students, it have proven interesting for the students to use. This is important to engage more people in studying and working with cybersecurity. The results of the survey were positive in this regards and also showed that the target group would recommend the platform to others, which is also a step in expanding the cybersecurity community. The survey and observations also pointed to potential improvements of the platform, which will be done as future work.

VII. Appendix

- Hvor mange CTF events har du været deltager i?
- Hvad er dit køn?
- Hvad er dit erfaringsniveau med CTF events?
- Hvordan var din oplevelse med Privacy Universet?
- Hvor intuitivt var Privacy Universet
- På en skala fra 1-5 Hvor meget vurderer du, at du har lært fra Privacy Universet? Hvori 1 er intet og 5 er meget.
- Efter at have prøvet Privacy Universe, hvor sandsynligt ville du foreslå andre at prøve det?
- Har Privacy Uniververse haft en effekt på din interrese inden for Cybersikkerhed?
- Hvis Prviacy Universe har haft en effekt på din interesse inden for cybersikkerhed, hvordan har det haft en effekt?

References

[1] Crick, T., Davenport, J.H., Hanna, P. Irons, A. and Prickett, T. (2020): Overcoming the Challenges of Teaching Cybersecurity in UK Computer Science Degree Programmes. IEEE Frontiers in Education (FIE). DOI: 10.1109/FIE44824.2020.9274033

[2] Hendrix, M. Al-Sherbaz, A. and Bloom, V. (2016): Game Based Security Training: are Serious Games Suitable for cyber security training? International Journal of Serious Games, Vol. 3, no. 1, pp. 53-61.

[3] Panum, T.K, Hageman, T., Pedersen, J.M and Hansen, R.R (2019): Haaukins: A highly Accessible and Automated Virtualization Platform for Security Education, IEEE Xplorer, IEEE 19th International conference on Advanced Learning Technologies (ICALT). DOI: 10.1109/ICALT.2019.00073

[4] Hack The Box (2022). A Massive Hacking Playground. [Online]. Available. https://www.hackthebox.com/

[5] Pico CTF (2022). Pico CTF. [Online]. Available. https://picoctf.org/

[6] Haaukins (2022). Haaukins. [Online]. Available. https://github.com/aau-network-security/haaukins

[7] Khan, M.A., Merabet, A., Alkaabi, S. and E-Sayed, H. (2022): Game-based learning platform to enhance cybersecurity eduation. Educational and Information Technologies (2022), 27:5153-5177, DOI: 10.1007/s10639-021-10807-6

[8] This Person Does Not Exist (2022). This Person Does Not Exist - Random Face Generator [Online]. Available. https://this-person-does-not-exist.com/en

[9] Forbes. The cybersecurity industry is short 3.4 million workers—that's good news for cyber wages. [Online]. Available. https://fortune.com/education/business/articles/2022/10/20/the-cybersecurity-industry-is-short-3-4-million-workers-thats-good-news-for-cyber-wages/

[10] IBM. Cost of a data breach 2022. [Online]. Available. https://www.ibm.com/reports/data-breach

[11] Federal Bureau of Investigation. Internet Crime Report 2021. [Online]. Available. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

[12] ISC2. A Resilient Cybersecurity Profession Charts the Path Forward. [Online]. Available. https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

[13] Cybercrime Magazine. Cybersecurity Jobs Report: 3.5 Million Openings In 2025. [Online]. Available. https://cybersecurityventures.com/jobs/

[14] A. Pho & A. Dinscore, "Game-Based Learning", American Library Association, [Online document], 2015. Available: https://acrl.ala.org/IS/wp-content/uploads/2014/05/spring2015.pdf

[15] Kalton, G., Julie Roberts, and D. Holt. "The Effects of Offering a Middle Response Option with Opinion Questions." Journal of the Royal Statistical Society. Series D (The Statistician) 29, no. 1 (1980): 65–78. https://doi.org/10.2307/2987495.

[16] T. K. Panum, K. Hageman, J. M. Pedersen, & R. R. Hansen, ”Haaukins: A Highly Accessible and Automated Virtualization Platform for Security Education”, 2019 IEEE, [Online document], 2015. Available: https://ieeexplore.ieee.org/document/8820918, doi: 10.1109/ICALT.2019.00073
[17] CyberSkills. Join the CyberSkills COMMUNITY. [Online]. Available. https://www.cyberskills.dk/
[18] Wikipedia. Acquiescence bias. [Online]. Available. https://en.wikipedia.org/wiki/Acquiescence_bias