Contributing Factors in Measuring Interest Levels in VR Cybersecurity Training

Shaila Rana[1], Saad E. Rana[2]
Cybersecure[1]
Independent Researcher[2]
USA

Abstract

There is a significant focus on cybersecurity training to thwart and respond to cyberattacks, which continue to grow in ubiquity and complexity. Traditional cybersecurity training may not always be effective in the aforementioned. Thus, Virtual Reality (VR) cybersecurity training modules may remediate ineffective cybersecurity training platforms. However, the interest levels in undergoing VR cybersecurity training and the potential acceptance of VR cybersecurity training need to be examined. Thus, this article aims to investigate the factors that influence interest in VR cybersecurity training modules. The factors being examined include gender and age. Overall, a better understanding of these factors can help decision makers understand if VR cybersecurity training platforms can be right for their organization. In general, this study found that gender and age do not affect the interest levels in undergoing VR cybersecurity training modules. Additionally, this study examines the relationship between traditional cybersecurity training methods and VR cybersecurity training methods. This study aims to gather participants' perceived interest levels, usefulness, and ease of using VR cybersecurity training platforms. Furthermore, this study explores the impact of previously undergoing a form of cybersecurity training on the overall interest levels of VR cybersecurity training. A difference was noted between the overall interest levels of participants that have not undergone a form of cybersecurity training and those that have undergone a form of training. The overall interest level, usefulness, and ease of use differed between the groups that did not undergo cybersecurity training. Consequently, this demonstrates that there may be a current gap in cybersecurity training that can be filled by an interactive and engaging cybersecurity training platform, such as VR simulations and games.

1. Introduction

Cybersecurity training is vital due to the ubiquity and growing complexity of cyberattacks. Consequently, there is a growing importance on effective cybersecurity training. There are issues that exist in traditional cybersecurity training methods [1]. Traditional cybersecurity training methods are noted as being "boring and ineffective" [2]. Other problems with traditional cybersecurity training methods include the inability to demonstrate real world scenarios and realistic attacks [3]. A lack of realistic, entertaining, engaging, and stimulating training methods may translate to poor learning outcomes [2]. Therefore, alternatives to traditional cybersecurity training need to be explored. VR training platforms may present remediations to the aforementioned issues. However, there are few studies that focus on the potential use of VR training modules for cybersecurity training. Moreover, there are few commercial entities that provide VR training for cybersecurity learners. Thus, this study aims to fill a gap in current research by examining what factors may influence the potential acceptance and adoption of VR training platforms to alleviate some of the issues present in traditional cybersecurity training methods.

Cybersecurity training exercises are becoming increasingly popular in universities and professional training paths [4]. The increasing demand points towards the necessity of effective training methods. In general, cybersecurity training is noted to be a critical research area [4]. Traditional training methods have been noted to have shortcomings, specifically with difficulties in creating training material that is engaging, interactive, and entertaining for users. VR training has had success in the medical field and has been inherently more engaging and interactive through an immersive experience. However, VR cybersecurity training remains understudied in academia, and its numbers in the commercial field remain low.

Effective cybersecurity training can help defend individuals and organizations alike against the growing complexity and number of cyber-attacks. Traditional cybersecurity training methods face challenges, which may be alleviated through VR training modules. However, VR cybersecurity training methods have not been heavily explored in academic and commercial settings. Thus, this study aims to determine if a gap exists within the cybersecurity training discipline and if that can be filled with VR training methods. TAM is a model that can determine if a new technology will be accepted or rejected. A survey is constructed utilizing concepts from TAM. This study attempts to gauge user

 | DOI: 10.20533/ijds.2040.2570.2023.0231

perceptions of VR cybersecurity training and determine a difference between users who have not undergone some cybersecurity training. Furthermore, this study explores the perceived ease of use and usefulness of VR cybersecurity training between the two groups mentioned above. If a difference is discovered, it may demonstrate a need to study and create VR cybersecurity training modules. Moreover, this may create a new direction for cybersecurity training.

2. Research Contribution

This study hopes to contribute to the cybersecurity training field by gauging interest levels in a new method to train users in cybersecurity awareness. As minimal research is done on VR cybersecurity training, this study hopes to determine its potential viability in the cybersecurity training discipline. If significant interest levels are found with traditional cybersecurity training satisfaction levels, it could demonstrate that a gap exists within the cybersecurity training discipline. This study may uncover the need for including training formats that are engaging, interactive, and entertaining for learners. Overall, if VR training is deemed interesting, this could create a new direction for cybersecurity training practices. Subsequently, this paper hopes to contribute to interesting and desirable cybersecurity training through VR simulations to address traditional training methods' challenges. Specifically, this paper hopes to demonstrate that VR training modules can be a preferable form of cybersecurity training.

2.1. Cybersecurity and Gender

Gender may play a role in the adoption and overall success of cybersecurity training platforms. In cybersecurity training, studies demonstrate a gender difference in cybersecurity self-efficacy and behavior [5]. Moreover, studies demonstrate that training is required to close the gender gap that exists in cybersecurity [5]. Gender was found to play a role in cybersecurity behaviors and affected security self-efficacy and self-reported cybersecurity behaviors [5]. Moreover, gender was found to be a factor in cybersecurity training [6]. Gender was found to be a significant factor in cybersecurity training [6]. Subsequently, this study aims to examine the influence that gender may have on the potential adoption of VR technology for cybersecurity training.

3. Cybersecurity and Age

Cybersecurity training is essential for everyone, regardless of age. However, age may be a factor in terms of the interest levels and potential adoption of VR cybersecurity training technologies. Age is found to be a factor in terms of peer behavior, familiarity with cyber threats, response efficacy, and more [7]. Thus, it is important to identify if this factor is a significant motivator in attitudes toward VR cybersecurity training modules. This information may allow decision makers to determine the potential acceptance or rejection of this technology within organizations. Furthermore, the potential efficacy of VR cybersecurity training solutions may be understood depending on whether or not age is a component of interest levels in undergoing VR training.

4. Technology Acceptance Model

The Technology Acceptance Model, or TAM, is a methodology that is a way in which to determine the acceptance or rejection of a technology [8]. Consequently, this model is the basis for exploring the potential use of VR training modules in the cybersecurity training discipline. Technology continues to evolve and be integrated into personal and professional atmospheres [8]. Consequently, this model demonstrates that before the technology is integrated into private and professional lives, the attitudes toward its use must be explored. VR cybersecurity training is sparse in both academia and the commercial field, demonstrating its rudimentary nature. Consequently, before widespread acceptance, attitudes toward the use of VR simulations must be gauged. In this study, VR cybersecurity training attitudes will be gauged through potential interest levels in undergoing this training module. TAM has become a key predictor of a new technology's potential acceptance or rejection [3]. TAM is seen as a model to study the initial and continual adoption of a technology [9].

For example, TAM was utilized to predict the acceptance of the Internet or the World Wide Web [10]. In a survey conducted with 163 participants, TAM demonstrated the potential ease of use and usefulness of the world wide web [10]. Essentially, the research investigated the potential acceptance of the World Wide Web as a practical application [10]. As demonstrated, this technology became the backbone of private and professional lives. Consequently, this study proposes to follow TAM to gauge user attitudes toward using VR in cybersecurity training to determine if it can remedy the problems found with traditional cybersecurity training methods.

TAM includes assessing the perceived usefulness, perceived ease of use, and overall attitudes toward technology to determine its overall acceptance [11]. TAM can explain behavior through surveys to determine positive attitudes towards a particular technology [shih]. Subsequently, this survey attempts to gauge the perceived usefulness, perceived ease of use, and overall attitude or interest levels of VR cybersecurity training. Utilizing this robust and

 | DOI: 10.20533/ijds.2040.2570.2023.0231

widely accepted model can predict the potential efficacy and widespread use of VR in the cybersecurity training field.

This study bases its theory on TAM. TAM is a model that researchers utilize to measure user attitudes toward new technology. Studies continue to utilize TAM to predict the acceptance of new technology. The variables of this study are interest levels in VR cybersecurity training. The Technology Acceptance Model, or TAM, is a method to predict the acceptance or rejection of a technology [8]. It is a model to predict human behavior toward new technology, explicitly adopting or rejecting it. This model has its origins in psychological theories of planned behavior and reason action [8]. However, this model determines user attitudes toward technology adoption. TAM is a pivotal model for predicting human behavior toward a new technology [8].

5. Survey

This study bases its theory on the Technology Acceptance Model, or TAM. TAM is a method researchers utilize to determine the potential acceptance of new technology. Furthermore, researchers continue to use TAM to investigate the influences and relationships of a variable on the potential acceptance of a new technology. Inferential statistics allow this study to utilize statistical analysis to understand a population [12]. A survey was created based on TAM that was disseminated via the SurveyMonkey platform. The results asked about a participant's age, gender, and interest levels, perceived ease of use, and perceived usefulness of VR cybersecurity training. This survey attempts to determine a correlation between gender and age and interest levels in VR cybersecurity training. Participants are asked to enter their gender and age range. The participants that did not enter this information were not included in this study. Furthermore, respondents were asked to rate their interest levels, perceived ease of use, and perceived usefulness on a scale from 0-10.

The population of participants was reached through two methods: emails and paid survey responses from SurveyMonkey. As cybersecurity training is becoming more prevalent, professionals have likely had cybersecurity training regardless of the professional field. Thus, emails with the survey link and brief descriptions about the study were distributed to professionals. Finally, SurveyMonkey has a paid method to distribute a survey to a general population. This study utilized this option to distribute the survey to a wide range of users.

The survey consists of thirteen questions and is a mix of yes or no questions, multiple select answers, and 11-point rating scales. Participants are asked if they have undergone some form of cybersecurity training, what training methods were utilized, and how many hours were dedicated to cybersecurity training. Participants in the survey were asked if they would be interested in VR cybersecurity training and the corresponding interest level on an 11-point scale. Additionally, participants were asked to rate their perceived ease of use and usefulness on an 11-point scale.

6. Gender

The average interest levels for males and females differed, as shown in Table 1. On average, the interest level for males was 7.17. On the other hand, the average interest level for females was 5.58. Moreover, the average perceived usefulness of VR cybersecurity training was 7.17 for males and 5.81 for females. The average perceived ease of use of VR cybersecurity training modules was 7.12 for males and 5.71 for females.

Table 1. Average Interest Levels for Males and Females

Gender	Interest Level	Perceived Usefulness	Perceived Ease of Use
Male	**7.16**	**7.18**	**7.12**
Female	**5.58**	**5.81**	**5.71**

In a t-test conducted, between the reported interest levels of males and females, no statistical significance was demonstrated (M = 6.56, SD = .31) with a result of t [86] = 15.65, p = 3.38. Consequently, this demonstrates that there may not be a significant difference in the potential attitudes and interest levels in VR cybersecurity training modules. Thus, this may assist organizations that are looking to determine whether or not the potential adoption or acceptance of this training platform is dependent upon gender.

7. Age

In the survey, age was broken down into four groups: 18-29, 30-44, 45-60, and over 60. Table 2 demonstrates the average interest level divided into the aforementioned groups. The highest reported interest levels, perceived usefulness, and perceived ease of use were among the age group of 45-60. Alternatively, the lowest interest level in undergoing VR cybersecurity training was for both the age groups 18-29 and 30-44, with an average of 6.31. The perceived usefulness of VR cybersecurity training was lowest among the age group of 18-29, with a reported average of 6.19. Moreover, the perceived ease of use was lowest among the age group of participants over 60.

 | DOI: 10.20533/ijds.2040.2570.2023.0231

Table 2. Average Interest Levels for ages 18-29, 30-44, 45-60, and 60+

	Interest Level	Perceived Usefulness	Perceived Ease of Use
18-29	6.31	6.19	5.5
30-44	6.31	6.21	6.41
45-60	7.07	7.47	7.57
60+	6.33	6.67	5

A t-test was performed to determine if age influenced interest levels in VR cybersecurity training. The t-test results determined that there is no significance on the effect of age on interest levels in VR cybersecurity training (M = 6.56, SD = .31) with a result of t [95] = 13.17, p = 1.84. Subsequently, this highlights that age may not be a critical factor in interest levels in VR cybersecurity training. Moreover, this demonstrates that the potential acceptance or rejection of VR modules in cybersecurity training may not be dependent upon the factor of age. Thus, decision-makers may not need to focus on age as a deciding factor when determining whether to implement VR cybersecurity training platforms.

8. Average Interest Levels

The distributed survey collected 377 user responses. Out of 377 collected responses, 238 respondents reported that they had previously undergone some cybersecurity training. One hundred thirty-nine participants have not previously undergone some form of cybersecurity training.

The average interest level for users that have undergone some form of cybersecurity training was 6.71. Furthermore, the perceived usefulness average was 6.85, and the perceived ease of use was 6.79. Alternatively, for users that have not previously undergone a form of cybersecurity training, the average interest level was 4.69. The perceived usefulness was averaged at 5.23, and the average perceived ease of use was 5.1. Subsequently, a difference in averages of interest levels, perceived usefulness, and ease of use was demonstrated between users who have not undergone some cybersecurity training.

The mode for users that have undergone cybersecurity training for an average interest level was 10. On the other hand, the mode for users that have not undergone any form of cybersecurity training was 0. Subsequently, this further demonstrates the difference in interest levels between the two groups. In general, the mode for both groups exhibits that interest in VR cybersecurity training exists for users that are required to or are interested in cybersecurity training. All in all, a general interest in VR cybersecurity training is demonstrated in the survey findings.

Table 3. Average interest levels, average perceived usefulness, and average perceived ease of use

	Cybersecurity Training	No Cybersecurity Training
Average Interest Level	6.71	4.69
Average Perceived Usefulness	6.85	5.23
Average Perceived Ease of Use	6.79	5.10

The difference in average results between the two groups of users: those who have and those who have not undergone some form of cybersecurity training, demonstrates a need for cybersecurity training modules. Lower average interest levels in undergoing VR cybersecurity training were demonstrated in the group of users that have not undergone some form of cybersecurity training. The lower average interest levels of VR cybersecurity training can be because the users do not need to undergo cybersecurity training. Furthermore, there may be no interest in undergoing any form of cybersecurity training. On the other hand, there was a higher average interest level in undergoing VR cybersecurity training for users that have undergone some form of cybersecurity training in the past. The higher average interest levels in VR cybersecurity training for users who have undergone some cybersecurity training demonstrates a need to study and develop VR cybersecurity training platforms. This may hint towards a general dissatisfaction with current cybersecurity training methods. Traditional cybersecurity training methods can be generally categorized as video-based, text-based, instructor-led, and game-based training [rana]. Traditional cybersecurity training is cited as being ineffective in changing user behavior and defending against cyber threats [13]. Learning models have been developed to deal with cybersecurity training [1]. However, issues are still ever-present in cybersecurity training tactics [1]. Training platforms are cited as being effective if they include interactive content [3]. Furthermore, some problems of traditional cybersecurity training include a lack of motivation and a lack of interest in training methods [3]. Cybersecurity training is essential to disseminate information regarding cybersecurity fundamentals, it must be done effectively [14]. For training to be effective, the material being taught should be exciting and simple [14]. Cybersecurity training is noted as being "heterogeneous" [15]. Factors that cause this heterogeneity include different target audiences,

 | DOI: 10.20533/ijds.2040.2570.2023.0231

organizations, content, technical capabilities, and more [15]. Visual-based training can work with heterogeneous activity because it is tailored to the user through specialized visual tools [15]. Visual-based learning is utilized in many other industries for effective training; thus, visual-based learning should be employed in the cybersecurity field [15]. Engagement is a critical factor for the successful learning of cybersecurity concepts [16]. The higher the level of engagement and interactivity, the more effective training can be. Replicating real-world scenarios is difficult, especially for traditional training methods [17]. Realistic and simulated training allows students to prepare for current and future threats [18]. Consequently, the aforementioned issues demonstrate a need for programs that are interactive, realistic, and entertaining. As highlighted in the survey, there is an interest level in undergoing VR training with users that have had some form of interaction with cybersecurity training.

Game-based training is a cybersecurity training method that has been demonstrated to foster positive user outcomes [19]. However, VR cybersecurity training is to be made distinct from game-based training in that most forms of game-based training do not account for the visual and highly interactive component of VR cybersecurity training. VR applications for cybersecurity training include thematic, stylistic, and mechanical aspects [20]. These design insights create cybersecurity training with a digital agent in VR applications [20]. In general, VR simulations are an extension of game-based training and include the component and layers of engaging and interactive material. In general, the difference in modes between the two groups demonstrates that users that have had cybersecurity training are interested in VR cybersecurity training modules.

9. Limitations of the Study

One of the limitations of this study is that the sample population mainly included adults from North America. Instead, a global population would give a more comprehensive view of the relationship between gender and age and interest in VR cybersecurity training. Furthermore, survey responses are subjective and depend upon the mood of the participant. Responses depend upon how the participant felt at that moment influence the ratings of interest levels and perceived levels of usefulness and ease of use of VR training. Subsequently, answers may vary upon the participant's emotional state. Thus, self-reported feedback is a limitation because answers can change depending upon a human emotion factor. This study's limitation also includes the sample population. A larger sample is always of more benefit for further analysis of a relationship between two variables. Consequently, a sample consisting of more than four hundred participants would be beneficial.

10. Future Work

The Technology Acceptance Model (TAM) utilizes interest levels, perceived usefulness, and perceived ease of use of a technology before predicting whether this technology will be accepted or rejected. Consequently, this study has the data to analyze the relationship between age and gender and the perceived ease of use and usefulness of VR cybersecurity training technologies. Moreover, future studies can conduct additional analysis on interest levels in VR training, especially in conjunction with attitudes toward the usefulness and ease of use of VR training modules. Hence, this would give a more comprehensive and holistic view to predicting the acceptance or rejection of VR training modules in the cybersecurity training industry.

11. Conclusion

Cybersecurity training is becoming commonplace in organizations and encouraging safe personal behavior. Cyber-attacks continue to evolve and grow in ubiquity and complexity. The first line of defense is noted as being adequate and effective cybersecurity training. Cybersecurity training comes in many forms, depending on the audience, learning objectives, budget, resources, and more. With the importance of cybersecurity training noted, this field remains an understudied and underdeveloped discipline.

A study has not yet been conducted gauging the potential interest in undergoing VR cybersecurity training. Furthermore, the potential influence of traditional cybersecurity training methods on the interest level of VR cybersecurity training has not been measured. If a significant interest level is detected, this may create a new direction for cybersecurity training.

VR training is helpful in the healthcare industry for medical training [21]]. Subsequently, this hints toward more widespread use of VR technologies in other industries to enhance user experiences for more positive learning outcomes. However, the interest levels in introducing VR cybersecurity training have not been examined. This study aims to fill the gap in the current literature to determine if there is a higher interest level in users who have undergone cybersecurity training than those who have not.

In this study, user attitudes towards VR cybersecurity training were higher in users who have had experience with cybersecurity training than users who have not. A higher average of interest levels, perceived usefulness, and perceived ease of use in users with experience with cybersecurity training demonstrate an interest in VR training platforms. Consequently, this need should be further explored in academia and commercial settings to fill the current gap in cybersecurity training.

 | DOI: 10.20533/ijds.2040.2570.2023.0231

Effective cybersecurity training needs to be explored to provide a defense against cyberattacks that threaten organizations and individuals alike. VR cybersecurity training has not yet received widespread focus on its potential efficacy in the cybersecurity training industry. Thus, this study aims to explore the factors that may affect the potential acceptance or rejection of VR cybersecurity training technologies. While gender and age have previously affected certain cybersecurity behaviors, statistical analysis demonstrated that gender did not affect the interest levels in undergoing VR cybersecurity training platforms. Moreover, while age has historically been a factor in cybersecurity behaviors, this study demonstrates that age did not significantly impact the interest levels in VR cybersecurity training modules. Consequently, the results of this study may be important for decision makers when determining whether or not to introduce VR cybersecurity training platforms for effective cybersecurity training. In general, this study determines that gender and age may not influence interest in undergoing VR cybersecurity training.

11. References

[1] Thakong, M., Phimoltares, S., Jaiyen, S., and Lursinsap, C. (2018). One-pass-throw-away learning for cybersecurity in streaming non-stationary environments by dynamic stratum network. PloS one, 13(9), e0202937.

[2] Abawajy, J. (2014). User preference of cyber security awareness delivery methods. Behaviour and Information Technology, 33(3), 237-248.

[3] Aldawood, H., and Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. Future Internet, 11(3), 73.

[4] Maennel, K. (2020, September). Learning Analytics Perspective: Evidencing Learning from Digital Datasets in Cybersecurity Exercises. In 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 27-36). IEEE.

[5] Anwar, M., He, W., Ash, I., Yuan, X., Li, L., and Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. Computers in Human Behavior, 69, 437-443.

[6] Daengsi, T., Pornpongtechavanich, P., and Wuttidittachotti, P. (2021). Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks. Education and Information Technologies, 1-24.

[7] Fatokun, F. B., Hamid, S., Norman, A., and Fatokun, J. O. (2019, December). The impact of age, gender, and educational level on the cybersecurity behaviors of tertiary institution students: an empirical investigation on Malaysian universities. In Journal of Physics: Conference Series (Vol. 1339, No. 1, p. 012098). IOP Publishing.

[8] Marangunić, N., and Granić, A. (2015). Technology acceptance model: A literature review from 1986 to 2013. Universal access in the information society, 14(1), 81-95.

[9] Hong, S., Thong, J. Y., & Tam, K. Y. (2006). Understanding continued information technology usage behavior: A comparison of three models in the context of mobile internet. Decision support systems, 42(3), 1819-1834.

[10] Lederer, A. L., Maupin, D. J., Sena, M. P., & Zhuang, Y. (2000). The technology acceptance model and the World Wide Web. Decision support systems, 29(3), 269-282.

[11] Chen, I. J., Yang, K. F., Tang, F. I., Huang, C. H., & Yu, S. (2008). Applying the technology acceptance model to explore public health nurses' intentions towards web-based learning: A cross-sectional questionnaire survey. International journal of nursing studies, 45(6), 869-878.

[12] Asadoorian, M. O., and Kantarelis, D. (2005). Essentials of inferential statistics. University Press of America.

[13] Sabillon, R., Serra-Ruiz, J., & Cavaller, V. (2019). An effective cybersecurity training model to support an organizational awareness program: The Cybersecurity Awareness TRAining Model (CATRAM). A Case Study in Canada. Journal of Cases on Information Technology (JCIT), 21(3), 26-39.

[14] Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour?. arXiv preprint arXiv:1901.02672.

[15] Ošlejšek, R., Rusnák, V., Burská, K., Švábenský, V., Vykopal, J., & Cegan, J. (2020). Conceptual Model of Visual Analytics for Hands-on Cybersecurity Training. IEEE Transactions on Visualization and Computer Graphics.

[16] Kam, H. J., Menard, P., Ormond, D., & Crossler, R. E. (2020). Cultivating cybersecurity learning: An integration of self-determination and flow. Computers & Security, 96, 101875.

[17] Wahsheh, L. A., & Mekonnen, B. (2019, December). Practical cyber security training exercises. In 2019 International Conference on Computational Science and Computational Intelligence (CSCI) (pp. 48-53). IEEE.

[18] Nevmerzhitskaya, J., Norvanto, E., & Virag, C. (2019). High impact cybersecurity capacity building. In The International Scientific Conference eLearning and Software for Education (Vol. 2, pp. 306-312). " Carol I" National Defence University.

[19] Gonzalez, H., Llamas, R., & Ordaz, F. (2017). Cybersecurity Teaching through Gamification: Aligning Training Resources to our Syllabus. Res. Comput. Sci., 146, 35-43.

[20] Adinolf, S., Wyeth, P., Brown, R., & Altizer, R. (2019, December). Towards designing agent based virtual reality applications for cybersecurity training. In Proceedings of

 | DOI: 10.20533/ijds.2040.2570.2023.0231

the 31st Australian Conference on Human-Computer-Interaction (pp. 452-456).

[21] Kasurinen, J. (2017). Usability issues of virtual reality learning simulator in healthcare and cybersecurity. Procedia computer science, 119, 341-349.

 | DOI: 10.20533/ijds.2040.2570.2023.0231