VPET: A Novel Visual Privacy Themed Cybersecurity Educational Game

Dr. Ankur Chattopadhyay
School of Computing & Analytics
Northern Kentucky University
Highland Heights, Kentucky
chattopada1@nku.edu

Saumya Sharma
School of Computing & Analytics
Northern Kentucky University
Highland Heights, Kentucky
sharmas2@nku.edu

Elisee Mbaya
Department of Computer Science - Alumni
University of Wisconsin Green Bay
Green Bay, Wisconsin
eliseembaya1@gmail.com

James Rice
School of Computing & Analytics
Northern Kentucky University
Highland Heights, Kentucky
ricej33@nku.edu

Abstract - **This full paper in the innovative practice category introduces a uniquely novel visual privacy themed game, which is meant to be used as an experiential learning tool for teaching plus demonstration of fundamental data privacy concepts and basic security concepts. To our knowledge, this new, innovative visual privacy themed game, as presented in this paper, is the first of its kind gamified educational tool, which makes use of the privacy through visual anonymity i.e. VPET (Visual Privacy Enhancing Technology) theme for effective illustration of privacy concepts along with basic security concepts. This paper describes our nifty, visually interactive VPET game, which teaches privacy plus security concepts through the PET illustration and demonstrates applied cryptography for privacy-driven de-identification through obscuration-based disguise tasks during the game play. It also discusses how we have successfully used a pilot, proof of concept prototype version of this game over the last few years for cybersecurity education and outreach primarily at the K-12 level. Over the last few years, we have surveyed several VPET game players, who are from a large, diverse group of K-12 community members, consisting mainly of high school students and teachers, who have played the VPET game, as part of several cybersecurity training camps and outreach workshop sessions, and have benefited from this exercise in terms of learning, as well as developing awareness plus interest in privacy and security topics. This paper shares and analyze the preliminary data collected from all these survey responses to evaluate the prospects of our unique VPET game as a potential educational and outreach tool for engaging K-12 learners, for teaching privacy plus security concepts, and for creating awareness plus interest in cybersecurity. In summary, we demonstrate how our unique VPET gamification approach for educational purposes can successfully engage students for effective learning of data privacy and cybersecurity concepts.**

Keywords - Visual Privacy, Privacy Enhancing Technology, Educational Game, Privacy Awareness, Cybersecurity Concepts, Privacy via Visual Anonymity, Learning

I. INTRODUCTION

Recent literature indicates that privacy education has not advanced as much as security education, even though both security and privacy education are essential for awareness and well-being of today's societal members, including the youth, who are tech users [18]. The latest K-12 curriculum standards advocate for inclusion of privacy, safety, ethics, and societal plus human security topics in the school lessons [4, 6]. Existing literature shows previous studies on data privacy educational research that includes several instances of work at the K-12 level. However, only a handful of these prior studies have utilized the visual privacy topic or the visual PET theme for privacy education [3, 4, 5, 20]. None of the existing few instances of visual privacy educational research have explored a gamified learning approach. This paper addresses this gap by presenting a first of its kind, novel visual privacy game.

Different types of personally identifiable information (PII) get exposed and compromised in modern society, which is vulnerable to various privacy threats. This includes visual data cues as well, such as photos and videos that are very commonly shared across the internet and social media. These visual data components involve biometric data, such as the human face. As the volume of visual data (including sensitive information) expands, external threats to the data grow as well, requiring users to be cautious about unwanted incursions. Hence, the topic of visual data protection leads us to the case for visual privacy and VPET s [2, 14].

Prior research literature indicates that the concept and theme of visual privacy is unique within the data privacy

space, especially around educational premises, including cyber education plus outreach at the high school level [3, 4, 5, 20]. The rising concern about data privacy and cybersecurity issues has motivated many educators to conduct educated research related to privacy and cybersecurity. As a result, many educational innovations have emerged and creative curricular initiatives have been developed on several security topics. However, privacy education related work has not advanced or progressed as much as security education related work or initiatives, as per a recent survey study [18]. On top of that, most of the existing K-12 educational resources or curriculum on data privacy primarily and pre-dominantly deal with privacy in textual data contents [13, 15, 16, 17]. In other words, very few of the previous data privacy educational research studies involve visual data privacy or utilize VPET s for that matter. In an effort to fill this hole in data privacy educational work, we have developed a uniquely new visual privacy themed cybersecurity educational game, VPET.

VPET is meant for innovating data privacy education using novel gamified learning components. It introduces data privacy plus cybersecurity concepts using the privacy through visual anonymity (PVA) theme. This multiplayer game involves one player (the disguise agent), who chooses to protect the visual privacy of a chosen individual by applying de-identification based privacy filter tools, while the other player i.e. the opponent (the bounty hunter) tries to beat the first player by defeating the privacy filter through identification of the de-identified individual. This research paper is based on how VPET is relevant to privacy and security education. Our nifty gamified educational approach, as exhibited through VPET, is intended to innovate privacy and security education, and our experimental study, as discussed later in this paper, shows the potential efficacy and impact of VPET for engaging leaners and advancing data privacy education.

II. Background

Privacy concerns are growing rapidly in the present digital world, and this poses challenges for the youth, including K-12 students, who depend on technology for their education, communication, and socialization [3, 4, 5, 7]. Visual privacy is focused on the goal to control what others can see for safeguarding private and sensitive visual cues. It is particularly important and relevant for today's youth, which includes high schoolers, so that they can make informed decisions about protecting personal data. This specifically applies to today's high school community, where the students are exposed daily to social media and the internet. A lack of clear understanding of private and public

TABLE I. Comparison Of Our VPET Gamified Learning Approach With Other Relevant Data Privacy Educational Research Studies

Research Study	Targeted Audience	Work Summary/Highlights	Functionalities/Mode of delivery	Goal/Focus
[14] (2017)	Social Media Users	Propose a novel model for predicting privacy attributes capable of detecting privacy-sensitive image elements. Address the problem of identifying and predicting privacy risks in images by considering personal information and user preferences.	• Predict up to 68 privacy attributes from images • Estimate the user's privacy score • Prevents leakage of private information • Available on mobile devices and web services	Visual Privacy Awareness on social images for social media
[15] (2022)	High School Level (implied)	Investigated how privacy policies apply to serious puzzle game scenarios. It explores the retention of information through puzzles in a mobile game vs a text-based game	• Available on mobile devices • Offers an escape room game concept • Various puzzles to interact with and attention to detail required	Awareness of data collection, data processing, and data transfer on top of visual privacy
[16] (2019)	Smart Watch Users	Explores the efficacy of games in encouraging protective smartwatch behavior and that it appears to promote protective behavior	• Available on smartwatches • Online simulation approach • Reduces the prevalence of the privacy paradox	Data privacy awareness
[12] (2019)	High School Students (implied)	Focuses on the data privacy in serious games and the privacy concerns of smart cities through the use of quizzes and real-life examples and the risks of digital services	• delivery through quizzes • Interactive UI with avatar modification • Promotes competitiveness through a leaderboard in the game	Data privacy awareness among teenagers, smart cities risks
[11] (2016)	Middle School Students (implied)	Promotes digital literacy through a game that aims to teach children how to make positive privacy and security-related choices online and offline	• Delivery through a web app on the internet • Simple narrative to ease the follow-through of users • Constant feedback on every scenario	Privacy & Data Collection awareness among children
[17] (2021)	High School Students	Teaches teenagers how to protect their personal information online and avoid online risks.	• Collaboration experience through partner matching mechanism	Privacy education, Social & emotional risks online

			• Delivery through a web app on the internet with various quizzes and games	
Our current work (VPET Game)	High School Students and Teachers	Hands-on experiential learning-based lesson activity that is conducted through a desktop app with various privacy exploitive features and security features, allowing users to experience both sides	• Delivery through desktop app • Concept based on an adversarial scenario • Explores the basics of cryptography	Visual privacy awareness, Cryptography

spaces can potentially make high school students relatively easy targets as naive users of social media, leading to a loss of privacy and a compromise of confidentiality [3, 4, 5, 20].

Existing literature on visual privacy education shows the use of educational utility tools, like YouTube Face Blur and the Obscura Cam mobile app, for delivering privacy education to high school and middle school students [3, 5]. According to a prior paper [5], the number of students interested in visual privacy increased by about 25%, that is, from 60% to 85%, after they were introduced to YouTube face blur and Obscura Cam apps. Similarly, another previous paper [4] describes an educational research study that makes a case for successfully engaging high school students through the use of a visual privacy tool. In this paper, we unveil the VPET game as an educational medium for high school students and teachers. We show how the VPET game play based learnings works, and then we discuss the results obtained from multiple VPET driven educational workshops we hosted for different high school audiences, who get first-hand opportunity to play the game and learn. At the end of these workshops, the participants were asked to take a survey and provide feedback plus inputs. This paper uses these survey data to analyze the impact of VPET on learning and engagement at high school level. Table I shows the differences between our VPET game-based learning approach and case study with other relevant data privacy educational approaches and studies. In addition, Table II compares our gamified VPET educational tool with other existing non-gamified VPET tools/utilities.

TABLE II. EXISTING NON-GAMIFIED VPET TOOLS VERSUS OUR VPET GAME-BASED EDUCATIONAL TOOL

Application	Targeted Audience	Features	Goal/Focus
Obscura Cam [5]	Accessible to the public	An Android application featuring automatic face detection and the addition of filters on the face Sharing of pictures/videos while protecting the privacy of you	The main goal of this application is to be able to share your photos and videos while protecting your privacy.
YouTube Face Blur [5]	Accessible to the public/ YouTube users	Is a YouTube feature and blurs parts of a video in YouTube Studio for privacy purposes	YouTube Face Blur is a feature added by YouTube to protect the visual privacy of its user by adding a face blur filter on their faces.
Our VPET Game	High-school community and undergraduate /college students	Has a game component to it Interactive multiplayer game Can add filters on the face to protect the privacy of individuals in photos	It was developed for an educational purpose. The main goal of this game is to reinforce the concept of visual privacy among users and help them learn more about it.

In the area of privacy and security educational research, serious games have emerged as a promising tool to raise awareness and promote responsible behavior. Friend Inspector [1], PrivaCity [12], and "A Day in the Life of the Jos [11] have gained attention in this regard for their innovative approaches to teach privacy and cybersecurity concepts through engaging and interactive scripts. However, it is noteworthy that none of these educational games utilize the visual privacy/PVA theme, unlike our VPET game. Table III illustrates the distinction of VPET from other existing privacy educational games.

TABLE III. COMPARING EXISTING PRIVACY & SECURITY EDUCATIONAL GAMES TO OUR VPET GAME

Game	Objectives	Strengths	Limitations
Friend Inspector [1]	• Enhance privacy awareness on social media • Reduce the gap between Actual and Perceived visibility	• Structured around a series of levels, each presenting a privacy-related scenario • Provides feedback on player actions and decisions	• Limited to contacts and shared items on Facebook • Exclusively accessible through the website, with no mobile version.
PrivaCity [12]	• Make the user understand that privacy is a trade-off and can be very subjective • Raise awareness of privacy risks	• Multiple rooms with different challenges • Chatbot interactions and adventure-based game.	• Absence of visual content in the game may lack engagement for younger teenagers
A Day in the Life of the Jos [11]	• Raise privacy awareness among middle school students	• Effective in teaching privacy concepts and consequences of actions in daily life	• Limited only a small age group (11 to 12 years age groups)

	• Presents educational content interactively and engagingly.	• 25 interactive scenarios, providing a comprehensive learning experience	
Our VPET Game	• Increase awareness of visual privacy • Enhance knowledge of cyber security concepts	• Features a multiplayer experience • Offers a user-friendly and interactive user interface	• Limited to only one scenario • Insufficient feedback provided

III. Related Works

There has been growing interest in developing serious games for privacy and security education in recent years. 'Friend Inspector' [1] is such a serious game developed to enhance privacy awareness in social networks. The game aims to help users learn about privacy risks associated with social media use by simulating a social media platform and providing feedback on the privacy implications of user actions. Similarly, 'A Day in the Life of the Jos' [11] is an educational game on privacy aimed at helping users understand how their personal data is collected, used, and shared by different actors in the digital world. This game uses storytelling to engage users in a privacy narrative and incorporates mini-games to reinforce critical concepts. However, as explained earlier, none of these privacy educational games use the PVA theme, as VPET does.

The original concept of VPET does not stem from the privacy education area, and it originates from privacy enhancing computer vision, that makes use of visual anonymity techniques to protect user privacy from privacy invading visual surveillance. The Privacy Cam model [2] is an example of this privacy enhancing computer vision work, and it represents a privacy-preserving camera that blurs faces in real-time. Another prior work [8] includes a visual exploration of cybersecurity concepts using visualization techniques to help users understand complex cybersecurity concepts. The first instance of applying the visual privacy theme for educational purposes is the PVA lab work [3] for enhancing cyber education and outreach through visual anonymity techniques. These previous works have provided valuable insights for the design of our VPET game as an educational tool. VPET builds on these approaches by providing a unique, immersive gamified experiential learning that combines gamification with privacy enhancing de-identification techniques to engage the game players in a combined privacy and security education narrative.

IV. Project Goals

We look to address the following primary research questions:

- *How to design and develop a PVA themed game that makes innovative use of VPET for privacy and security education plus outreach?*
- *How to determine and assess the potential of this VPET game for effectively engaging learners and for creating interest plus awareness in privacy and security topics?*

To address the first question, we describe our approach to design and build the VPET game for creating an engaging learning platform for educating youth in data privacy and security education. The multiplayer component of the game helps the game to encourage competitive spirit among learners, thereby making it more inclusive The objective of this game is to introduce what visual privacy is and why it is so important. To answer the second question, we evaluate the effectiveness of our work by analyzing the survey data we obtained from piloting this game with multiple different groups of high school students and teachers. For this purpose, we analyze the survey responses collected the VPET learning session participants. Additionally, we review existing literature on visual privacy, and look at existing educational research. We make use of these findings to build a uniquely novel VPET game, which is a first of its kind. We also found that there were only a limited number of educational research studies on visual privacy, and none of them explicitly studied the role of gamification to illustrate visual privacy concepts and other associated notions of security. of privacy using a game component as an educational tool.

V. OurVPET Game Design

As briefly explained earlier, our VPET game incorporates a unique gameplay concept involving two distinct roles played by separate users on the same device. In this game, one user assumes the role of an agent tasked with safeguarding their personal information. In contrast, the other user takes on the role of an adversary attempting to exploit the agent's vulnerabilities. As VPET is the central theme of this game, we implemented various elements within the game to emphasize the importance of protecting one's visual privacy, aligning with fundamental GenCyber concepts [19]. Table IV displays how we have specifically integrated critical cybersecurity concepts to design our VPET game. It shows

TABLE IV. Mapping Our VPET Game To The GenCyber Concepts [19]

GenCyber Concept	Mapping Justification / Relevance
Confidentiality	• VPET Game has access to spies on user's inputs and selected filters • Use of encryption to protect data privacy
Integrity	• VPET Game lets the user alter the filters applied as much as the user desires
Defense in Depth	• Uses multiple filters for hiding faces and encryption to stop decryption through luck
Adversarial Thinking	• VPET Game provides a better option and requires two agents - one will be the applying layers of defense, while the other will be breaking through them
Simplicity	• Uses simple filters and encryption for ease of comprehension

how we incorporate these concepts into the game play to provide players with a holistic understanding of visual privacy, including privacy filters, and empower them to make informed decisions for controlling their personal information.

Fig. 1. Original Image Privacy Enhancement Features in VPET Game. Picture Order 1: Original Image, 2: Face Blur Version, 3: Scribble Version

Fig. 2. Original Image Privacy Enhancement Features in VPET Game. Picture Order 1: Original Image, 2: Gaussian Blur Version, 3: Full Color

- *VPET Blur Face Functionality/Feature:* A privacy enhancement based face obscuration feature that adds a pixelation blur covering an individual's face in a selected/chosen picture (as seen in Figure 1)
- *VPET Scribble Functionality/Feature:* A privacy enhancing deidentification option that overwrites the picture, creating a scribble-like effect in the image (as seen in Figure 1).
- *VPET Gaussian Blur Functionality/Feature*: A privacy enhancing deidentification option for complete modification, that blurs the whole image (as seen in Figure 2).

- *VPET Full Color Functionality/Feature*: A privacy enhancing deidentification option with total modification, where the picture is camouflaged with a filter that changes the picture's color (as seen in Figure 2). This privacy filter works better when combined with another privacy filter.

These privacy filters are used by the first player (the Disguise Agent) to obscure or hide the identity in the chosen/selected picture, so that player two (also known as the Bounty Hunter) cannot identify who the chosen/selected individual is. The VPET introduces a key component of applied cryptography to enhance the gameplay experience and reinforce the importance of data security. After the first player successfully applies a privacy filter to camouflage a picture, the player is prompted to enter a unique four-letter code (as seen in Figure 3). This code is then encrypted and stored within the system. If the Bounty Hunter (second player) intends to reverse the privacy enhancing modification filter and uncover the identity in the picture, this player must decrypt the locked code (or ciphertext) correctly in order to capture the original picture. This aspect of encryption and decryption adds new layers of challenge and reinforces the significance of protecting sensitive information in the privacy context. This additional layer also demonstrates applied cryptography by encoding plaintext and decoding ciphertext.

If the Bounty Hunter successfully decrypts the four-letter code, then this second player can undo the effect of the privacy filter, that ws originally applied to the concerned picture. However, the second player is not provided with information regarding the specific type of privacy filter that was applied. Once the second player succesfully undoes the

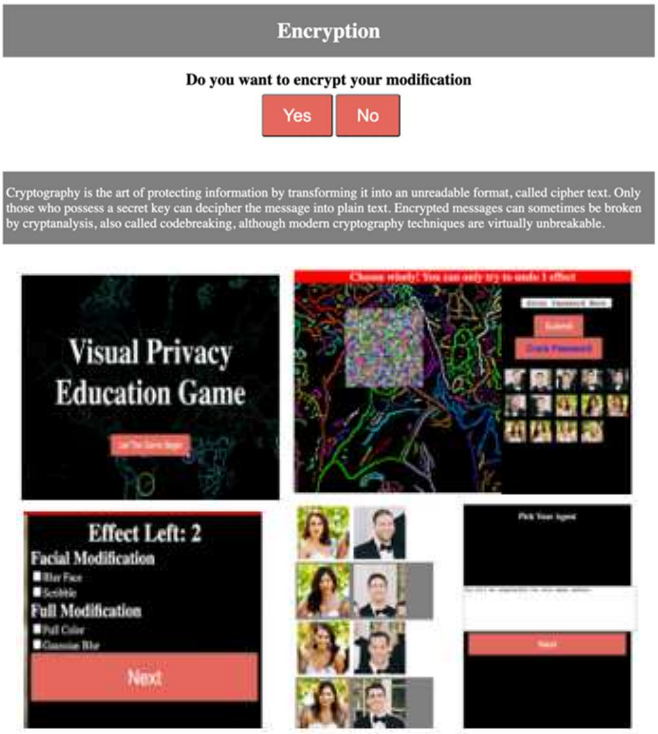

Fig. 3. Different Play Mode Screenshots & Features In Our VPET Game.

the privacy enhancing feature, then the individual identity (in the concerned picture) becomes compromised. This VPET game at the end challenges the Bounty Hunter to guess the identity (or identify the original picture), for which the player must rely on the individual's deduction skills. If the Bounty Hunter correctly guesses the identity, then that player wins the game. Conversely, if that player makes an incorrect guess, then the first player (Disguise Agent) wins the game and emerges victorious. Overall, this game emphasizes the concept of visual privacy through the hands-on demonstration and illustration of how the privacy of an individual is potentially compromised/breached, as well as how to safeguard/protect it via privacy-enhancing filters plus robust deidentification techniques. Figure 3 portrays some visuals from different play modes within the VPET game. We aim to evaluate whether our unique VPET gamification for educational purposes can successfully engage students for effective learning of data privacy and cybersecurity concepts.

VI. Survey Data And Results

Our work was aimed to develop data privacy awareness in players via the VPET gamified learning tool, and, therefore, we asked the participants/players to complete surveys for providing/sharing feedback plus inputs, so that we could evaluate the effectiveness of our VPET tool based gamified learning approach. The survey data, that we received as part of this research study, are categorized into two samples: Data Sample 1, which is the data collected from piloting an older, legacy version of the VPET game, and Data Sample 2, which is the data obtained through piloting of the current, work-in-progress version of the VPET game.

Data Sample 1 is based upon the participant insights and assessment of the game's impact on the participants awareness levels. It thus serves as a baseline for determining the game's effectiveness. By drawing inferences upon the findings from Data Sample 1, we made iterative improvements to the game design and enhanced the game contents to enhance its educational value and impact. Data Sample 2, which is the most recent survey data, was gathered after improvisations were made to the game. Our survey questionnaire was intended to evaluate the impact of the game on participants' awareness and perceptions of visual privacy. By comparing Data Sample 1 and Data Sample 2, we can assess the effectiveness of our design changes/enhancements, as implemented for the present VPET version, and the overall progress towards our goals.

The division of the survey data into two separate samples allowed us to track the evolution of participants' awareness and perceptions over time, providing valuable insights into the effectiveness of the VPET game as a learning tool. The survey data will be discussed in detail and analyzed in the following sections, highlighting the results achieved and the corresponding implications for visual privacy education.

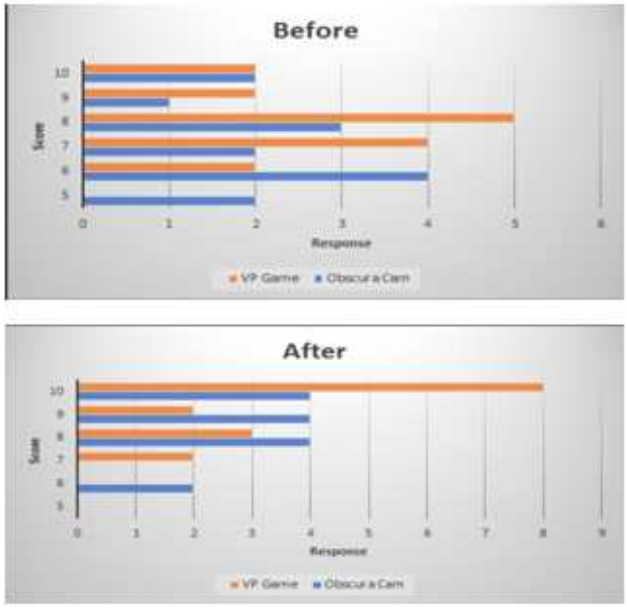

Fig. 4. Data Sample 1 Snapshot 1: *Participant Interests In Privacy Before & After Playing The VP Game Versus Before & After Using ObscuraCam.*

A. *Quantitative Survey Data Collection: Sample 1*

As part of our first data sample collection i.e. for collecting Data Sample 1, we did a comparative study involving two separate groups of high school student participants. One group was made to use the assigned to use different applications: one used the Visual Privacy (VP) game, while the other group made to use a VPET mobile app i.e. Obscura Cam. At the end of these separate group sessions, the participants were surveyed to gauge their interest level in data privacy before and after using the session. These participant responses are seen in Figure 4. Notably, this comparative data analysis reveals significantly higher interest levels among the student group who played the VP game, in comparison to the student group, who used the Obscura Cam app. This resulting observation indicates our game's positive and better impact on raising student interest levels in privacy, thus outperforming the Obscura Cam mobile app.

As part of the Data Sample 1 collection, we also asked the participants whether the VP themed game made their privacy conceptual learning experience enjoyable. This survey question resulted in a unanimous positive response, with 100% of the participants reporting that the VP game's theme contributed to a more engaging, interesting, and enjoyable learning experience, as displayed in Figure 5. This result underlines our game's effectiveness in creating an interactive and captivating environment for data privacy learning.

The Data Sample 1 results provide empirical evidence supporting the fact that the VP game not only stimulates player interest in data privacy, but also serves as an effective educational medium for engagement and enjoyment. These findings validate our approach of integrating gamification into visual privacy education, offering a novel and impactful method to create data privacy awareness and promote privacy plus security education among student participants.

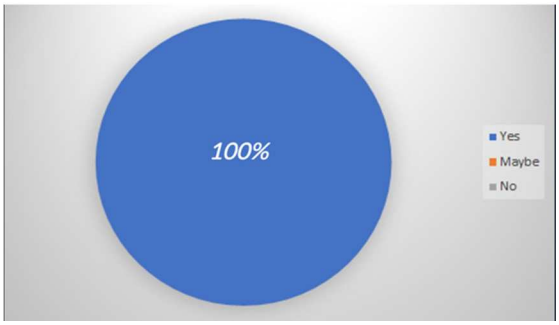

Fig. 5. Data Sample 1 Responses Snapshot 2: 100% Partcipant Agreement On Survey Question: *Do You Agree That The VP Game Made Your Data Privacy Learning Experience More Enagaging, Interesting and Enjoyable?*

As part of the Data Sample 1, we also specifically inquired about the participants' interest in data privacy by asking them to rate their interest levels in privacy on a scale of 1 to 10 before and after playing the VP game. The survey responses we received, as shown in Figure 6, reveal a substantial increase in interest levels among the participants after engaging with the game. To be more specific, before playing the game, the average participant interest was found

to be 7.21, and after playing the game, the average interest level notably improved by rising to 8.52. This increased average interest level points to the game's ability to captivate and engage participants fostering a greater interest in privacy.

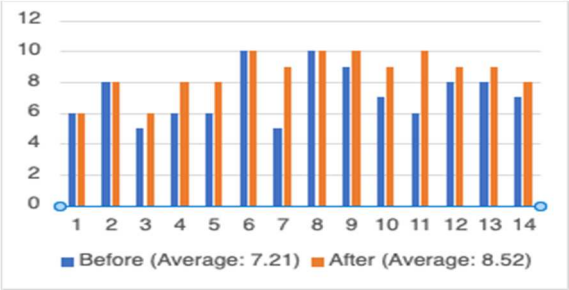

Fig. 6. Data Sample 1 Snapshot 3: Responses Showing *Average Interest Level in Privacy On A Scale Of 1 - 10 Before & After Playing The VP Game.*

Furthermore, as part of the Data Sample 1, we additionally gauged the participants' interest in cybersecurity concepts, including adversarial/offensive thinking and defensive strategies. Participants were asked to rate their interest levels in cybersecurity on a scale of 1 to 10 before and after playing the game. The survey responses, as highlighted in Figure 7, reveal a significant increase in interest levels following the VP gameplay experience. Before playing the game, the average interest level in cyber concepts was 7.92 on a scale of 1 to 10. However, after playing the VP game, the average interest level improved, notably rising to 8.81. This increase in interest indicates the VP game's efficacy in generating curiosity and interest in cybersecurity concepts, paving the participant learning path towards understanding of security concepts, adversarial thinking and defensive strategies.

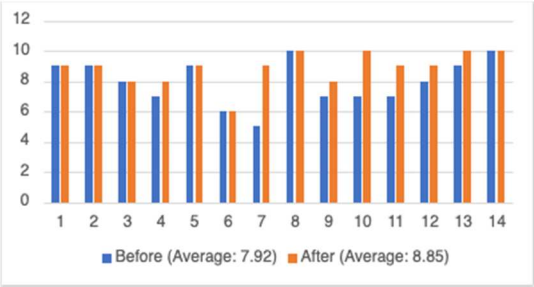

Fig. 7. Sample 1 Snapshot 4: Responses Showing *Average Interest Level in Cybersecurity On A Scale Of 1-10 Before & After Playing The VP Game*.

B. Quantitative Survey Data Collection: Sample 2

Fig. 8. Sample 2 Snapshot 1: Resonses Showing *Average Interest Level In Data Privacy On A Scale Of 1-5 Before & After Playing The VPET Game.*

As part of our Data Sample 2, we surveyed 32 high school community members, comprising of both students and teachers using the Qualtrics survey tool. After these participants played the present, work-in-progress version of the VPET game, we offered them some survey questionnaires. These survey responses have given us valuable insights into the participant experiences, including pre/post thoughts i.e. their perceptions before and after the VPET game sessions.

The first of these survey questions was focused on assessing the participants' interest in data privacy before and after engaging with the VPET game. On a scale of 1 to 5, we received an average interest score of 3.12 prior to playing the game. However, after experiencing the VPET game, the participants' average interest in privacy increased to 3.73, as shown in Figure 8. This observed improvement in participant interest level offers evidence of the game's efficacy in enhancing participants' interest in privacy, thereby contributing to a more enriching and engaging experience.

Fig. 9. Sample 2 Snapshot 2: Resonses Showing *Average Interest Level In Cybersecurity On A Scale Of 1-5 Before & After Playing The VPET Game.*

Continuing with our Data Sample 2 analysis, we next investigated the participants' level of interest in various cybersecurity topics, including data hiding, confidentiality, and cryptography, both before and after playing the VPET game. Using a scale of 1 to 5, we gathered insightful data regarding the participant interest level in these concepts. Before playing the game, the participants demonstrated an average interest level of 3.73. However, after they experienced the VPET game, we observed a modest increase in the average interest level to 3.88, as seen in Figure 9.

Fig. 10. Sample 2 Snapshot 3: Responses Showing *Average Participant Understanding Level Of Data Privacy On A Scale of 1-5 (On The Left) And The Average Rating of The VPET Game Design & Features In Terms Of Engagemnet & Education Value On A Scale of 1-5 (On TheRight).*

Additionally, the participants were asked to rate their overall understanding and awareness based on the knowledge acquired from playing the game. Using a scale of 1 to 5, we

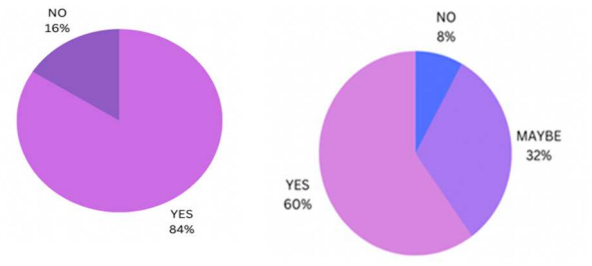

Fig. 11. Sample 2 Snapshot 4: Responses Showing *The Percentage Of Participants Who Think That Data Privacy Should Be In The K-12 Curriculum (On The Left) And The Percentage Of Participants Who Agreed That The Game Increased Their Learning Interests (On The Right).*

obtained an average rating of 3.4 on the overall understanding level of data privacy after engaging with the VPET game, as displayed in Figure 10. This result suggests that the VPET game effectively contributes to participants' understanding of data privacy notions and related cybersecurity concepts.

In addition, we sought feedback on the VPET game's design and features, focusing on aspects such as engagement and educational value. Participants were asked to provide a score on a scale of 1 to 5. The average rating obtained was 3.08 (as seen in Figure 10), indicating a positive evaluation of the game's overall design and ability to engage players. Additionally, the rating suggests that the game successfully presented a suitable level of challenge to keep participants engaged throughout their gameplay experience. Furthermore, participants were asked for their opinions on whether data privacy topics should be included in the K-12 curriculum. The responses were overwhelmingly positive, with 84% of participants agreeing to include data privacy in the K-12 curriculum, as revealed in Figure 11. Participants were further asked about their interest level and curiosity in learning more about data privacy after playing the VPET game. As illustrated in Figure 11, the responses indicate that 60% participants responded with a yes, asserting a confirmed interest, while 32% responded with a maybe, suggesting a possible interest, and the remaining 8% responded a with a no, indicating no interest. Participants were moreover asked to rate the overall significance of learning about data privacy as an information literacy topic. On a scale of 1 to 5, the average rating was 4.12, as eveident from Figure 12. This suggests that individuals perceive data privacy as an important literacy component in today's digital world.

In summary, these survey results imply that the VPET game has had a positive impact on learner engagement, interest and understanding of data privacy. The findings here have important implications for privacy education among young people. Visual privacy themed educational games like VPET could effectively increase privacy awareness and attitudes among youth, including high school learners. Our study also highlights the importance of privacy education for young people, especially at K-12 level, in today's digital age. By increasing awareness and promoting positive attitudes towards privacy, we can help empower young people to protect their personal information and make informed decisions about their digital lives.

Fig. 12. Sample 2 Snapshot 5: Responses Showing *Average Participant Rating Of The Significance Of Data Privacy As An Info Literacy Topic*

C. *Qualitative Survey Data Collection*

At the end of our participant survey, we asked the participants for feedback and additional comments about the game. The feedback we received was mostly positive. We even received some suggestions about the game that helped us improvise the game. Some feedback comments were:

- "An effective tool to help learn visual privacy."
- "Very clever idea, ideal for young students."
- "Nice activity to do with students to reinforce multiple layers of defense."

VII. Future Work

Based on the received feedback on our game, we plan to expand the game's functionality and specifications. We plan on making the game more interactive and practical. We will continue to pilot the game to a broader and more diverse audience beyond the high school learners. Though VPET has shown promise as an educational gamified tool for increasing privacy awareness, future improvements are needed. We could expand the game's contents to cover a broader range of privacy topics, incorporate multiplayer plus collaborative gameplay, enhance accessibility on different platforms & devices, and add to the current set of privacy filters. These enhancements would make the game more engaging, interactive, and adaptable to individual learning needs, ensuring effective results in privacy and security awareness.

VIII. Conclusion

Our main contribution is a novel, first of its kind VPET educational game. Our study has demonstrated the effectiveness of this game in increasing high school learners' data privacy awareness, engagement and interests. Our results show that playing the game improved participants' knowledge, attitudes and perceptions toward privacy. By making privacy education more engaging and interactive, such games could help bridge the gap between what students know and what they do to protect their personal info. Overall, this paper presents the prospects, benefits, and efficacy of our fresh, non-traditional approach in delivering privacy plus security education via a VPET theme based gamified experiential learning model, which is a maiden venture in cybersecurity educational research, and is unlike any of the existing privacy or security educational research studies.

REFERENCES

[1] A. Cetto, M. Netter, G. Pernul, C. Richthammer, M. Riesner, C. Roth, and J. Sänger, "Friend Inspector: A serious game to enhance privacy awareness in social networks" (Best Paper Award), 2014.

[2] A. Chattopadhyay and T. E. Boult, "Privacycam: a privacy preserving camera using uclinux on the blackfin dsp," in 2007 IEEE Conference on Computer Vision and Pattern Recognition, June 2007, pp. 1-8.

[3] A. Chattopadhyay and T. Nehring, "PVA (privacy through visual anonymity) lab for enhancing CS education and outreach," in Proceedings of the 45th ACM Technical Symposium on Computer Science Education, March 2014, pp. 723-723.

[4] A. Chattopadhyay, D. Christian, A. Oeder, and I. Budul, "A Novel Visual-Privacy Themed Experiential- Learning Tool for Human-Privacy & Societal-Security Awareness in Middle-School and High-School Youth," *IEEE Xplore*, Oct. 01, 2019. https://ieeexplore.ieee.org/abstract/document/9028375

[5] A. Chattopadhyay, D. Christian, A. Ulman, and C. Sawyer, "A Middle-School Case Study: Piloting A Novel Visual Privacy Themed Module for Teaching Societal and Human Security Topics Using Social Media Apps," in 2018 IEEE Frontiers in Education Conference (FIE), October 2018, pp. 1-8.

[6] Joint Task Force on Cybersecurity Education, "Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity," Association for Computing Machinery, New York, NY, USA, 2018. [Online]. Available: https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf. [Accessed: May 14th, 2023].

[7] S. Livingstone, "Children: a special case for privacy? " Intermedia, vol. 46, no. 2, pp. 18-23, 2018.

[8] M. Sturdee, L. Thornton, B. Wimalasiri, and S. Patil, "A Visual Exploration of Cybersecurity Concepts," in Creativity and Cognition, June 2021, pp. 1-10.

[9] "ObscuraCam: The Privacy Camera," *Guardian Project*. https://guardianproject.info/apps/org.witness.sscphase1/.

[10] X. Yu and N. Babaguchi, "Privacy preserving: hiding a face in a face," in Computer Vision–ACCV 2007: 8th Asian Conference on Computer Vision, Tokyo, Japan, November 18-22, 2007, Proceedings, Part II 8, November 2007, pp. 651-661.

[11] C. Mekhail, "A Day in the Life of the Jos: The Design of an Educational Game on Privacy," Doctoral dissertation, Carleton University, 2016.

[12] E. Berger, T. H. Sæthre, and M. Divitini, "PrivaCity: A Chatbot Game to Raise Privacy Awareness Among Teenagers," in Informatics in Schools. New Ideas in School Informatics: 12th International Conference on Informatics in Schools: Situation, Evolution, and Perspectives, ISSEP 2019, Larnaca, Cyprus, November 18–20, 2019, Proceedings 12, 2019, pp. 293-304.

[13] Privacy Curriculum Matrix K-12 BEaPRO, "iKeepSafe," [Online]. Available: https://ikeepsafe.org/content/uploads/2017/08/2017iKeepSafe-Privacy-Curriculum-Matrix-K-12-BEaPRO.pdf.

[14] T. Orekondy, B. Schiele, and M. Fritz, "Towards a visual privacy advisor: Understanding and predicting privacy risks in images," in Proceedings of the IEEE International Conference on Computer Vision, October 2017, pp. 3706-3715.

[15] C. Stellmacher, J. Ternieten, D. Soroko, and J. Schöning, "Escaping the Privacy Paradox: Evaluating the Learning Effects of Privacy Policies With Serious Games," Proceedings of the ACM on Human-Computer Interaction, vol. 6 (CHI PLAY), pp. 1-20, 2022.

[16] M. Williams, J. R. Nurse, and S. Creese, "(Smart) Watch Out! encouraging privacy-protective behavior through interactive games," International Journal of Human-Computer Studies, vol. 132, pp. 121-137, 2019.

[17] R. Yusri, A. Abusitta, and E. Aïmeur, "Teens-online: A game theory-based collaborative platform for privacy education," International Journal of Artificial Intelligence in Education, vol. 31, pp. 726-768, 2021.

[18] Sumit Kumar Paul and D. A. Knox, "A Taxonomy and Gap-Analysis in Digital Privacy Education," pp. 221–235, Jan. 2023, doi: https://doi.org/10.1007/978-3-031-30122-3_14.

[19] "GenCyber – DoD Cyber Exchange," *public.cyber.mil*. https://public.cyber.mil/gencyber/.

[20] A. Chattopadhyay, D. Christian, A. Ulman, and S. Petty, "Towards a Novel Visual Privacy Themed Educational Tool for Cybersecurity Awareness and K-12 Outreach," in Proceedings of the 19th Annual SIG Conference on Information Technology Education, September 2018, pp. 159-159.