

Enhancing Adults' Understanding of Security Concepts through a Cybersecurity Game

Combined Participant Information Sheet and Consent Form for Anonymous Online Surveys for Adult Participants

Study Title: Enhancing Adults' Understanding of Security Concepts through a Cybersecurity Game

Researcher(s): William Mayhew

University email: wm4g21@soton.ac.uk

Ethics/ERGO no: 92262

Version and date: Version 1, 25/03/2024

What is the research about?

My name is William Mayhew and I am a Bachelors of Science in Computer Science at the University of Southampton in the United Kingdom.

I am inviting you to participate in a study regarding how effective a cybersecurity game is at teaching cybersecurity concepts. The aim of the study is to understand who is likely to be most affected by the game.

This study was approved by the Faculty Research Ethics Committee (FREC) at the University of Southampton (Ethics/ERGO Number: 92262).

What will happen to me if I take part?

This study involves completing an anonymous questionnaire which should take approximately 15-30 minutes of your time. Participants are permitted to complete the questionnaire across multiple sittings, but it is recommended to complete the game and the final questionnaire in one sitting. If you are happy to complete this survey, you will need to tick (check) the box below to show your consent. As this survey is anonymous, the researcher will not be able to know whether you have participated, or what answers you provided.

Why have I been asked to participate?

There are no inclusion/exclusion criteria for participants themselves, but they must be able to run the Unity application.

I am aiming to recruit as many participants for this study as possible.

What information will be collected?

The questions in this survey ask for information in relation to age range, technical background, current cybersecurity knowledge of basic principles, and effectiveness of the game.

Some of the survey questions contain textboxes where you will be asked to type in your own

answers. Please note that in order for this survey to be anonymous, you should not include in your answers any information from which you, or other people, could be identified.

You do not have to answer the questions in textboxes if you do not wish to do so.

What are the possible benefits of taking part?

If you decide to take part in this study, you will not receive any direct benefits; however, your participation will contribute to knowledge in this area of research.

Are there any risks involved?

It is expected that taking part in this study will not cause you any psychological discomfort and/or distress, however, should you feel uncomfortable you can leave the survey at any time.

What will happen to the information collected?

All information collected for this study will be stored securely on a password protected computer and backed up on a secure server. In addition, all data will be pooled and only compiled into data summaries or summary reports. Only the researcher and their supervisor will have access to this information.

The information collected will be analysed and written up as part of the researcher's dissertation.

The University of Southampton conducts research to the highest standards of ethics and research integrity. In accordance with our Data Management Policy, data will be securely destroyed after conferment of the researcher's degree in Summer 2024.

What happens if there is a problem?

If you have any concern or complaint, contact William Mayhew (wm4g21@soton.ac.uk) or Dr Nawfal Al Hashimy (nawfal@soton.ac.uk)

Otherwise, If you are unhappy about any aspect of this study and would like to make a formal complaint, you can contact the Head of Research Integrity and Governance, University of Southampton, on the following contact details: Email: rgoinfo@soton.ac.uk, phone: + 44 2380 595058.

Please quote the Ethics/ERGO number above. Please note that by making a complaint you might be no longer anonymous.

More information on your rights as a study participant is available via this link:

<https://www.southampton.ac.uk/about/governance/participant-information.page>

Thank you for reading this information sheet and considering taking part in this research.

* Indicates required question

1. Please tick (check) this box to indicate that you have read and understood information on ^{*} this form, are aged 18 or over and agree to take part in this survey.

Tick all that apply.

☐ I understand and agree to participate

Skip to question 2

Pre-Game Questions

These questions should be answered before playing the game.

2. What is your age range? ^{*}

Mark only one oval.

☐ 18-25

☐ 26-35

☐ 36-45

☐ 46-55

☐ Over 55

3. How familiar are you with using technology? ^{*}

Mark only one oval.

☐ Not at all familiar

☐ Moderately familiar

☐ Very familiar

4. How familiar are you with cybersecurity concepts? ^{*}

Mark only one oval.

☐ Not at all familiar

☐ Moderately familiar

☐ Very familiar

Rate your understanding of the following cybersecurity concepts:

Phishing: Deceptive attempts to obtain sensitive information, such as passwords or financial details, by posing as a trustworthy entity in electronic communication.

Romance and Friendship scams: Scams that exploit emotional connections to deceive individuals into sending money or sensitive information to someone they believe they have a romantic or friendly relationship with.

Password Security: Knowledge and practices related to creating strong, unique passwords.

Cyber Policies: Policies and procedures established by organizations to mitigate cyber risks, protect sensitive information, and ensure compliance with relevant laws and regulations.

Scareware: Malicious software that tricks users into believing their computer is infected with malware or other security threats, often prompting them to purchase unnecessary or fake security solutions.

5. Phishing *

Mark only one oval.

- ☐ No understanding
- ☐ Limited understanding
- ☐ Moderate understanding
- ☐ Good understanding
- ☐ Expert understanding

6. Romance and Friendship Scams *

Mark only one oval.

- ☐ No understanding
- ☐ Limited understanding
- ☐ Moderate understanding
- ☐ Good understanding
- ☐ Expert understanding

7. Password Security *

Mark only one oval.

- ☐ No understanding
- ☐ Limited understanding
- ☐ Moderate understanding
- ☐ Good understanding
- ☐ Expert understanding

8. Cyber Policies *

Mark only one oval.

- ☐ No understanding
- ☐ Limited understanding
- ☐ Moderate understanding
- ☐ Good understanding
- ☐ Expert understanding

9. Scareware *

Mark only one oval.

- ☐ No understanding
- ☐ Limited understanding
- ☐ Moderate understanding
- ☐ Good understanding
- ☐ Expert understanding

Play the Game

Please click the link below to access the game. Depending on your level of knowledge, it may take anywhere from a 5 minutes to over 10 minutes to complete.

<https://willmayhew.itch.io/cyber-fraud-educational-game>

Post-Game Questions

These questions should be answered after playing the game.

10. How effective do you think the game was at teaching cybersecurity concepts? *

Mark only one oval.

- ☐ Not effective at all
- ☐ Slightly effective
- ☐ Moderately effective
- ☐ Very effective
- ☐ Extremely effective

11. How effective do you think the game was at reinforcing cybersecurity concepts? *

Mark only one oval.

- ☐ Not effective at all
- ☐ Slightly effective
- ☐ Moderately effective
- ☐ Very effective
- ☐ Extremely effective

Rate your understanding of the following cybersecurity concepts after playing the game:

Phishing: Deceptive attempts to obtain sensitive information, such as passwords or financial details, by posing as a trustworthy entity in electronic communication.

Romance and Friendship scams: Scams that exploit emotional connections to deceive individuals into sending money or sensitive information to someone they believe they have a romantic or friendly relationship with.

Password Security: Knowledge and practices related to creating strong, unique passwords.

Cyber Policies: Policies and procedures established by organizations to mitigate cyber risks, protect sensitive information, and ensure compliance with relevant laws and regulations.

Scareware: Malicious software that tricks users into believing their computer is infected with malware or other security threats, often prompting them to purchase unnecessary or fake security solutions.

12. Phishing *

Mark only one oval.

- ☐ No understanding
- ☐ Limited understanding
- ☐ Moderate understanding
- ☐ Good understanding
- ☐ Expert understanding

13. Romance and Friendship Scams *

Mark only one oval.

- ☐ No understanding
- ☐ Limited understanding
- ☐ Moderate understanding
- ☐ Good understanding
- ☐ Expert understanding

14. Password Security *

Mark only one oval.

- ☐ No understanding
- ☐ Limited understanding
- ☐ Moderate understanding
- ☐ Good understanding
- ☐ Expert understanding

15. Cyber Policies *

Mark only one oval.

- ☐ No understanding
- ☐ Limited understanding
- ☐ Moderate understanding
- ☐ Good understanding
- ☐ Expert understanding

16. Scareware *

Mark only one oval.

- ☐ No understanding
- ☐ Limited understanding
- ☐ Moderate understanding
- ☐ Good understanding
- ☐ Expert understanding

Challenge Improvements

If you can, please provide some improvements which could be made to the challenges.

17. What could be improved for the Phishing challenge? (2nd Room, Accepting/Rejecting Letters)

18. What could be improved for the Romance and Friendship Scam challenge? (3rd Room, NPC Conversations)

19. What could be improved for the Password Workshop challenge? (3.5 Room, Creating a strong password)

20. What could be improved for the Password Identification challenge? (3.5 Room, Identifying a strong password)

21. What could be improved for the Cyber Policies challenge? (4th Room, during the boss battle)

22. What could be improved for the Scareware challenge? (Pop-ups occurring during gameplay)

Confidence, Engagement and Enjoyment

23. On a scale from 'Learning' to 'Reinforcing,' where 'Learning' indicates primarily acquiring new knowledge or skills, and 'Reinforcing' indicates primarily strengthening existing knowledge or skills, how would you objectively characterize the game? *

Mark only one oval.

1 2 3 4 5

Lear ☐ ☐ ☐ ☐ ☐ Reinforcing

24. How confident do you feel in applying the cybersecurity concepts shown in the game to real-life situations? *

Mark only one oval.

- ☐ Not confident at all
- ☐ Slightly confident
- ☐ Moderately confident
- ☐ Very confident
- ☐ Extremely confident

25. Did you find the game engaging? *

Mark only one oval.

- ☐ Not engaging at all
- ☐ Slightly engaging
- ☐ Moderately engaging
- ☐ Very engaging
- ☐ Extremely engaging

26. What would you rate the overall enjoyment of playing the game? *

Mark only one oval.

- ☐ Not enjoyable at all
- ☐ Slightly enjoyable
- ☐ Moderately engaging
- ☐ Very engaging
- ☐ Extremely engaging

27. Are there any improvements that could be made to the game to enhance overall confidence in applying cybersecurity concepts, increase engagement, or improve enjoyment?

Other

28. Was the game responsive? Specifically, was functionality maintained throughout gameplay without issue.

Mark only one oval.

☐ Yes

☐ No

29. Did the game stutter at all? *

Mark only one oval.

☐ Yes

☐ No

30. Was the interface intuitive? *

Mark only one oval.

☐ Yes

☐ No

31. Was the interface user-friendly? *

Mark only one oval.

☐ Yes

☐ No

32. Did you encounter any issues running the game?

End of Questionnaire

Thank you for taking part.

This content is neither created nor endorsed by Google.

Google Forms