National College of Ireland

Configuration Manual

MSc Research Project
MSc Cybersecurity

Efoseh Iliya Fachano
x22198911

School of Computing
National College of Ireland

Supervisor: Dr. Vanessa Ayala-Rivera

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: ……. Efoseh Iliya Fachano……

Student ID: ……x22198911……..……

Programme: …MSc Cybersecurity…… **Year:** ……2024……..

Module: ……Msc Research project……..……

Lecturer: ……Dr. Vanessa Ayala-Rivera……..……

Submission Due Date: ……31/01/2024……..……

Project Title: Gamification in Cybersecurity: Improving Employee Compliance through Game-Based Learning and Incentives.

Word Count: ……1168…… **Page Count:** ……11……..……..……

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: ……Efoseh Iliya Fachano……

Date: ……31/01/2024……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Efoseh Iliya Fachano
x22198911

1 Introduction

This document highlights the configuration of the research project titled Gamification in Cybersecurity: Improving Employee Compliance through Game-Based Learning and Incentives. It aims to answer the research question, *how does incorporating gamification elements and incentives improve employee adherence to cybersecurity protocols?*

To implement this project you create two groups, the control and experimental group. The control group has no gaming elements while the experimental group has gaming elements. They both take a quiz at the end of the experiment then analysis on which group performed better in the quiz is carried out by assessing the overall score of the groups' performance.

2 Questionnaire

Each group fills out a participation form to collect some background data on the participants prior knowledge on OWASP Top 10, experience in the cybersecurity field and few other questions. The links to the participation forms are below.

Control group link: https://forms.office.com/e/sHhUU2q2z3

Experimental group link: https://forms.office.com/e/Vs59822Jai

After filling the form click **Submit.**

There is a link to the slide presentation on OWASP Top 10 for the control group.

Figure 1: Slide Presentation for Control Group

After completing the form for the experimental group there is a link to the Scratch game.

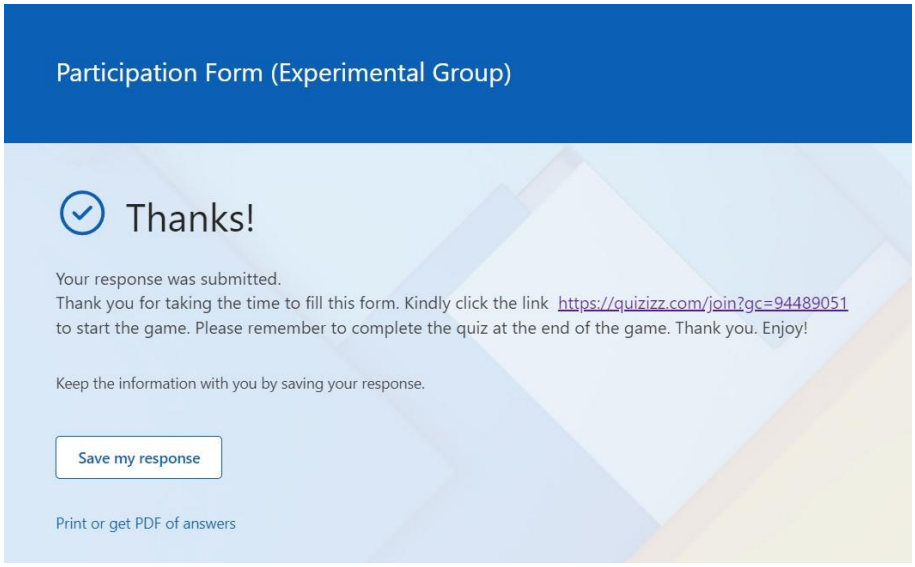

Figure 2: Prompt to start the game after filling the form.

3 Gamification

In simple terms gamification is the process of adding gaming elements into non-gaming areas. The platform used to create a game to learn more about OWASP Top 10 is Scratch platform.

The link to the Scratch game https://scratch.mit.edu/projects/935146687

If you download the Scratch file to your computer, it can be uploaded by clicking https://scratch.mit.edu

Click **Create** then go to **File** and click **Load from your computer.**
Select the .sb3 Scratch file on your computer and click **Ok.**
The first screen you will see is below.
Click the **green flag** to start the game. Then click the **Start** button below the topic.

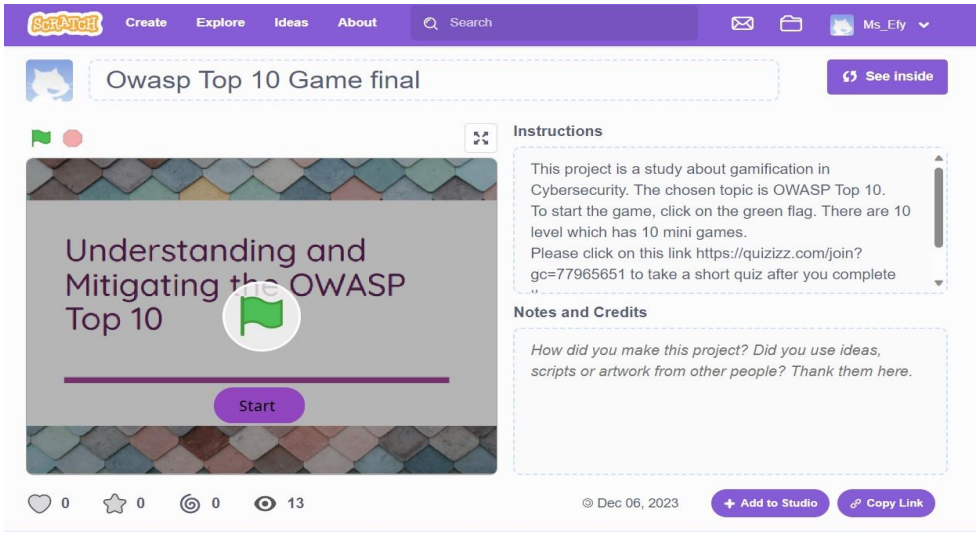

Figure 3: OWASP Top 10 Game

After that, click **Learn more.**

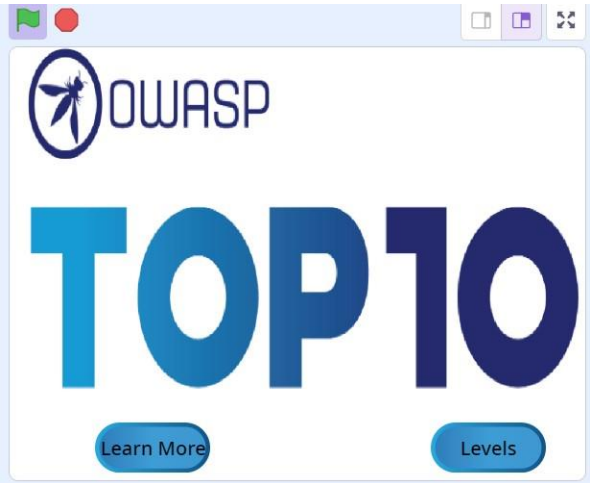

Figure 4: Start Screen

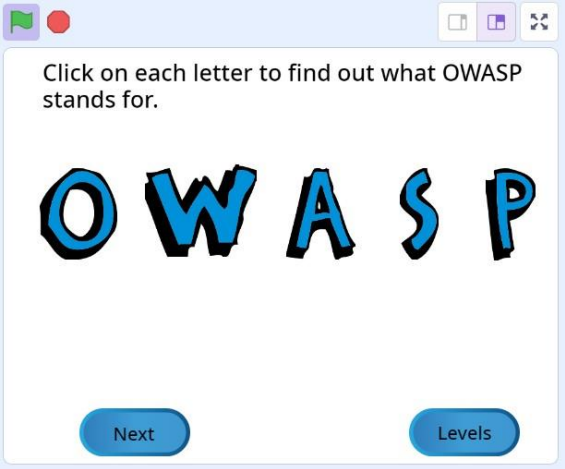

Figure 5: Learn More Screen

When you click **Levels**, you should see all the levels of the game.
Start with the first level **A01-2021: Broken Access Control.**

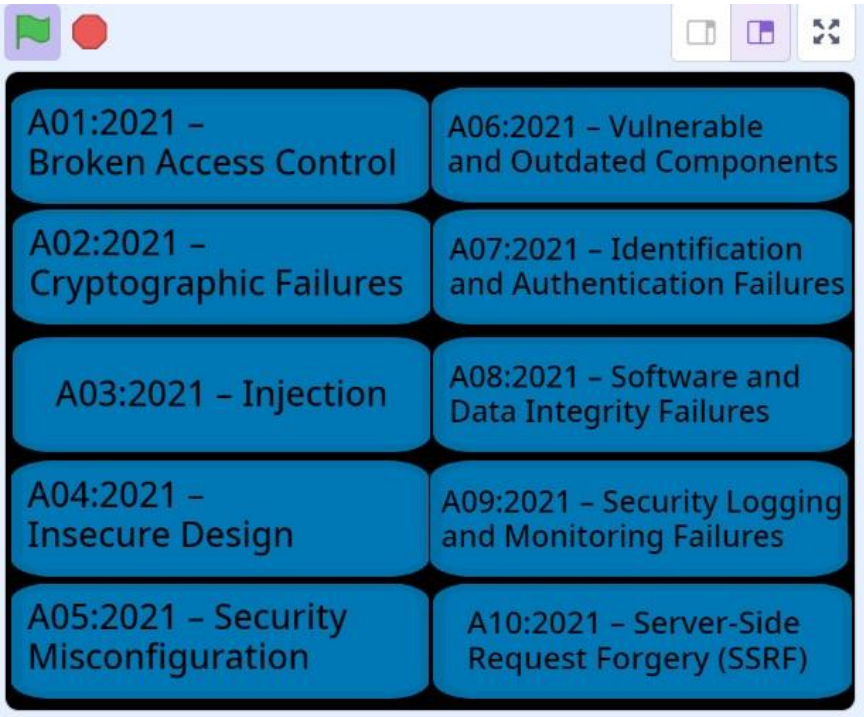

Figure 6: Levels Screen

After reading the instructions on how to play the game click **Start game.**

Figure 7: Level 1 game screen

Move your arrow keys and attempt to touch the silver door to gain access.

When you touch the door twice you will get 2 points and you will be taken to the command centre where you gained access to.

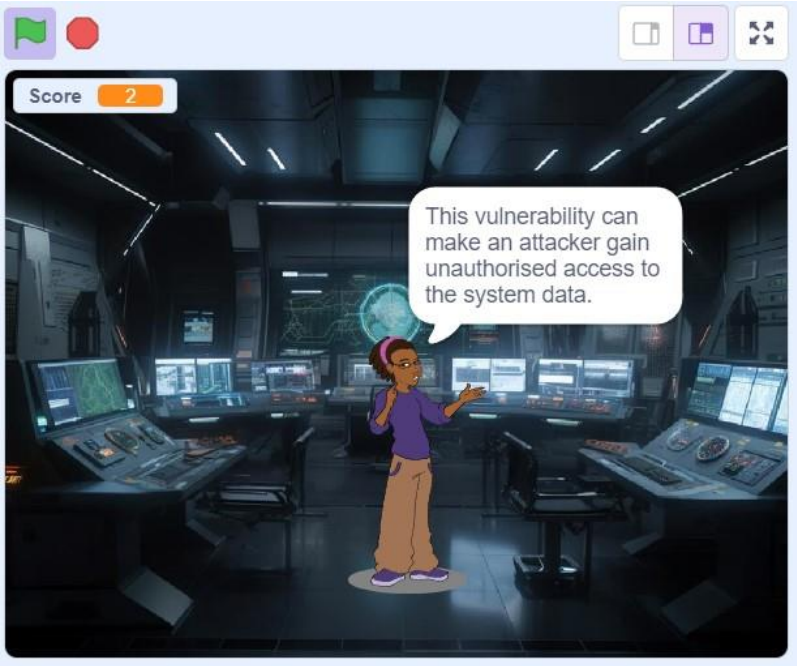

Figure 8: Command centre Screen

You will then be taken to the next level, A02-2021: Cryptographic Failures.
Click **Start game.**

Figure 9: Start screen for Level 2

To view the code blocks in Scratch click **see inside** on the top right hand corner.

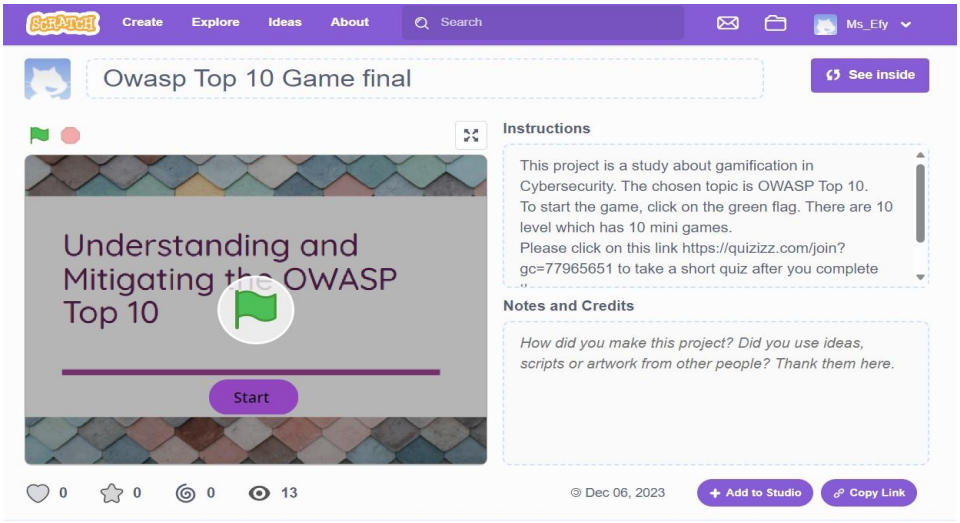

Figure 10: See Inside Screen

Then you will get a screen like the one below. The code blocks are on the left hand side and can easily be dragged and dropped in the white space in the middle which is the script area.

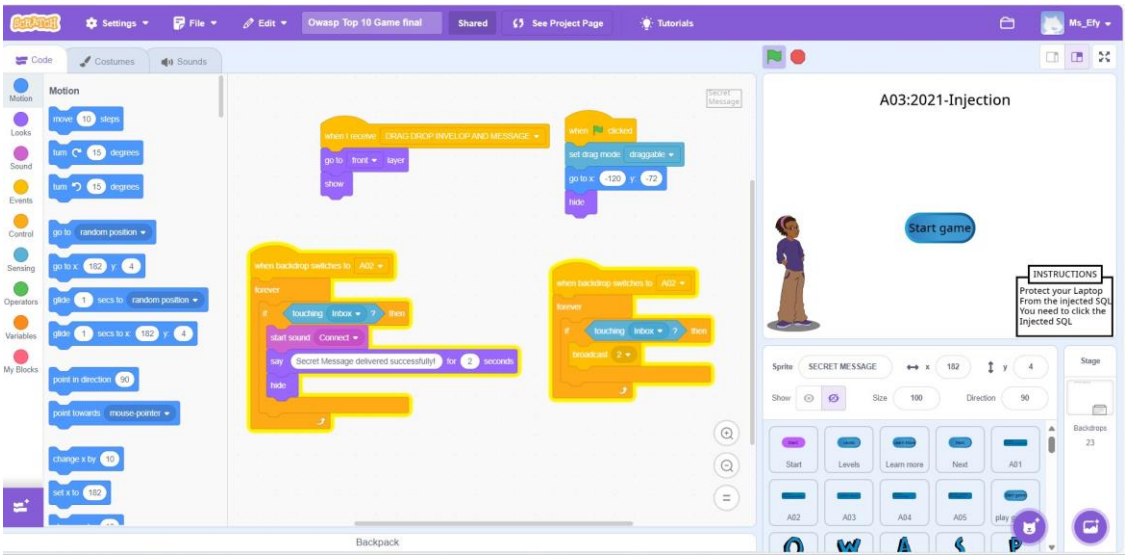

Figure 11: Scratch Platform

The sprite (characters) each have code in them to carry out instructions. This code below is for Avery Walking sprite.

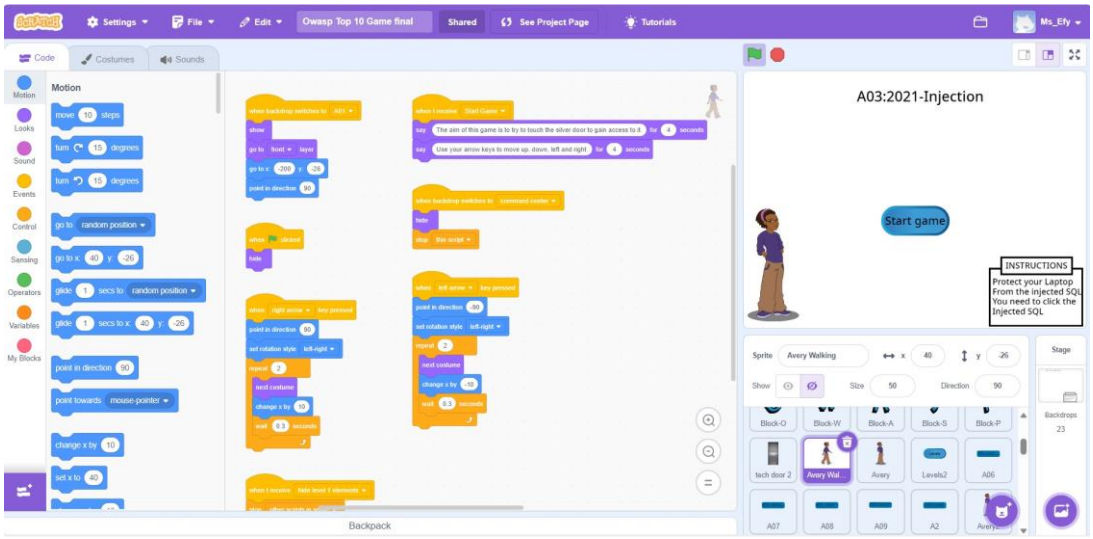

Figure 12: Code blocks for the Sprite called Avery walking

4 Final Quiz

After the game and the slide presentation there is a quiz for both groups. **Please note that the link for the quiz may display invalid game code as both quizzes are closed after 2 weeks (a default setting by the Quizziz platform) therefore it may have expired by the time you click the link to the quiz.**

The questions in both quizzes are the same, however, for the purpose of analysis participants are given separate links.

Link to Quiz for control group https://quizizz.com/join?gc=84285375

Link to Quiz for experimental group https://quizizz.com/join?gc=78830752

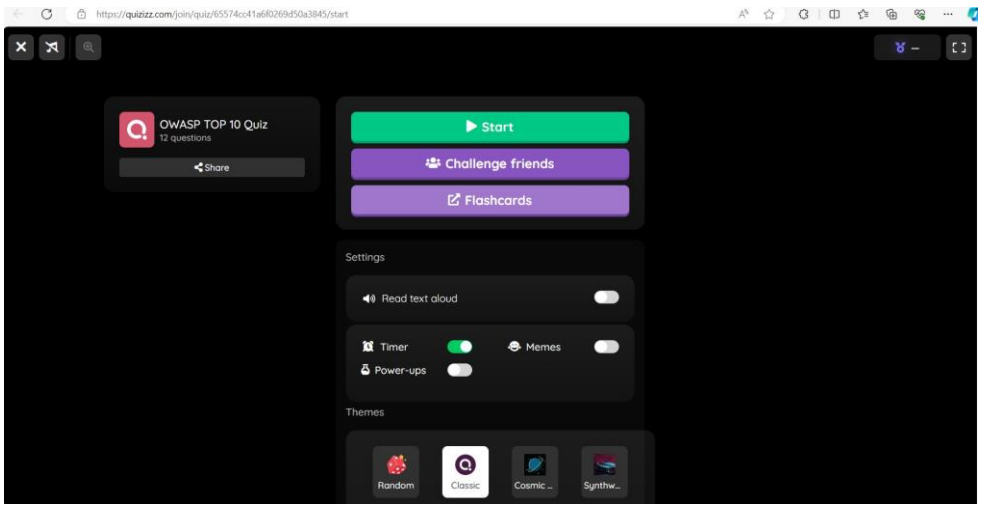

Figure 13: Start Screen for the quiz

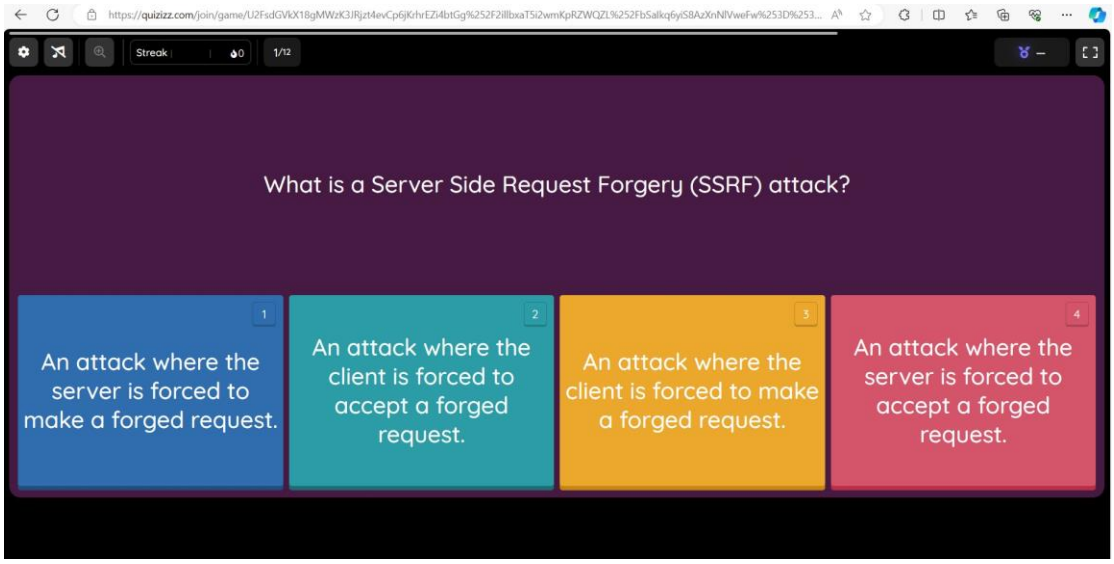

Figure 14: Quiz question

5 Conclusion

This research can be reproduced using the steps highlighted above. The research aims to explore gamification and how it can enhance and improve compliance amongst employees and participants of the experiment. Based on the results from the quiz there was a 6% difference in performance between the control group and experimental group. The experimental group with the gaming elements performed better than the control group, which had only the slide presentation. This suggests that gamification can improve or enhance compliance.

References

Berisford, C. J., Blackburn, L., Ollett, J. M., Tonner, T. B., Yuen, C. S. H., Walton, R., & Olayinka, O. (2022) 'Can gamification help to teach Cybersecurity?', in *2022 20th International Conference on Information Technology Based Higher Education and Training (ITHET)*, Antalya, Turkey, 2022, pp. 1-9, doi: 10.1109/ITHET56107.2022.10031716.

Davis, N., & Grant, E. S. (2022) 'Simulated Phishing Training Exercises versus Gamified Phishing Education Games', in *2022 Fourth International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT)*, Mandya, India, 2022, pp. 1-8, doi: 10.1109/ICERECT56837.2022.10060595.

Hill, W. A., Fanuel, M., Yuan, X., Zhang, J., & Sajad, S. (2020) '*A Survey of Serious Games for Cybersecurity Education and Training*', in KSU Proceedings on Cybersecurity Education, Research and Practice. 7.

Oroszi, E. D. (2020) '*Using Gamification to Improve the Security Awareness of Users: The Security Awareness Escape Room*', *ISACA Journal*, vol. 4, pp. 1-6.

Van Steen, T., & Deeleman, J. R. A. (2021) 'Successful Gamification of Cybersecurity Training', *Cyberpsychology, Behavior, and Social Networking*, *24*(9), pp. 593–598 doi: 10.1089/cyber.2020.0526.