The Need for Game-Based Learning Methods to Address Cyber Threats

George Andrews, Chitra Balakrishna and Alexander Mikroyannidis
The Open University, Milton Keynes, UK

George.andrews@open.ac.uk
Chitra.balakrishna@open.ac.uk
Alexander.mikroyannidis@open.ac.uk

Abstract: Cyber security threats are increasingly a serious concern to organisations, with an annual worldwide cost of a trillion dollars in 2021. Potentially the most significant contributor to cyber security threats is the human element, yet this has typically been insufficiently addressed in proposed solutions. Significant resources have been allocated to software, training and other solutions designed to tackle this threat, yet existing methods to improve cyber security have failed to deliver the desired results. Commonly cited issues include the lack of engagement in training, leading to disinterest and a 'one size fits all' approach, meaning some groups benefit from training more than others. This study will examine the need for game-based training methods in addressing cyber security threats caused by human error. Game-based training methods have previously been proposed to improve engagement in training and this study will discuss other potential benefits of game-based training. The aim of this work is to justify the use of game-based training methods in cyber security and begin to determine which aspects of games may be most effective at causing long-term positive behaviour change. Following an extensive literature review, a pilot study was run in which a survey was presented to 37 individuals who have taken cyber security training in the past, to query opinions and perceptions regarding cyber security training participants had previously taken, and how they feel they would behave when faced with certain cyber security threats. Upon analysis in SPSS, the results of this work indicate that factors such as training frequency and exposure to cyber security attacks have a significant impact on cyber security behaviour. A correlation between engaging training and impact of training on behaviour also serves to justify the development of such training methods. When combined with previous results on cyber security training this highlights the need for training to be engaging, regular, and relevant, and shows that the realistic simulation of cyber security threats (such as in game-based training) is of significant benefit. These results will help inform future development of effective game-based training methods and encourage their use more widely.

Keywords: Game-based learning, Workplace, Non-Expert, Cyber behaviour

1. Introduction

Online digital systems have become a fundamental component of society today. A significant proportion of the population has some form of online presence (Johnson, 2021) with many individuals doing their shopping, banking, and socialising online. This is not limited to individuals, as Abawajy (2014) notes that many organisations are becoming increasingly dependent on such digital technologies. While these systems offer convenience and efficiency, they are not without downsides. A report from PwC (2013) along with a recent report from Accenture (2021) show a consistent increase in the average number of cyber breaches faced by organisations each year.

It has been suggested that humans and human error is the weakest link in the cyber security chain (Zwilling *et al*., 2022; Cain, Edwards & Still, 2018). Streeter (2013) suggested that over 35% of breaches are due to human error, with a more recent Kaspersky (2017) analysis finding at least 27% of breaches due to careless employees, loss of hardware, or social engineering.

Lack of engagement is a significant issue reported with existing security training programs (Furnell, Bryant & Phippen, 2007; Reeves, Calic & Delfabbro, 2021). Haney & Lutters (2018) describe a perception of cyber security as boring and dull to many individuals, discouraging engagement. It would, therefore, be beneficial to increase the engagement of security training programs. Games – particularly video games – are well known for being engaging (Laffan *et al*., 2016). There is evidence that game-based learning is effective at causing behaviour change (Hamari, 2016), which existing cyber security training has been, however game-based cyber security training is not yet widespread.

This study will aim to work towards a method of cyber security training which addresses lack of engagement, through the use of game-based methods.

2. Literature Review

2.1 The Effectiveness of Current Cyber Security Training

It has been frequently stated that existing cyber security awareness methods are insufficient (Bada, Sasse & Nurse, 2019). The distribution of both paper-based and electronic resources can be considered among the most basic form of training. While it is possible for conventional delivery methods to reach a wide range of individuals, the actual impact is difficult to measure. Kumaraguru *et al.* (2007) look at responses to such delivery methods, finding security notices ineffective at improving perceived awareness. Similarly, Bada, Sasse & Nurse (2019) describes the materials themselves as often not being engaging, which can lead to the training being unsuccessful, potentially due to trainees getting bored and losing focus (Reeves, Calic & Delfabbro, 2021).

Instructor-led training methods are commonly used and involve the use of an expert to deliver the relevant information from the top down are also common. Haney & Lutters (2018) discuss the variance in delivery by instructors, noting that audiences can be lost by poor presentations, even when the information and material are valuable. Despite being generally more effective than conventional delivery methods in improving cyber security behaviour, they are more resource-intensive to implement, and still rely on the ability of the instructor.

Individuals not engaging with cyber security training has been identified as a significant issue with existing cyber security training methods (Reeves, Calic & Delfabbro, 2021; Bada, Sasse & Nurse 2019). As a result, existing cyber security training methods have generally been found to have been ineffective, at least in part leading to an increase in the security incidents.

2.2 Games for Cyber Security Training

Games, and in particular video games, are known for being engaging activities. Hamari *et al*. (2016) find a positive correlation between the challenge within game-based learning and the engagement of participants, which further correlates to perceived learning.

Game based training is a proposed alternative to more traditional forms of cyber security awareness training (conventional, instructor-led and others). A notable advantage of game-based cyber security training is the engagement factor of video games, which can also contribute to increased motivation (Zhang-Kennedy & Chiasson, 2022).

The concept of *flow* is very important in the study of engagement. Flow refers to a state of intense focus to the point of loss of awareness, brought about by a balance between challenge of an activity and skill level (Nakamura & Csikszentmihalyi, 2002). Kiili (2005) suggests that flow has a positive impact on learning, indicating that a training method involving flow would help increase engagement with training materials, which has previously been cited (Reeves, Calic & Delfabbro, 2021) as being beneficial to learning. Challenge is a significant factor in the induction of flow, as Jin (2012) determines that challenge contributes towards flow, but only when the challenge is matched to skill level. Sherry (2004) goes on to describe a gradual but continuous increase in difficulty as most effective in inducing flow. The impact of the difficulty of training will therefore be a worthwhile inclusion in training studies.

Game-based methods do not necessarily solve all issues facing cyber security training but where appropriately challenging and engaging, game-based training methods can take advantage of flow to improve the positive impact of cyber security training programs.

2.3 Effectiveness of Existing Game-Based Training Methods

Some game-based cyber security training has been developed and investigated previously. Zhang-Kennedy & Chiasson (2022) and Hendrix, Al-Sherbaz & Bloom (2016) reviewed multiple game-based tools for cyber security training finding that only a small proportion of investigated tools (fewer than one-third) had been properly evaluated, and even fewer in their long-term impact. Where they have been evaluated, outcomes were typically positive – demonstrating some positive impact on cyber security awareness/behaviour, at least immediately following the training. Only six of the reviewed games directly matched the demographic of this study, but these studies found generally positive results as well.

One of the most well-known tools reviewed is Anti-Phishing Phil (Sheng, S. *et al.*, 2007), a game in which players (aimed at non-expert players) must distinguish between real and fake URLs, represented by worms. Despite this game being referred to often, and several studies into its effectiveness, there is no investigation of how this game impacts knowledge and behaviour of participants over a period longer than two weeks.

The long-term impact of game-based methods has not often been investigated, and even in studies such as Egelman *et al.* (2016) in which a long-term impact is assessed, the population studied is limited (in this case to university undergraduates). A part of determining whether game-based methods are useful in awareness and behaviour modification is the assessment of cyber security awareness/behaviour. To achieve this, a long-term assessment of behaviour change would be very useful.

3. Methodology

The research this study aims to work towards involves taking advantage of the challenge and engagement of game-based methods in order to change the behaviour of adult users with limited digital knowledge (non-expert). To approach this problem, this study aims to discover what behaviours end users currently have, and how they are impacted by cyber security training they have taken in the past.

Part of the survey also aims to investigate how users perceive cyber security training, to determine which aspects are most in need of improvement and whether game-based training would likely be effective. The target group of this study is adults in the age range 24-64 with limited knowledge of cyber security, who have taken part in some form of cyber security training. N = 37 participants responded to requests for participants, which were shared in university and affiliated groups. All participants who responded before the deadline were included in the data analysis. N = 36 participants were within the desired age range of 24-64 and were mostly known to have taken part in similar cyber security training programs (At least N = 35 participants have taken part in training, at least N = 31 through their job).

3.1 Survey Design

This survey contains 18 questions, some of which were adapted from a previous study – GICAST (n.d.), but were mostly written specifically for this study. The questions aim to primarily assess the users' perceptions of cyber security training - both their perceptions of the effectiveness of training, and how they perceive their experiences of it. The questions analysed use a Likert scale, typically from 1 to 5 (strongly disagree to strongly agree).

The first set of questions aims to address the current cyber security behaviour of end users, as current cyber security behaviour is considered to be insufficient to combat the growing impact of cyber threats (Zwilling *et al*., 2022; Cain, Edwards & Still, 2018). The questions focus on actions participants may or may not take, that are typically considered either good or bad practice. This will overlap with how users believe they should behave in cyber contexts, as participants may not be aware of how they can best protect themselves.

Most of the remaining questions focus on attitudes towards existing cyber security training. Works such as Bada, Sasse & Nurse (2019) suggest that current cyber security training has failed to cause the desired level of behavioural change, and one of the aims of this survey is to discover whether participants feel that their behaviour has been changed by cyber security training, and if so, why they feel this is the case.

Once developed the survey was internally distributed via an online link. The responses were collected over 12 weeks, and then analysed quantitively and qualitatively.

3.2 Interview Design

Five participants then took part in focused interviews, with 15-20 more detailed questions based on their survey responses, such as how they feel cyber security training has impacted their day-to-day lives.

These interviews aim to improve the detail of information gathered throughout the initial surveys and allow questions that have not been addressed through the surveys to be asked.

Data from these interviews is used to contextualise results from the surveys and offer some additional insights.

4. Results and Analysis

In total, the end user survey had N = 37 responses before the response deadline. Of these N = 23 were aged 24-44, N = 1 aged under 24 and N = 13 aged 45-64. N = 14 were female, N = 1 non-binary, N = 21 male and N = 1 declined to say. From these results, several measures were constructed. All analysis, unless stated otherwise was carried out in SPSS version 28, using similar methods to that of Hong & Furnell (2021) in which the impact of various factors on behaviour were analysed.

First, relevant factors were isolated (such as engagement), then correlations will be run between each of these (where appropriate) and significant correlations were recorded. Finally, a linear regression was run on the most important dependent variables, iteratively eliminating independent variables to find the strongest model.

A behaviour score was calculated for each participant, based on their responses to each of the Likert-style questions which refer to their cyber security behaviour (such as whether they use anti-virus software, or use strong passwords) and whether they have changed their behaviour in response to cyber security incidents (such as whether they are more cautious, or sought additional training). Each of these answers were normalised (to have a score between 0 and 1), reversed if necessary (where the question indicated a negative behaviour), ignored if no response was given and then averaged across all included responses with equal weighting. A total of 16 variables were used in this calculation. The final behaviour score for each participant is a number between 0 and 1, the lowest of which was 0.51667, and the highest was 1.

4.1 What is the Current Cyber Security Behaviour of end Users?

Past work has claimed that cyber security behaviour among the general population is poor (Kaspersky, 2017). Using the cyber security behaviour metric, the mean cyber security behaviour score returned was 0.79, which roughly corresponds to participants *usually* taking the more secure action in their day-to-day lives when faced with cyber security situations, and *usually* responding in a secure way to incidents.

The most significant independent variables that are being measured come from the following questions:

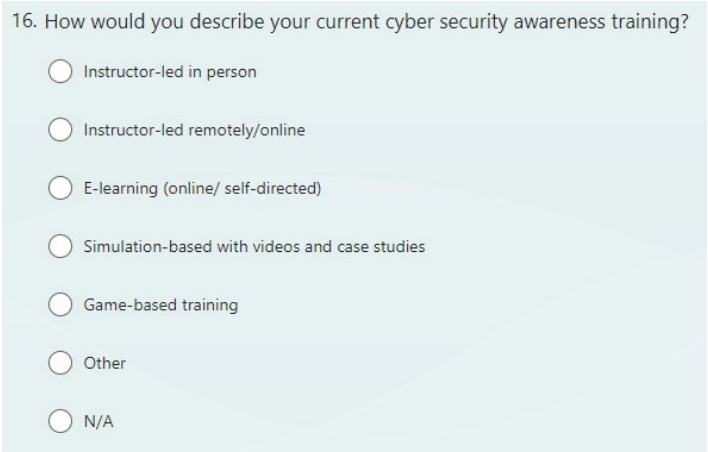

Figure 1: Question 16 – the basis for 3 of the independent variables tested against the likelihood of participants feeling their behaviour had changed (game-based and instructor-led in person were not selected by any participants)

Figure 2: Question 17 – the Basis for 5 of the independent variables tested against both dependent variables

- Training Frequency is an estimate of how often participants are required to take part in training. (Q15)

- Cyber_Attack_Exposure is the number of types of cyber security threat participants report having encountered. (Q8)
- Personal_Responsibility_Level is the number of external entities participants felt were responsible for their online security. (Q10)
- Gameplay_Frequency is an estimate of how often participants reported playing games. (Q6)

Table 1: Correlation between training factors and cyber security behaviour

Predictor	Correlation	Lower C.I	Upper C.I
Training_Frequency	0.400	0.082	0.644
Relevance	0.508	0.199	0.725
Enjoyment	0.303	-0.045	0.585
Engagement	0.196	-0.158	0.505
Cyber_Attack_Exposure	0.420	0.111	0.655

There was significant positive correlation between all considered factors and the behaviour score of participants (Training frequency, enjoyment, engagement, relevance, and previous exposure to cyber threats) as shown in the table above. For enjoyment and engagement, the confidence interval including zero would typically result in any hypothesis being rejected ($p > 0.05$). Nevertheless, given the nature of this study, it is not necessary to discount these results entirely.

Table 2: Partial results of linear regression on cyber security behaviour

Variable	Initial Model		Strongest Model		Final Model	
	Standardised B	*p*	*Standardised B*	*p*	*Standardised B*	*P*
Training_Frequency	0.261	0.201	0.253	0.116	0.232	0.124
Improved Understanding and awareness about cyber security	0.162	0.507	0.198	0.335	-	-
Engaging	-0.434	0.189	-0.465	0.099	-	-
Relevant	0.430	0.051	0.435	0.029	0.431	0.006
Enjoyable	0.250	0.486	0.251	0.341	-	-
Difficult	0.025	0.910	-	-	-	-
Cyber_Attack_Exposure	0.250	0.179	0.303	0.052	0.282	0.065
Personal_Responsibility_Level	-0.042	0.833	-	-	-	-
Gameplay_Frequency	0.069	0.696	-	-	-	-
R^2		0.480		0.475		0.410
R^2 (adjusted for number of variables)		0.268		0.354		0.349

A linear regression was run to find the most significant predictors of cyber security behaviour. The least significant factor was iteratively removed, and the regression rerun, until adjusted R^2 was maximised. In this case, this occurred with two variables having very high p values ($p > 0.3$), so these were removed as unreliable (and this made almost no change to the adjusted R^2 score). The model is still included in the results. The factors of Frequency, Relevance, and Previous exposure to cyber threats made up the final prediction, with the adjusted R^2 value being almost maximised with only these three (the R^2 value could be slightly increased but only with the addition of statistically insignificant variables).

The conclusion that would be drawn from this model is that the relevance of training, the frequency of training and the cyber threats previously exposed to have the greatest (positive) impact on cyber security behaviour.

4.2 What Perceptions of Cyber Security Training Do End Users Have?

It has been frequently stated that existing cyber security training is not engaging and not fun, and these results tend to support that – when participants were asked whether they felt training they had taken was engaging/enjoyable, the mean of the responses were around 3 (3.33 and 2.94 respectively) – which approximately corresponds to a neutral response. As is the case for all the results, the small sample size means it is difficult to make definitive conclusions.

There was a moderately strong correlation between all queried factors and the likelihood that participants felt that training had changed their behaviour. In particular, the correlation between relevance and engagement was particularly strong (around 0.6). It was expected that there would be some correlation between the likelihood of participants feeling that their behaviour had been changed and the types of training they took, however the correlations found were not significant.

Table 3: Correlation between training factors and feeling that training has changed their behaviour

Predictor	Correlation	Lower C.I	Upper C.I
Difficulty	0.345	-0.005	0.619
Relevance	0.599	0.321	0.781
Enjoyment	0.528	0.225	0.737
Engagement	0.614	0.343	0.791

With a more in-depth analysis, there are some moderately strong correlations. Looking particularly at the question "What do you think about the following statements regarding cyber security awareness training that you have taken?" the table above shows various correlations between various responses and the likelihood of participants feeling that previous training has changed their behaviour.

Another linear regression was run on this data, with the dependent variable being whether participants felt that training they had previously taken has changed their behaviour. The method for this linear regression is the same as the regression in the previous section.

Table 4: Partial results of linear regression on whether participants feel training has changed their behaviour

Variable	Initial Model		Final Model	
	Standardised B	*p*	*Standardised B*	*P*
Engaging	0.223	0.393	0.390	0.016
Relevant	0.327	0.053	0.349	0.029
Enjoyable	0.123	0.644	-	-
Difficult	0.366	0.022	0.281	0.040
Instructor-led remotely/online	0.116	0.496	-	-
E-learning (online/self-directed)	-0.039	0.846	-	-
Simulation-Based	0.116	0.496	-	-
R^2		0.565		0.529
R^2 (adjusted for number of variables)		0.438		0.479

The (adjusted) R^2 value of 0.479 is higher than in the previous regression, but considering the difficulty of measuring human behaviour, it is difficult to tell if this is a good result. Given results that have been found previously it seems reasonable that engagement, relevance, and difficulty would have an impact on behaviour change.

Ultimately the final model contained only engagement, relevance, and difficulty as the most significant predictors of how likely users feel their behaviour has been changed. All three have a $p<0.05$, which indicates statistical significance. Engagement and enjoyment continue to be influential factors, which are also viewed to

be lacking in existing training. While Enjoyment was not in either model, there was correlation between both variables, and it was excluded by a small margin.

It is not clear whether difficulty of training positively or negatively contributes to actual behaviour change. As these results are centred around perceived change, it may be the case that participants internally correlate the difficulty of training with the effectiveness of training – as they feel that training that is difficult must be effective, while training that is easy may not have much of an impact.

4.3 How do end Users Believe They Should act in a Cyber Security Context?

All participants responded that they believed that they were responsible for their own security. In addition to this, however, 32 respondents of the 37 (86%) felt that at least one of ISPs (Internet Service Providers), employers, technology and government were also responsible for keeping their online information secure.

Additionally, participants felt most compelled to act securely where their behaviour could potentially impact their family members and personal finances (both 35/37). Behaviour impacting peers/strangers was not as compelling a motive (20/35 – still 57%).

4.4 What do end Users Think of Game-Based Cyber Security Training Methods?

Only a single question asked participants what they thought of game-based training methods. There was a mean response of 4 roughly corresponding to a positive response, but not overwhelmingly so. There are many reasons as to why some individuals may be sceptical of game-based training, but it is promising that only 3 of the 35 responses (under 10%) were strictly negative while 25 (over 70%) were positive. As was the case previously, this data is not statistically significant due to the small sample size.

In the interviews, participants were mostly receptive to the use of game-based training options, however, it was frequently stressed that traditional cyber security training methods should not be abandoned and should be offered as an alternative for individuals who do not want to use the game-based methods. Most participants have not taken part in game-based cyber security training previously.

5. Discussion

While these results are interesting, the number of responses is such that it is difficult to make any conclusive arguments. The response pool was limited mostly to university students and researchers, particularly in the cyber security field, and is therefore not directly applicable to the population at large. Despite this, these results can give a good foundation to build upon and are worthwhile to analyse.

5.1 What is the current Cyber Security Behaviour of end Users?

While the overall behaviour score was reasonably high, detailed analysis demonstrates that some further steps should be taken, especially in certain areas in which poor behaviour is commonplace.

There was a clear correlation between the frequency and relevance of training, and the cyber security behaviour of participants. It makes sense that the relevance of training has a positive impact on cyber security behaviour, as irrelevant training would likely have limited impact on behaviour. The frequency of training would have multiple benefits to behaviour – most notably improving retention of material, as well as reminding individuals to behave securely. No training at all, or a single training course at the beginning of employment tend to result in significantly worse behaviour. Adaptive training in response to incidents and new recommendations would likely be an improvement, but there was not enough data to conclude so. The long-term impact of training in cyber security, particularly game-based training, is not well researched, so it is useful to have some empirical data to justify cyber security training being regular.

Previous exposure to cyber threats was another factor that correlated with behaviour. It would seem reasonable that individuals who have previously experienced cyber threats would be motivated to prevent recurrence, but this is not something organisations can control. Having real-world consequences/punishments for cyber breaches has been described by Maalem Lahcen *et al.* (2020) as counterproductive, and so it would be better to simulate these punishments in a safe environment. Reward/punishment mechanics in a simulated game environment could be a solution to allow this, and can also improve flow (Laffan *et al.*, 2016). This would indicate that game-based training is very suitable to the requirements of cyber security training, as it results in greater concentration and learning (Kiili, 2005), while also allowing a natural improvement in behaviour through the simulated exposure to cyber attacks. In addition to this, (more) frequent training would have a significantly reduced cost if training was at least partially automated through a game/suite of games.

5.2 What Perceptions of Cyber Security Training do end Users Have?

There was no indication that participants considered existing training to be engaging or enjoyable consistent with observations such as by Haney & Lutters (2018). In the interviews, participants who had taken limited cyber security training could remember very little of the training they had done in the past, but still felt as though they had learnt at least something from it. The most memorable parts of the training were generally the most fun/interesting parts, though this was not always the case.

Overall, participants felt only somewhat (3.66) that previous cyber security training had changed their behaviour. Participants who found training to be fun and engaging almost always felt that training had changed their behaviour. This perception may not carry over to reality, but similar studies also often use self-report data, so this observation would be using comparable data. It would be useful to know why participants felt that their behaviour changed, perhaps as part of future study.

Participants typically do not feel that cyber security training was enjoyable or engaging, yet participants who found training enjoyable and engaging were more likely to say that their behaviour had improved because of the training, and overall seemed to have better cyber security behaviour.

The relevance of training was another important factor in the perception of training; however, it is possible that this result is largely caused by the positive response to training being relevant, with 26/33 responses finding training to be relevant. Since this was also a positive factor for behaviour, it can be considered important, and is perhaps evidence that training should be more tailored to individuals/groups and not 'one-size-fits-all' – something echoed in Bada, Sasse & Nurse (2019) which reported similar conclusions.

Difficulty did arise as an influential factor in perceptions of training impact, with a moderate correlation. This may be a result of the experience of flow, as the appropriate difficulty of an activity is a significant factor in flow (Jin, 2012), which subsequently positively impacts learning (Reeves, Calic & Delfabbro, 2021)

5.3 How do end Users Believe They Should act in a Cyber Security Context?

Participants typically recognise that they are responsible for their own cyber security behaviour. While discussions with some participants revealed that behaviour is somewhat changed by relying on others, the answers mostly reflect situations beyond a users' control – such as data stored by websites being covered by online safety laws. Good security behaviour in some cases may require some trust in external factors – for example the safety of a password manager. It would not be surprising if in some cases cyber security behaviour was relaxed due to trusting a system that insufficiently protects their information.

Participants were typically more motivated to change their behaviour to protect family members and their own finances than to protect strangers/peers. This makes sense, as finances and family members will usually have a more significant impact on their lives than colleagues and strangers. This may indicate that emphasising the impact of their behaviour on the organisation they work at would be less effective. Instead, it may be more influential to make individuals aware of personal consequences – potential loss of employment or bonuses, or the possibility of attackers using reused passwords to access bank details. Cheng *et al.* (2013) suggests that while punishments for poor cyber security behaviour can be beneficial, this will only be the case when the consequences are clearly outlined beforehand, and these results would seem to support this as participants seem willing to change behaviour, if likely consequences are clearly communicated to them.

5.4 What do end Users Think of Game-Based Cyber Security Training Methods?

Overall, the opinions of game-based cyber security training were quite positive. Some of the responses distinguish between different types of game-based training, with one respondent stating that puzzle-solving does not "particularly interest or motivate" them. Different types of games will engage different groups of users and a particular area of further study will be to categorise different genres of games and determine how they impact on learning and behaviour change. As previously discussed, a potential advantage of game-based learning is the ability to simulate cyber incidents, to provide practical experience, and to demonstrate the consequences in a safe environment. The responses for game-based methods specifically were limited, but they were generally in line with these reasons, as well as an increase in engagement, complementing the general result that existing training is not engaging (Haney & Lutters, 2018).

6. Limitations and Further Work

Cyber security behaviour among the sample was reasonably good, but there may be flaws with the method in which this conclusion was reached. All factors were weighted equally, with no context considered in the analysis.

For example, a participant who always uses the same password for all sites, but otherwise acts securely, will receive a very strong behaviour score. Each aspect of behaviour could be considered separately, though this would increase the volume of analysis necessary, and increase the likelihood of extreme results. With a larger sample size, it may be reasonable for a future study to focus specifically on password behaviour (for example) and take the overall risk of behaviours into account.

There was no training for participants to complete – the survey was entirely focused on training that participants had done in the past. As there is no way to analyse all the training they took, it is impossible to determine which techniques were used in the training. A more in-depth study could ask similar questions of a pre-determined training exercise, or even use pre- and post- training questionnaires/tests to attempt to determine behaviour change.

The responses themselves were self-report in nature – meaning bias and misunderstanding may have skewed the results. Future data collection would be strengthened if collected through another method, such as by a neutral observer, or through performance-based assessment through some tool.

As has been previously stated, the sample size in this case was quite small. Larger and more varied sample sizes would permit a more detailed analysis, with richer conclusions. Nevertheless, the results obtained show evidence that game-based cyber security training can address many of the issues that exist within cyber security training currently. Future work will aim to expand on this, by investigating which specific aspects of games are most well suited to cyber security training and considering what aspects of existing training are the most significant barriers to behaviour change. Several correlations were found, but there is no data that would encourage drawing any causal relationships. As many variables were compared against each other, it is quite likely that some level of coincidence would arise.

There was a minimal focus directly on game-based training, with only a single question, and some discussions in later interviews. Nevertheless, it was demonstrated that engagement and enjoyment impact on behaviour, two factors that are often relevant to game-based learning.

Directly following this study, there will be several next steps. Firstly, the various game characteristics that impact cyber security behaviour must be determined. For example, engagement has frequently been mentioned as a possible factor. This information will be used to develop prototype game-based methods, which implement effective methods to change behaviour. These will be tested against traditional cyber security training methods, and the resultant data will be used to develop a set of guidelines for developing game-based training methods that effectively impact cyber security behaviour.

References

Abawajy, J. (2014) 'User preference of cyber security awareness delivery methods', *Behaviour & information technology*, 33(3), pp. 237–248. doi: 10.1080/0144929X.2012.708787.

Accenture (2021) *How aligning security and the business creates cyber resilience*. Available at: https://www.accenture.com/_acnmedia/PDF-165/Accenture-State-Of-Cybersecurity-2021.pdf (Accessed: 8 May 2023).

Bada, M., Sasse, A.M. & Nurse, J.R.C. (2015) 'Cyber Security Awareness Campaigns: Why do they fail to change behaviour?', *Proceedings of the International Conference on Cyber Security for Sustainable Society*, Coventry, United Kingdom, 26 February. doi: 10.48550/arXiv.1901.02672.

Cain, A.A., Edwards, M.E. & Still, J.D. (2018) 'An exploratory study of cyber hygiene behaviors and knowledge', *Journal of information security and applications*, 42, pp. 36–45. doi: 10.1016/j.jisa.2018.08.002.

Cheng, L. *et al.* (2013) 'Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory', Computers security, 39, pp. 447–459. doi:10.1016/j.cose.2013.09.009.

Egelman, S. *et al.* (2016) 'The teaching privacy curriculum', *Proceedings of the 47th ACM Technical Symposium on Computing Science Education*, Memphis, Tennessee, 17 February. pp. 591-596. doi: 10.1145/2839509.2844619.

Furnell, S., Bryant, P. & Phippen, A. (2007) 'Assessing the security perceptions of personal Internet users', *Computers & security*, 26(5), pp. 410–417. doi: 10.1016/j.cose.2007.03.001.

GICAST (n.d.) *GICAST BOC End of Course*. Available at: https://www.surveymonkey.com/results/SM-536C6Y257/summary/ Password: G1cast?0penlearn (Accessed 1st July 2022)

Hamari, J. *et al*. (2016) 'Challenging games help students learn: An empirical study on engagement, flow and immersion in game-based learning', Computers in human behavior, 54, pp. 170–179. doi: 10.1016/j.chb.2015.07.045.

Haney, J. & Lutters, W. (2018) '"It's scary...it's confusing...it's dull": how cybersecurity advocates overcome negative perceptions of security'. *Proceedings of the Fourteenth USENIX Conference on Usable Privacy and Security (SOUPS '18).* Baltimore, USA, 12-14 August. pp. 411–425. Available at: https://www.usenix.org/conference/soups2018/presentation/haney-perceptions (Accessed: 14 May 2023).

Hendrix, M., Al-Sherbaz, A., & Bloom, V. (2016) 'Game Based Cyber Security Training: are Serious Games suitable for cyber security training?', *International Journal of Serious Games*, 3. doi: 10.17083/ijsg.v3i1.107.

Hong, Y. and Furnell, S. (2021) 'Understanding cybersecurity behavioral habits: Insights from situational support', *Journal of information security and applications*, 57, p. 102710–102712. doi: 10.1016/j.jisa.2020.102710.

Jin, S.-A.A. (2012) '"Toward Integrative Models of Flow": Effects of Performance, Skill, Challenge, Playfulness, and Presence on Flow in Video Games', *Journal of broadcasting electronic media*, 56(2), pp. 169–186. doi: 10.1080/08838151.2012.678516.

Johnson, J. (2021) *Global digital population as of January 2021*. Available at: https://www.statista.com/statistics/617136/digital-population-worldwide/ (Accessed: 8 May 2023).

Kaspersky (2017) *The Human Factor in IT Security: How Enployees are Making Businesses Vulnerable from Within.* Available at: https://www.kaspersky.com/blog/the-human-factor-in-it-security/ (Accessed: 8 May 2023).

Kiili, K. (2005) 'Content creation challenges and flow experience in educational games: The IT-Emperor case', *The Internet and higher education*, 8(3), pp. 183–198. doi: 10.1016/j.iheduc.2005.06.001.

Kumaraguru, P. *et al.* (2007) 'Protecting people from phishing: the design and evaluation of an embedded training email system', *Proceedings of the SIGCHI Conference on human factors in computing systems.* ACM, pp. 905–914. doi: 10.1145/1240624.1240760.

Laffan, D.A. *et al*. (2016) ', *Computers in human behavior*, 65, pp. 544–549. doi: 10.1016/j.chb.2016.09.004.

Maalem Lahcen, R.A. *et al.* (2020) 'Review and insight on the behavioral aspects of cybersecurity', *Cybersecurity*, 3(1), pp. 1–18. doi:10.1186/s42400-020-00050-w.

Nakamura, J., Csikszentmihalyi, M. (2002) 'The concept of flow'. In C. R. Snyder S. J. Lopez (Eds.), *Handbook of positive psychology* pp. 89–105. Oxford, UK: Oxford University Press

PwC (2013) 2013 *Information Security Breaches Survey.* Available at: https://www.pwc.co.uk/assets/pdf/cyber-security-2013-technical-report.pdf (Accessed: 8 May 2023).

Reeves, A., Calic, D. and Delfabbro, P. (2021) '"Get a red-hot poker and open up my eyes, it's so boring"1: Employee perceptions of cybersecurity training', *Computers & security*, 106, 102281. doi: 10.1016/j.cose.2021.102281.

Sheng, S. *et al.* (2007) 'Anti-Phishing Phil: The design and evaluation of a game that teaches people not to fall for phish.' *Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS'07)*. ACM, 88–99

Sherry, J.L. (2004) 'Flow and Media Enjoyment', *Communication theory*, 14(4), pp. 328–347. doi: 10.1111/j.1468-2885.2004.tb00318.x.

Streeter, D. (2013) *Operational Security and Cyber Security*. Available at: https://www.academia.edu/5490787/Operational_Security_and_Cyber_Security (Accessed: 8 May 2023).

Zhang-Kennedy, L. and Chiasson, S. (2022) 'A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education', *ACM computing surveys*, 54(1), pp. 1–39. doi: 10.1145/3427920.

Zwilling, M. *et al.* (2022) 'Cyber Security Awareness, Knowledge and Behavior: A Comparative Study', *The Journal of computer information systems*, 62(1), pp. 82–97. doi: 10.1080/08874417.2020.1712269.