Augmented Reality-Based Cybersecurity Education on Phishing

Yan-Ming Chiou, Chien-Chung Shen
Department of Computer and Information Sciences
University of Delaware
Delaware, USA
steveice@udel.edu/cshen@udel.edu

Chrystalla Mouza, Teomara Rutherford
School of Education
University of Delaware
Delaware, USA
cmouza@udel.edu/ teomara@udel.edu

2021 IEEE International Conference on Artificial Intelligence and Virtual Reality (AIVR) | 978-1-6654-3225-2/21/$31.00 ©2021 IEEE | DOI: 10.1109/AIVR52153.2021.00052

***Abstract*—With the rising of remote work and schooling, the adaption of emerging technologies to teach the concepts of cybersecurity becomes critical. In this work, we present the concept, design, and prototype of a Mixed Reality-based cybersecurity education application on phishing, so that school children could be exposed to the subject remotely and practice to differentiate malicious from genuine messages.**

Keywords- Mixed Reality, Cybersecurity Education, Phishing.

I. INTRODUCTION

The technologies of Augmented Reality (AR), Virtual Reality (VR), and Extended Reality (XR) have expanded their application domains from entertainment (such as gaming and virtual tours) to education, healthcare, and manufacturing in the past few years [13]. Using these immersive technologies, people can interact and collaborate with one another around the world without being constrained by physical boundaries or locations. In the Covid-19 pandemic, people have been utilizing single-user or multi-user collaborative VR applications in all aspects of daily life–work, social, education, business, entertainment [15]. In particular, for education, teachers and students can join a virtual classroom together to learn and share knowledge in any context, such as going for a field trip [14]. In addition, companies can train their employees remotely in virtual environments so that they may learn and experience with the operations and maintenance of sophisticated machines without having to physically travel to a particular training center [15].

As more and more educational activities move online, children are spending more time on-line with the increasing risk of being the targets of phishing attacks by hackers and criminal organizations. Therefore, cybersecurity education for school children becomes critical [17]—children must be able to recognize different attacks and protect their personal information. And for the educators, the cybersecurity education content needs to be more accessible and easily implemented by educators without highly specialized cybersecurity expertise and programming skills.

More specifically, we focus on designing and prototyping an interactive application that can make phishing, an essential abstract cybersecurity concept, more tangible for learners using the immersive technology of Mixed Reality. Moreover, many studies showed some positive impacts of using AR applications on motivation, long-term memory retention, and conceptual knowledge understanding [1]. However, there is a gap in integrating AR with real-world objects to show how students interact with these systems with their peers in-person or remotely [2,3]. To address this gap, we plan to examine ways of designing creative AR applications that improve students' motivation, learning, and collaboration by combining physical and virtual interactions between the AR system and people [4]. For this purpose, AR can not only interact with the real-world object but can promote remote collaboration through a shared network session via a network-connected device (smartphone or tablet) to engage students to work as a team from anywhere in the world. Therefore, students can become collaborative partners and co-creators of their learning [5].

This paper presents our design and prototype of an interactive activity to educate the cybersecurity concept of phishing, which is addressed in the Computer Science Teacher Association standards (Networks & the Internet with a specific focus on safety, privacy, and security). In particular, the paper describes (1) the initial[1] design of AR-based cybersecurity activity with the potential to engage and motivate school students, (2) the implementation of a Mixed Reality-based phishing applications and its procedure of using this application.

II. RELATED WORK

A. Augmented Reality Education

AR technology has been showing its potential in areas such as education, medicine, and entertainment due to its capability of bringing digital contents into the physical world [18]. The coexistence of virtual and tangible information in AR allows people to visualize and interact with abstract concepts [6]. Taking education as an example, Tomoki Itamiya [7] used VR/AR for disaster education which includes that most of the natural disasters (e.g. tsunami,

[1] Our project draws on a transdisciplinary approach that includes the end-users (both educators and students) in every aspect of iterative design. In this work-in-progress paper, we present the initial design of the phishing application without any input from the end-users yet.

978-1-6654-3225-2/21/$31.00 ©2021 IEEE
DOI 10.1109/AIVR52153.2021.00052

earthquakes, and typhoons) in Japan's elementary and junior high schools. Lin et al. [8] combines AR with the deep learning recommendation system to help students from non-CS majors to learn programming and computational thinking.

B. *Cybersecurity Education for Phishing*

As time moves on, the techniques of designing phishing messages become too elegant and sophisticated to be distinguished from legitimate messages without regular training or the help of antivirus software [19]. There are literatures focusing on phishing training using web-based platforms [9,10,11]. For instance, Nicholson et al. [9] used PhishTank (a famous phishing mail database) to design twelve phishing emails to test teenagers' ability to distinguish the emails in an interactive web platform. Similarly, Nima et al. [10] developed a web game called "what could go wrong?" to help the player understand the consequence of making the wrong decision after clicking a malicious link on a mobile device. Wen et al. [11] developed *What.Hack*, an anti-phishing online simulation game that teaches phishing concepts and simulates actual phishing attacks in a role-playing game. This work ussed the web as the platform to educate students on the essential cybersecurity concepts. In contrast, our work focuses on the new interaction form of AR technology and collaborative learning to help students learn this abstract cybersecurity knowledge with an tangible and immersive way of learning.

III. RESEARCH GOALS AND PROPOSED WORK

The overall research goals of the work are to design AR-based applications for teaching several concepts of cybersecurity in a tangible manner. In particular, we focus on phishing in this paper and discuss about how we designed an AR-based applications for teaching cybersecurity knowledge in an immersive and collaborative fashion. Overall, we plan to conduct a pilot study to measure and evaluate the cybersecurity knowledge and motivation of the students.

A. *Concept of Phishing*

Phishing [16] is a deceitful attempt to obtain personal information, such as national identity number, birthday, address, and credit card numbers, by disguising oneself as a well-known or trustworthy authority in the electronic form or physical form. Typically, hackers use emails, instant messages, texts, and social media to trick the users into clicking or entering a website that looks and feels like the genuine website they intend to browse; once the user clicks, they are asked to enter their personal information.

B. *Design of AR-based Phishing Application*

Below, we present how AR can make the concept of Phishing concrete and interactive. As depicted in Figure 2, two students are using the AR application remotely or in-person with their respective iPads. They need to discuss the messages on the table and decide whether to open the associated attachments or links based on their digital contents. If they make the wrong choice, the AR app will play an animation showing, for instance, the disappearance of apps, photos, or emails on the iPad to demonstrate the damage caused by the phishing attack. The detailed operations are described in Section III-D.

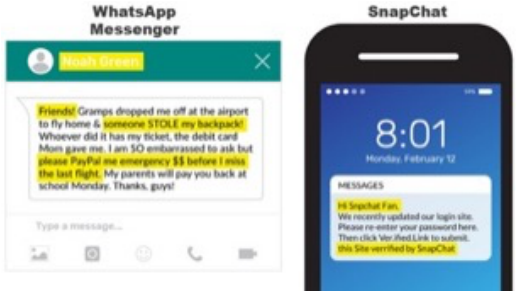

Figure 1. Phishing Examples in Instagram and WhatsApp

Figure 2. Example Phishing AR Activity

C. *Prototype*

To prototype the AR-based Phishing application, we have implemented the user interface (UI) and user experience (UX) with Adobe XD. As shown in Figure 4, the user needs to fill up some personal information to start the AR session. Before the AR session, we provided an AR session guide agent to help the user start the exploration and provide a better user experience (UX). Students can use their fingers to touch the screen to interact with the AR application to offer tangible interactions. Also, with iPads, students can walk around freely without being constrained by any connected cable.

To support the AR application over multiple platforms (such as Apple iOS, Google Android, and Microsoft HoloLens), we used the Unity game engine with AR Foundation framework and AR Foundation subsystem, ARKit Plugin, ARCore XR Plugin, and Windows XR Plugin. In addition, to facilitate the image detection feature for recognizing phishing questions on the table in Figure 5, we implement this feature with a 2D Image tracking API and create an image library to store for the API to detect the feature points. Also, we implement a GameManager object to track user's behavior and provide the corresponding feedback along with their AR experience.

D. *Operations of AR-based Phishing Application*

1. Open the AR-based phishing application with your partner (in-person or remotely).
2. Enter personal information for the experimental data collection purposes.

3. Start the AR session and follow the guideline with the UX agent for AR experience.
4. Scan different pictures on the table and figure out what is the digital content for that specific area (i.e., email and social media platforms).
5. Discuss the digital content with your partner and determine whether the content is phishing content or unharmed content.
6. When the final decision is made, use a finger to drag the content either into the trashcan to delete the digital content or over the mail scissors to open the digital content.
7. Repeat this process until every picture is scanned and solved the tasks.
8. The system will automatically show the result once all the tasks are finished.
9. On the result page, the system provided the details of each selected question with the explanation and related phishing examples and identified tips for the students to learn more about the phishing attacks.

Figure 3. Mixed Reality Anti-Phishing Program Start Page

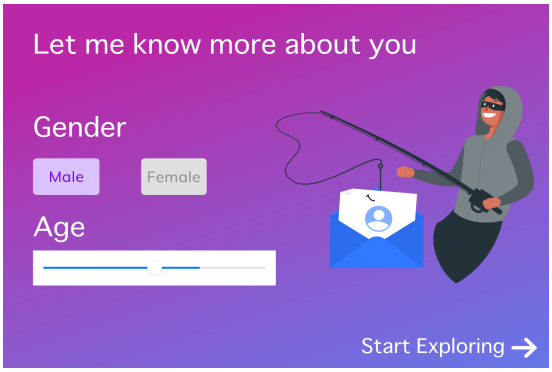

Figure 4. Mixed Reality Anti-Phishing Program Basic Information Page

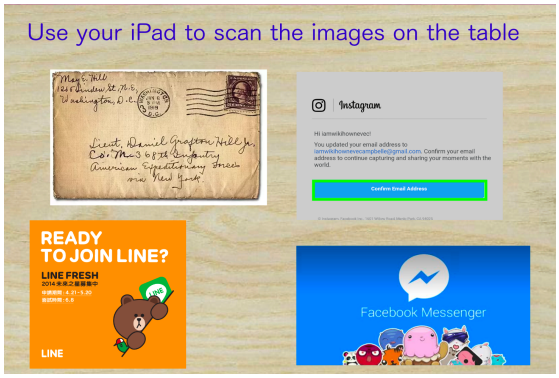

Figure 5. Mixed Reality Anti-Phishing Program Challenges Page

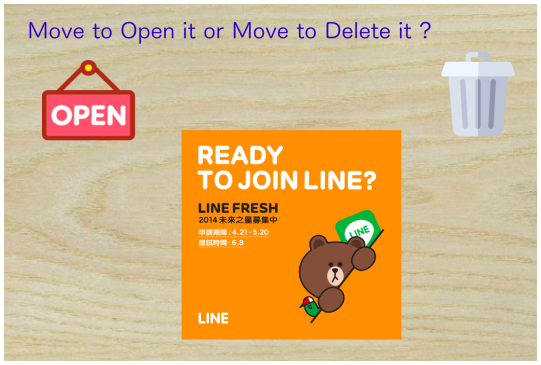

Figure 6. Mixed Reality Anti-Phishing Program Questionnaire Page

E. Design of Phishing Questions

To train the students to differentiate the phishing content as much as possible, we have collected and designed the phishing contents from popular social media platforms. Also, to support different world regions, we customized the questions based on the popularity of the local social media platforms from the iOS store's ranking. Taking Taiwan as an example, we used LINE (the most popular instant messaging in the country), Facebook, and Instagram to create the digital content for testing. We also prepared emails of different contexts for this training application, such as schools, banks and famous companies.

IV. Conclusion

In this paper, we proposed a Mixed Reality based education application for teaching about phishing from concept, design, prototype to implementation. With the AR technology, we can transform the abstract cybersecurity concepts into a tangible and highly interactive training application. We plan to conduct a pilot study to evaluate learning interest. In addition, we will collect the user's feedback for the initial design for cybersecurity education application in mixed reality to further improve other advanced cybersecurity topics.

Acknowledgment

This work is supported in part by National Science Foundation under grant NSF DRL-2048874.

REFERENCES

[1] Kim, J., Marotta, K., Leo, J. Agarwal, S., Li, S., & Chau, D.H. (2019). Mixed reality for learning programming. Proceedings of ACM IDC conference, June 2019, https://doi.org/10.475/123_4.

[2] Fotaris, P., Pellas, N., Kazanidis, I., & Smith, P. (2017). A systematic review of Augmented Reality game-based applications in primary education. In Proceedings of the 11th European Conference on Games Based Learning (ECGBL17). Graz, Austria (pp. 181-190).

[3] Seo, D.W., & Lee, J.Y. (2013). Direct hand touchable interactions in augmented reality environments for natural and intuitive user experiences. Expert Systems with Applications, 40(9), pp.3784-3793.

[4] Radu, I. (2016). Exploring the usability of augmented reality interaction techniques during children's early elementary-school tears (Doctoral dissertation, Georgia Institute of Technology).

[5] Bovill, C., Cook-Sather, A., & Felten, P. (2011). Students as co-creators of teaching approaches, course design, and curricula: implications for academic developers. International Journal for Academic Development 16,2, 133–145.

[6] Shelton, B.E., & Hedley, N.R.(2002). Using augmented reality for teaching earth-sun relationships to undergraduate geography students. In the First IEEE International Workshop Augmented Reality Toolkit. doi: 10.1109/ART.2002.1106948

[7] Itamiya, Tomoki. "VR/AR and Its Application to Disaster Risk Reduction." Emerging Technologies for Disaster Resilience. Springer, Singapore, 2021. 63-79.

[8] Lin, Pei-Hsuan, and Shih-Yeh Chen. "Design and evaluation of a deep learning recommendation based augmented reality system for teaching programming and computational thinking." IEEE Access 8 (2020): 45689-45699.

[9] Nicholson, James, et al. "Investigating teenagers' ability to detect phishing messages." 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE, 2020.

[10] Zargham, Nima, et al. "What could go wrong? raising mobile privacy and security awareness through a decision-making game." Extended Abstracts of the Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts. 2019.

[11] Wen, Z. A., Lin, Z., Chen, R., & Andersen, E. (2019). What.Hack: Engaging anti-phishing training through a role-playing phishing simulation game. Conference on Human Factors in Computing Systems - Proceedings, 1–12. https://doi.org/10.1145/3290605.3300338

[12] Van Der Stappen, A., Liu, Y., Xu, J., Yu, X., Li, J., & Van Der Spek, E. D. (2019). MathBuilder: A collaborative AR math game for elementary school students. CHI PLAY 2019 - Extended Abstracts of the Annual Symposium on Computer-Human Interaction in Play, 731–738. https://doi.org/10.1145/3341215.335629

[13] "The Top 6 Industries for Enterprise AR/VR in 2021." XR Today, 18 Dec. 2020, Accessed: www.xrtoday.com/mixed-reality/the-top-6-industries-for-enterprise-ar-vr-in-2021/

[14] Morgan, H. (2020). Best practices for implementing remote learning during a pandemic. The Clearing House: A Journal of Educational Strategies, Issues and Ideas, 93(3), 135-141.

[15] "Virtual Reality Is Booming in the Workplace amid the Pandemic. Here's Why." CNBC, 4 July 2020, Accessed: www.cnbc.com/2020/07/04/virtual-reality-usage-booms-in-the-workplace-amid-the-pandemic.html.

[16] "Phishing." Wikipedia, Wikimedia Foundation, 16 Aug. 2021, en.wikipedia.org/wiki/Phishing.

[17] Siddiqui, Zeeshan, and Nida Zeeshan. "A Survey on Cybersecurity Challenges and Awareness for Children of all Ages." 2020 International Conference on Computing, Electronics & Communications Engineering (iCCECE). IEEE, 2020

[18] "Augmented Reality." Wikipedia, Wikimedia Foundation, 7 Aug. 2021, en.wikipedia.org/wiki/Augmented_reality.

[19] Belcic, Ivan. The Essential Guide to Phishing: How It Works and How to Defend against It, Avast, 14 May 2021, www.avast.com/c-phishing.