Gamified Provocations of Interest for Cybersecurity Awareness

Steven Furnell[1], James Todd[1], Lucija Šmid[2], Simon Castle-Green[1] and Xavier Carpent[1]
[1] School of Computer Science, University of Nottingham, UK
[2] School of Management, University of Bath, UK

steven.furnell@nottingham.ac.uk
james.todd@nottingham.ac.uk
ls2793@bath.ac.uk
simon.castle-green@nottingham.ac.uk
xavier.carpent@nottingham.ac.uk

Abstract: Cybersecurity awareness is important for all users of digital technology, but it can often be challenging to capture the attention of those that need it. Gamification can potentially contribute in provoking interest and engagement, but consideration still needs to be given to potential barriers to entry (in terms of the time required to understand and play the game, and any prior knowledge or support that players may need to do so). Many current cybersecurity games are well suited for use in settings where time has been set aside to play them. However, they are less applicable to being used as initial provocations of interest, or to attract and engage players on a more casual basis. With this in mind, the paper presents three game-based activities that have been specifically designed to support short-form cybersecurity engagement and awareness: Cyber Defence Dice, Hacker Whacker, and Password Enlightener. The discussion highlights how these activities offer an entry point for additional cybersecurity engagement, providing a foundation for further awareness and education activities or a reference point that can be used within them.

Keywords: Cybersecurity awareness, Cybersecurity education, Cybersecurity games

1. Introduction

Baseline cybersecurity awareness is now arguably essential for all users of digital technologies to recognise common threats and how to protect against them. Unfortunately, those seeking to promote awareness can face an immediate challenge in terms of how to capture initial interest, which often includes an accompanying challenge of turning what many regard as a technical (and potentially boring) topic into something that feels more accessible to a wider audience. Gamification is often put forward as a potential solution, and there are indeed already a variety of existing games in the cybersecurity space (Zhang-Kennedy and Chiasson, 2021; Shostack, 2026). However, these also have some potential shortcomings in the context of offering something that is suited to taking the initial steps with a layperson audience. The focus of this paper is to offer an alternative perspective, supported by a series of activities that have been implemented and tested in practice.

The paper begins by briefly surveying existing cyber security games, with a specific focus upon those realised in physical formats. The main paper then presents and describes three cyber-engagement activities developed by the authors: *Cyber Defence Dice, Hacker Whacker, and Password Enlightener.* Each of the activities is designed to act a provocation of interest, providing a means to attract and engage participants that may benefit from being nudged towards cybersecurity and related awareness. As such, while not going as deeply into the detail of cybersecurity as the other games, they offer a means of getting a foot in the door in terms of user engagement and providing a foundation upon which to build further awareness and learning.

2. Existing Cyber Security Games

Cybersecurity games exist in digital and physical formats. Our interest is particularly focused upon the latter, as the offline experience is considered to have several advantages. Firstly, it breaks people away from *using* their technology, which potentially enables them to take a step back and think about its protection. Secondly, it creates a social scenario in which players can interact, observe each other's actions, and discuss the shared experience together (which may take place during and/or after the game). Lastly, and linked to both prior points, it serves to make playing the game feel like more of occasion, as compared to an online or app-based game that a player may more easily load but then leave on a whim. By contract, once a game is started in the physical context, it creates more of a commitment to play, with a physical and social experience also potentially being more memorable.

A range of related games exist, including card games, board games and other tabletop formats. For readers interested in gaining a fuller appreciation of the volume and variety of tabletop games available, a relevant resource is maintained by Shostack (2026). For the purposes of this paper, however, the following examples offer an illustrative cross-section of some of the more well-known and established games:

- **Backdoors & Breaches**: A card game for two or more players, which involves defending against attack scenarios (Black Hills, nd). Cards include four categories of Attacks (Initial Compromise, Pivot and Escalate, C2 and Exfil, and Persistence), plus Procedures and Injects. An attack scenario is created by a player designated as 'Incident Captain', and one or more further players then take the role of Defenders (drawing from Procedure cards to counter the attack). Games typically last 30-60 minutes, and end if the Defenders have successfully revealed all four attacks, or if ten turns have been taken.
- **Control-Alt-Hack**: A card-based game based on the scenario of players working for a white-hat ethical hacking company (Denning et al, 2013). The game is based around Hackers with different skills (e.g. cryptanalysis, hardware hacking, social engineering) being required to complete Missions (which involve a number of required tasks). Play involves rolling numbered dice to determine what level of skill is required for each task in the Mission, and then seeing if the player's Hacker has that level. Entropy cards, Money and Hacker Cred tokens are also involved in the gameplay, and games last around one hour.
- **Cyber Threat Defender**: A two-player game involving four types of cards - Assets, Defences, Events and Attacks (CIAS, 2024). Players create a network of Assets, and build Defences to protect them from Attacks. Events then occur that may help or harm security. Each card has a resulting effect, and a points value. Games take an average of 20 minutes, and end when a player wins (by reaching 30 points) or loses (by reaching -45).
- **Decisions & Disruptions**: A LEGO-based tabletop game, focused around industrial control systems security, in which 5-8 players are responsible for managing the security of a small utility company (Frey et al, 2019). The LEGO pieces are used to construct the environment and defences, and players then make decisions about how to protect against attacks, while working within the limits of their budget. A Game Master is needed to run the game and play lasts up to two hours.
- **Riskio**: A tabletop game in which players protect their organisation's data and services against various threats (with 78 related cards covering categories of Spoofing, Tampering, Repudiation, Information Disclosure, Denial of services, and Elevation of Privilege) (Hart et al, 2020). Games need 3-5 players, plus an experienced cyber professional to act as Games Master, and can last around 45 minutes

Even this small sample highlights that while a range of games are available, most are clearly designed for relatively long-form play and are often focus on aspects of cybersecurity that go beyond the interest of a layperson audience. As such, while very valid in their target space, they do not lend themselves to more casual use or towards promoting more entry-level cybersecurity concepts. This is not meant to be seen as a criticism of the existing games. All are fit for their intended purpose, but it is important to be clear on what that purpose is. For example, they are all very suitable as educational aids for those already active or interested in cybersecurity (e.g. for cybersecurity students, cyber teams within organisations etc), but arguably less suited to a more general population. Indeed, none appear to have been designed for promoting initial engagement and awareness raising, and so there is an opportunity for games and related activities that fit within this space.

3. Expanding the Landscape of Games for Cyber Security Engagement and Awareness

Having identified the gap offered by the existing games, the authors have created a series of gamified physical cyber-engagement activities:

- *Cyber Defence Dice* – an awareness raising game of attack and defence
- *Hacker Whacker* – a fast-paced arcade style game that raises awareness of assets, threats and safeguards
- *Password Enlightener* – a password meter realised in the manner of a light-up fairground-style strength tester machine.

These have collectively been designed for use in public-facing events and offer a means of attracting interest amongst both general audiences and more specific groups, such as young people and small business owners.

The Cyber Defence Dice and Hacker Whacker games are both based around a common set of cybersecurity concepts, in terms of Assets (i.e. elements that require protection), Threats (i.e. events that could harm the Assets), and Defences (i.e. cybersecurity safeguards that protect against the Threats). These are illustrated in Table 1, along with the images that we have designed to represent each of them. In terms of incorporating them into the gameplay, Hacker Whacker promotes basic recognition of the different items, whereas Cyber Defence Dice introduces interrelationships between them and elements of decision making. The images were specifically designed to ensure that they would be able to be rendered clearly when 3D printing a standard six-sided die.

Table 1: Assets, Threats and Safeguards used in the games

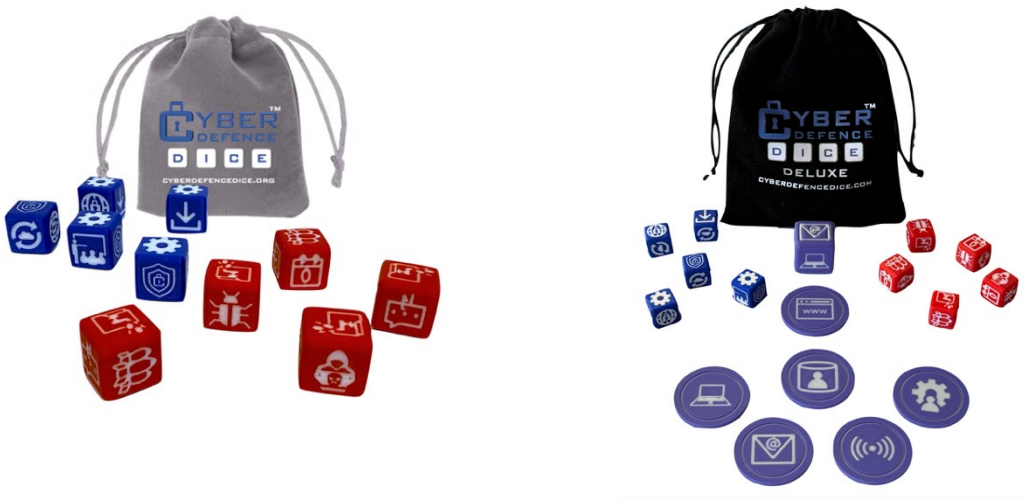
Assets	Threats	Defences
 Admin Account	 Malware	 System and App Updates
 Email Server	 Hackers	 User Awareness
 Personal Computer	 Accidental Breach	 Backup
 Personal Data	 Phishing	 Secure Configuration
 Website	 Denial of Service	 Internet Security
 Wireless Router	 Zero Day Attack	 Defence in Depth

3.1 Cyber Defence Dice

Cyber Defence Dice offers an entirely physical engagement experience, based upon the concepts of attack and defence. The basic premise of the game involves one side (which can be an individual player or a small team of up to 4-5 people) playing the role of an attacker and the other side taking the role of defender. Attacks and defences are mounted by means of dice rolls, with each side having an associated set of five dice. The attacker dice are red (reflecting the notion of a Red Team in cybersecurity testing), with the six die faces reflecting the Threats from Figure 1. Meanwhile, the defender dice are Blue (again, reflecting the established cybersecurity concept of a Blue Team being defenders), with the die faces taken from the Defences in Figure 1. The game works by attackers throwing a suitable set of threats, and defenders then throwing their dice in an attempt to offer a suitable defence (alternatively, the defenders can start, with the attackers then trying to beat the security posture that has been established). The starting side can take up to three throws and can keep or re-roll whatever dice they choose on their second or third attempts. They may, however, elect to stop after one or two rolls, and the other side is then also limited to that number of rolls when making their response. Players use an accompanying reference card to confirm which attacks beat which defences and vice versa.

The core version of the game is called Match Mode, where players must meet (to draw) or exceed (to win) the *number* of matching dice thrown by the other side, using a defence (or attack) *type* that is matched to the attack (or defence) *type* previously thrown. The authors have also created rules for two alternative game variants (called Combinations, and Attack Matcher), as well as an extension to Match Mode that makes use of Assets, While the presentation of the full game rules is outside the scope of this paper, interested readers can refer to www.cyberdefencedice.com for more details (which includes descriptions of different game variants and worked examples of gameplay). Additionally, the background to the core game, and details of associated evaluations are reported in Furnell et al. (2026).

The game is produced in standard and deluxe versions, as depicted in Figure 1, with the difference being that the latter incorporates the use of assets that players must compete to acquire or protect. These are represented by tokens, with each asset type being targeted via different combinations of attack or defence (with players again being able to use the accompanying reference card to check which attacks/defences work for which assets).



(a) (b)

Figure 1: Cyber Defence Dice in (a) standard and (b) deluxe formats

The dice and asset tokens are 3D printed in-house, with the accompanying imagery also having been designed and drawn by the authors. Additionally, sets of larger format dice have also been produced for use in public engagement events such as exhibitions. These are designed to be thrown on the floor, as shown in Figure 2.

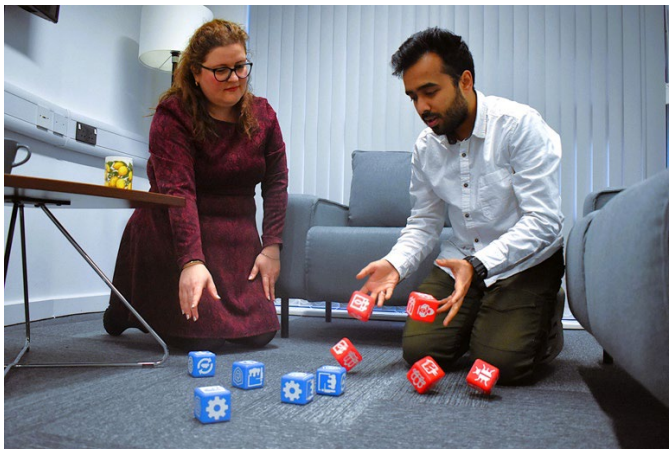


Figure 2: Playing with large format dice

The game has been successfully play-tested with a range of audiences (including groups from the general public, as well as those already familiar with the concepts, such as cybersecurity students and professionals), with positive ratings being obtained in relation to both the awareness value and the enjoyability of the game. It has also been used as a basis for teaching and awareness-raising sessions for small businesses.

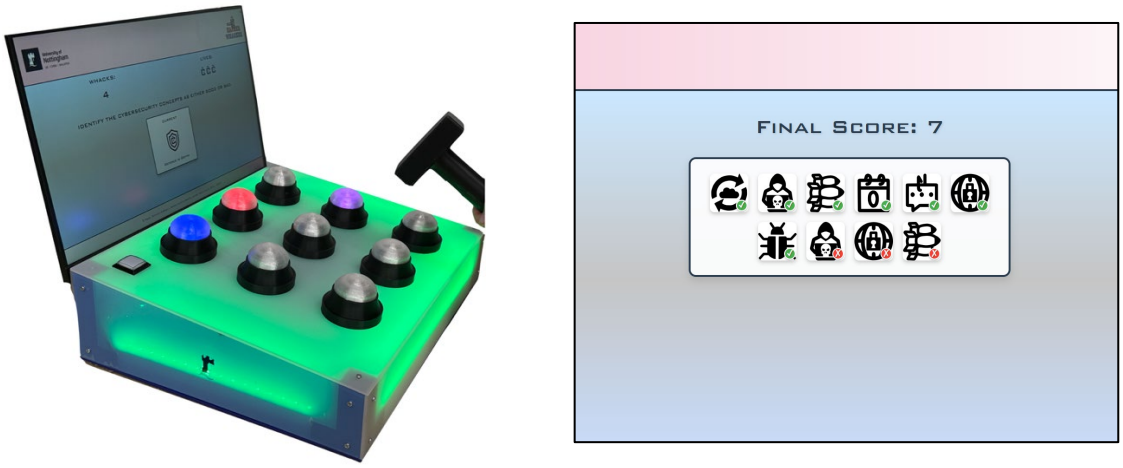
3.2 Hacker Whacker

Inspired by the popular arcade game Whac-a-Mole, Hacker Whacker is a custom device, designed and implemented by the authors (Todd et al. 2026). The game uses the same images as the Cyber Defence Dice, but this time they appear on-screen and players are required to recognise and respond to the category being shown. Unlike the colour-coded usage in the dice game, the images now appear as simple black on white representations so as not to convey which category they belong to. The game has two variants:

- *Threats and Safeguards* – Blue and red buttons illuminate on the playboard, with players needing to hit the blue button if the current image is a safeguard, or the red button if it is a threat.
- *Assets, Threats and Safeguards* – As above, but with displayed images also including the Assets, and a purple button also being lit on the playboard (i.e. the player now needs to correctly hit one of three displayed colours).

In both cases, the players must react quickly enough (i.e. before the image changes and the light pattern changes) and hit the appropriate button to match the category of the item shown on screen. If they fail to do so

within a time limit (which starts at a couple of seconds and reduces as the game progresses), or they hit the wrong button, then they lose a life. The game ends after three lives are lost, at which point the player is shown a summary of all the items they were presented with, and whether they got each one right or wrong. Figure 3 shows the game in action, with the Threats and Safeguards variant being played, as well as the feedback delivered to the player at the end of the game.



(a) (b)

Figure 3: The Hacker Whacker game (a) device, and (b) example end-of-game summary

It is to be expected that many players initially score poorly because they may not *recognise* the threats, safeguards and assets, and so part of the learning value of the gameplay is that it enables these concepts to be reinforced as they play further. At the same time, the learning potential of the game is ultimately limited, as there is no basis for players to go *beyond* this once the initial lessons have been learned. As such, repeated gameplay simply serves to reinforce notions of things that are good or bad, and does not have any of the resulting decision-making aspects that occur in Cyber Defence Dice. Having said this, the time investment in the game - even if somebody plays multiple times - is only a few minutes, and so the awareness-raising outcome still represents a reasonable return on investment relative to the time involved. Moreover, the arcade-style nature of the game has the potential to attract players that may not be interested in playing dice, and so opens the opportunity for resulting engagement in a different way.

3.3 Password Enlightener

The issue of user authentication is one that is notably missing from the defences represented in the other games, but it is specifically the focus of the Password Enlightener device. This, as shown in Figure 4, is a password meter reimagined in the form of a fairground style 'test your strength' machine. The concept of password meters will already be familiar to many through their use of websites (de Carné de Carnavalet and Mannan, 2014), and so the Enlightener typically requires little explanation for first time users. The device is more of an engagement activity than a game, but participants do tend to end up competing with each other to achieve better scores.

The player enters their password via the touchscreen at the bottom of the device (Figure 4b), and then presses the large illuminated red button to initiate the assessment. The scoring process is then based on a series of checks:

- assessing the length and complexity of the string
- checking against a dictionary of commonly leaked passwords
- calculating how long it would take to brute force the string
- checking if character substitution has been used (e.g. h3ll0, Croiss@nt) using a reverse leet algorithm (to identify use of common words with substituted characters)
- looking for patterns (e.g. dates, repetitive words etc.)

In addition to the rating, which is revealed by the progressive lighting of the lights, the player is also provided with some resulting feedback (Figure 4c) that explains the implications of their score and how it was determined.

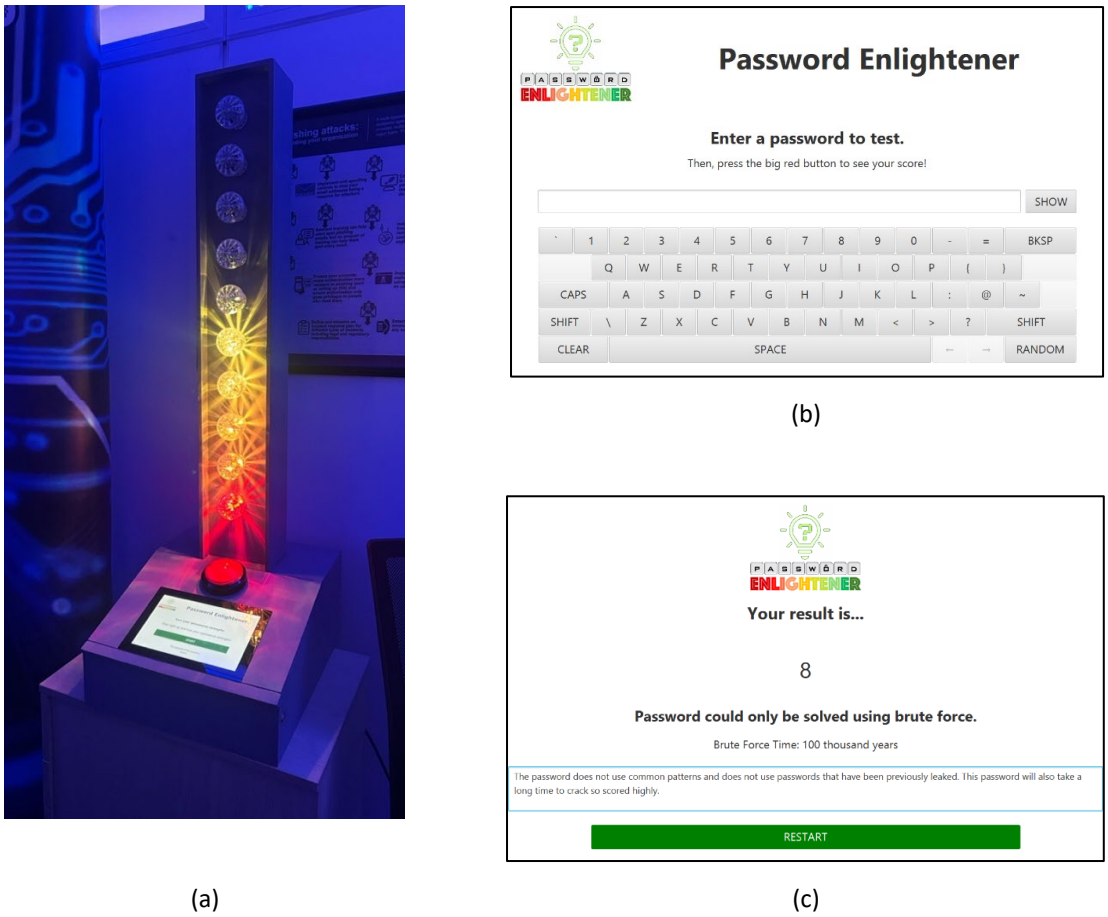


Figure 4: The Password Enlightener (a) device, (b) password entry and (c) example of feedback

This game is typically the one case in which players come to the activity with some pre-existing knowledge around what is involved. Many already have (and often express) some level of expectation around how their password will score ("I think mine is really bad", "I use a very strong password" etc). The main concern from the more security-aware users is "Are you capturing the passwords?", and this is not the aim of the exercise. Regardless of whether the question arises, players are assured that their passwords are not stored in any way and that no further use is made of them. Users are also advised to be cautious if they plan to enter an existing password in case somebody is observing (given that shoulder surfing or filming of their activity cannot be ruled out in public events).

In most events the device has been made available for visitors to come and use on an individual basis. However, it is also possible to use it in a more structured manner, with a group of players being asked to create new passwords and take turns to enter them on the device to see who scores the best. To ensure fair play, and show that they can remember the information rather than just type something in that maximises their score, the process works as follows:

- Each player writes their candidate password on a piece of paper, and then turns their paper over.
- Players take turns to enter their passwords and record the scores. On each attempt, the person running the Password Enlightener reveals the password on the device and makes a note of it.
- When all players have taken their turn, everyone then writes their password again, on the blank side of their paper.
- The team member can then check that the winning player(s) have written the *same* password on both sides of their paper (i.e. that they could remember it for the duration of the activity) and that this also matches what was entered on the device (i.e. that they did not cheat by remembering something easy and then entering a more lengthy or complex string on the device in order to score better).

The learning outcome tends to be a level of reassurance if indeed the players prove themselves able to select and enter strong passwords, or alternatively a pause for thought if they enter a password that scores poorly. In the latter case team members running the activity can give advice on strategies for improving password strength

(e.g. focusing on the length and using techniques such as three random words (McCormack, 2016) to aid memorability). The memorability of what was entered is a key issue, and many players readily discover that they can score highly by entering long strings of random characters. However, they soon fall foul this if the team member running the activity asked them to enter the same thing again, in some cases introducing an additional lesson about the memorability of passwords.

4. Discussion

When considering them as provocations of interest, the games clearly have potential to attract players for different reasons. The dice offer a direct basis for players to compete against each other, while Hacker Whackers delivers a fast-paced arcade experience. Meanwhile, Password Enlightener works on the basis of potential curiosity about how well they may be able to score. In all cases, the visual prompts (the colours of the dice, the coloured lights of the devices) and the kinetic activities (throwing the dice, hitting the buttons) provide further elements that help to generate interest and draw people in.

As previously mentioned, each of the games has proven successful in the context of public engagement events, and Figure 5 shows an example of the three activities ready for use in such a setting. The extent of engagement in this context can still vary. Some players will come, have a go, and then leave. Others will stay for longer and have multiple attempts (sometimes then needing to be encouraged to let someone else have a go). In all cases, their engagement offers an opening to discuss the cybersecurity concepts involved, whether they understand the threats, protect their own systems, and so on. As such, even in an event context there is the opportunity for some basic awareness raising to occur. However, this can be enhanced further if the activities are used in more structured settings, such as being a prelude or accompaniment to a more specific security awareness session.

Figure 5: An example of activity setup for an engagement event

When comparing the new games to those discussed earlier, the other tabletop games are all more substantial in terms of their game dynamics and complexity. However, there is also a trade-off to be recognised. The other games may provide more depth in terms of the cybersecurity learning experience, but equally they require a much more significant investment of time to both understand and play the games. This in turn potentially reduces the audience to those with the time and inclination to take part. An interesting basis for illustrating this is to compare the instructions/guides that accompany each of the games, the length and readability of which is likely to further influence their accessibility and applicability to different audiences. For example, if there is a lot to read and/or the language is complex, then this could represent a barrier to some players. To this end, the instructions for the five games listed earlier in the paper were assessed, alongside those from Cyber Defence Dice (listing the standard and 'Deluxe' versions of the game separately, as the latter requires additional text to be read to understand the use of Assets). The 'Editor' feature within Microsoft Word was used to perform the assessments, and in each case the input in was raw text describing the game and how to play it (with documents having been stripped of title pages, table of contents, tables, appendices, etc). Hacker Whacker and the Password Enlightener were excluded because they have no accompanying instruction booklets – brief guidance is displayed on-screen and the rules can quickly be determined from play and observation. While not quite as brief as the classic instructions that appeared on Atari's Pong machine (i.e. "Ball will serve automatically. Avoid missing ball for high score"), players have proven to require little guidance to get going.

The findings are shown in Table 2 and there is some clear variation in the amount of text that the players need to read to understand and play the games. While several amount to the equivalent of just a couple of pages of text, others are considerably lengthier. In addition to this, it is also relevant to consider the ease with which potential players may understand what they are reading. The Flesch Reading Ease score assesses the average sentence length (words per sentence) and the average number of syllables per word. It delivers a resulting score between 0 and 100, with a higher score denoting text that is easier to read (Flesch, 1948). From the table, we can see that four of the entries in fall into the 70-80 range (which is classed as 'Fairly easy to read'), while two are in the 60-70 band (which is considered to be 'Plain English', and easily understood by those in their early teens). The outlier in the table, in both length and readability is Decisions and Disruptions, where the Reading Ease score that falls into the 'Difficult to read' category (30-50). This is also reflected in the higher Grade Level score, which indicates the US school grade at which someone would be expected to be able to read and understand the text.

Table 2: Comparing the length and readability of instructions for different games

Game	Source Material	Words	Flesch Reading Ease	Flesch-Kincaid Grade Level
Backdoors and Breaches	www.blackhillsinfosec.com/wp-content/uploads/2019/09/How-to-Play-BB.pdf	954	72.5	6.1
Cyber Defence Dice	www.cyberdefencedice.com	589	72.3	7.6
Cyber Defence Dice Deluxe	www.cyberdefencedice.com	884	72.8	7.2
Cyber Threat Defender	cdn.getshifter.co/fd026a43ee1b 7b095c768a9039a2a236c0a0d590/uploads /2025/07/CTD-Instructions-2025Rulebook.pdf	>2,000	76.2	6.4
Control-Alt-Hack	www.controlalthack.com/ downloadrules.php	>3,000	68.4	7.3
Decisions & Disruptions	github.com/Bristol-Cyber-S ecurity-Group/decisions-disruptions-kit/blob/master/D-D_Instruction_Booklet.pdf	>9,300	47.6	11.7
Riskio	www.riskio.co.uk/game-play-setup www.riskio.co.uk/game-play-attack www.riskio.co.uk/game-play-attack-1 www.riskio.co.uk/game-play-information-deck	941	62.1	9

When interpreting the results for the Cyber Defence Dice, it should be noted that the full guide covers different game variants and includes other supporting information. As such, the assessments in the table are based specifically upon the text that needs to be read to understand and play the main version of the game. This includes the general rules, the specific rules for the core game (Match Mode), and the descriptive text for a worked example (which is also accompanied by illustrations in the guide itself). It excludes background information about the threats and defence types, descriptions of alternative game modes, and a section that discusses parallels to real-world cybersecurity. All of these would, of course add to the word count and affect other scores, but they do not *need* to be read to understand and play the core game. Moreover, the essence of the standard game can be distilled down to a much more succinct set of rules, as presented in the Quick Reference Guide provided in the dice pouch. These are expressed as follows, in 60 words (with the Reading Ease reaching 83.2 and the Grade Level now just 4.9):

> *"Either side may start and has up to 3 throws, but can stop after 1 or 2 if preferred. The responding side is limited to that number of throws. Players choose which dice to keep or throw again. To win a round, throw more defence dice than the corresponding attack (or vice versa). A matching number is considered a draw."*

They are accompanied on the reference card (see Figure 6) by a list of the Threats and Defences (presenting the images alongside the names), plus the two matrices (showing which attacks beat which defences, and vice

versa). If players are comfortable with the outline and how the matrices work, then they may not need the more descriptive guidance and the worked example from the full rules.

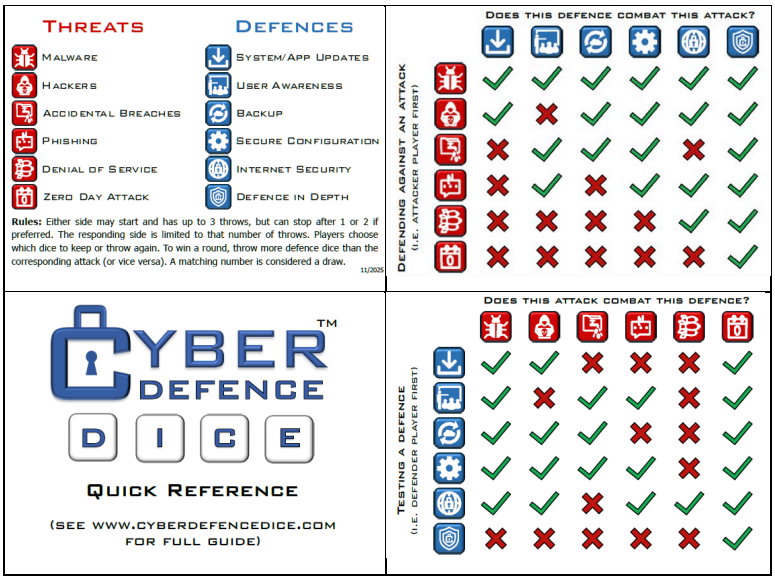


Figure 6: Cyber Defence Dice Reference Card

Another aspect to note is that the above is just considering the presentation of the text required to explain the game – it does not start to address whether they understand the *concepts* under discussion. While the Cyber Defence Dice instructions briefly explain the nature of the Threats, Defences and Assets, the other game guides rarely do this - the player is assumed to know about the basic cybersecurity issues involved, or (where appropriate) to be able to get guidance from the Game Master. For example, while Backdoors and Breaches has a relatively low word count and good readability scores, what it is actually referring to includes some potentially challenging security concepts. For example, even the names of the attack categories highlighted earlier (e.g. Pivot and Escalate, C2 and Exfil) – are unlikely to be immediately meaningful to a lay audience. Picking some examples of terminology from the card titles (e.g. Dynamic Link Library Hijacking, Domain Fronting as C2, External Password Spray, and Kerberoasting) makes it very clear that players are expected to have some significant prior knowledge in the domain.

The lower barriers to entry are not intended to imply that the Cyber Defence Dice is 'better' than the other games, but it does help to further illustrate that it is simpler. Whether this is a good or bad thing depends upon how it is intended to be used. Part of the reason that some of the game guides are more substantial is because there is more to learn. The games themselves go deeper into cybersecurity concepts and decision making (thereby addressing different audiences), and so there is a clear trade-off (or indeed trade-up) to be made against the effort required to learn how to play them. However, if the aim is to have a means of capturing initial interest and engagement, then the dice (and Hacker Whacker and Password Enlightener) are likely to offer the more suitable basis for doing so.

5. Conclusions

As in other disciplines, gamification offers a means of making cybersecurity more accessible and interesting for those who might otherwise find it less engaging. At the same time, the nature of the game needs to be matched to the target audience involved. Those with limited cybersecurity knowledge and awareness are clearly a desirable population to assist, but many of the existing games are aimed above this level. In contrast, the three games presented in this paper offer contributions more directly suited to a layperson audience. While the nature of the underlying games is very different, they share the characteristic of being quick and providing a foundation for further engagement.

All three games have been designed in ways which maximise their ability to provoke interest at events. Both Hacker Whacker and the Password Enlightener have been used at many such events, and have proven to attract players through their lights, sounds, hammer (Hacker Whacker) and large red button (Password Enlightener). Cyber Defence Dice has also been used at various events, with the larger format dice proving successful at attracting attention due to their physical size and novelty, and the smaller sets being popular giveaways, allowing

attendees to continue their education after the event. Further developments are intended, including inclusion of extra features to the game play of Hacker Whacker and the Password Enlightener, whilst still maintaining the prompt playtime and interactivity levels that have currently been achieved.

Ethics and AI declarations: The playtesting of the Cyber Defence Dice was approved by the School of Computer Science Research Ethics Committee at the University of Nottingham (CS-2024-R44). All participants read and signed associated consent forms before play began. AI tools were not used in the writing of this paper.

References

Black Hills. (nd) "Backdoors & Breaches: Visual Guide" [Online], Black Hills Information Security, https://www.blackhillsinfosec.com/wp-content/uploads/2024/03/BnB_VisualGuide_v2_03052024.pdf

CIAS. (2024) "Cyber Threat Defender", Center for Infrastructure Assurance & Security, The University of Texas at San Antonio. https://cdn.getshifter.co/fd026a43ee1b7b095c768a9039a2a236c0a0d590/uploads/2025/07/CTD-Instructions-2025Rulebook.pdf

de Carné de Carnavalet, X. and Mannan, M. (2014) "From Very Weak to Very Strong: Analyzing Password-Strength Meters", in *Network and Distributed System Security Symposium (NDSS'14)*. San Diego, CA, USA. https://www.ndss-symposium.org/ndss2014/programme/very-weak-very-strong-analyzing-password-strength-meters/

Denning, T, Lerner, A., Shostack, A. and Kohno, T. (2013) "Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security (CCS '13)*. Association for Computing Machinery, New York, NY, USA, 915–928. https://doi.org/10.1145/2508859.2516753

Flesch, R. (1948) "A new readability yardstick", *Journal of Applied Psychology*, Vol. 32, No. 3, pp21–233.

Frey, S., Rashid, A., Anthonysamy, P., Pinto-Albuquerque, M. and Naqvi. S.A. (2019) "The Good, the Bad and the Ugly: A Study of Security Decisions in a Cyber-Physical Systems Game," in *IEEE Transactions on Software Engineering*, vol. 45, no. 5, pp. 521-536. https://doi.org/10.1145/3180155.3182549.

Furnell, S., Šmid, L., Todd, J., Carpent, X. and Castle-Green, S. (2026) "Roll with it: Awareness raising with Cyber Defence Dice", to appear in *Journal of the Colloquium for Information Systems Security Education*.

Hart, S., Margheri, A., Paci, F. and Sassone, V. (2020) "Riskio: A Serious Game for Cyber Security Awareness and Education", *Computers & Security*, Volume 95,101827, https://doi.org/10.1016/j.cose.2020.101827.

McCormack, I. 2026 "Three random words or #thinkrandom", [Online], National Cyber Security Centre, UK, 27 October 2016, https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0

Shostack, A. (2026) "Tabletop Security Games + Cards", [Online], Shostack + Associates, https://shostack.org/games.

Todd, J., Furnell, S., Castle-Green, S., Šmid, L. and Carpent, C. (2026) "Hacker Whacker: An interactive game for cybersecurity education", to appear in *Proceedings of HCI-CPT 2026*.

Zhang-Kennedy, L. and Chiasson, S. (2021) "A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education", ACM Computing Surveys, 54, 1, 2021, https://doi.org/10.1145/3427920.