

VirSec – Immersive Security Training within Virtual Reality

Max Hedges¹ and Tasmina Islam^{1,*}

King's College London, London, UK

Abstract

Given the proliferation of online services and the ever-accelerating threat posed by online entities, an exploration of other vectors to educate vulnerable online users is now imperative. This paper explores Virtual Reality (VR) technology as a phishing-focused social engineering training tool with 'VirSec'. It is designed not only to inform users of threats, but to immerse users in realistic scenarios. 'VirSec' strives for replay incentive, which is reflected in its immersion-centric design choices and exciting branching-path gameplay structure.

Keywords

Cyber Security, Cyber Security Training, Virtual Reality, Immersive Learning, Phishing

1. Introduction


The infancy-period of the internet saw little to no criminal activity by virtue of its relative inaccessibility in the public domain. As time has progressed so did the knowledge and capabilities of cybercriminals. No longer were criminals simply defacing websites – cybercrime became a vessel for state sponsored corporate espionage and international warfare. Vast scale financial crimes, such as those committed by the Carabanak/Cobalt Group [1], amount to billions of dollars in stolen capital from international banks – often through the use of simple phishing emails.

The importance of cyber-security awareness is readily apparent. Personal and corporate cyber security controls such as encryption, secure coding, and vulnerability assessments – whilst effective and necessary, are evidently not enough to guarantee one's online security. Criminals throughout history have attacked weak points. Why attack multi-layered controls when you can target a person's willingness to comply? Or a person's sense of urgency and fear? This is where education becomes a driving factor in the stemming of cyber-attacks. One may urge an internet user or employee to become cyber-security aware, yet many choose to ignore or deprioritize cyber-awareness by virtue of its erroneously perceived unimportance. A middle eastern study [2] to determine the level of information security awareness among researchers, academic staff, and undergraduate students in academic institutions showed alarming levels of unawareness to cyber-threat indicators and mitigations. The implications of this study raise

2nd International Workshop on CyberSecurity Education for Industry and Academia (CSE4IA 2024)

* Corresponding author.

 max.hedges@kcl.ac.uk (M. Hedges); tasmina.islam@kc.ac.uk (T. Islam)

 0009-0000-8648-4488 (M. Hedges); 0000-0002-6437-8251 (T. Islam)



© 2024 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

alarms, as subjects lacked cyber-awareness despite the academic aptitude of the participants involved. Moreover, one could assume that those outside of academia may be even less informed. It can be argued that the educatory mediums are to blame for this lack of awareness, and so expansions into Virtual Reality solutions could open up a new door. Users within VR have the capability to interact directly with their environment using hands and even fingers [3] using tracking technology. Users can also see through an entirely new perspective – in essence allowing them to transport to any ‘real’ or fictional location. Virtual reality as a pedagogical tool is still a new frontier, bounded simply by the age and prevalence of its hardware. However, the future looks very promising [Section 2.2].

VirSec is implemented within virtual reality to utilize the immersive capabilities presented by VR technology. VirSec aims to teach its users to identify cyber-security threats in the workplace, with a focus on phishing in the form of malicious email identification. Section 2 provides a brief overview of related work in the area as well as justifies and explains VirSec’s focus. VirSec’s design motives and decisions are then discussed in Section 3, followed by their implementations and tests in Section 4 and 5 respectively. Section 6 finally concludes the paper with some indication of future expansions.

2. Related Work

2.1. Prevalent Attack Vectors

An Oxford study [4] in 2015 aggregated attack data over the 3 previous years from reports, news and surveys issued by global market players within cyber security, amassing over 15 million data points to ascertain the most prevalent attack types facing corporations and home internet users. The most common were found to be: social engineering (phishing), stolen devices/documents, malware, denial of service, and malicious insiders. As VirSec is a training application, the latter three vectors, whilst relevant, are impractical to implement. VirSec will therefore focus on phishing and social engineering, more specifically within the context of email communication – as despite advents of new technology, 95% of companies still use email as their main communication tool [5]. Email communication allows VirSec to also train users in the identification of malware within email attachments and links.

Social engineering is the manipulation of fellow human users to grant some degree of unauthorized access to the attacker. Phishing is a form of social engineering whereby attackers attempt to obtain sensitive information from a victim (login credentials, bank details, personal info etc) for some malicious end. Phishing as a technique will almost never be upfront with its intentions, it will instead play on several principles of social engineering. Workman [6] categorized these ‘*weapons of influence*’ into 7 distinct approaches: Commitment and Consistency, Reciprocation, Social Proof, Likeability and Trust, Authority Scarcity and Fear. It’s worth noting that attacks commonly involve some combination of the aforementioned principles for maximum effect.

Stolen (sensitive) devices/documents refer to the theft of devices/items containing information that can be used for a cyber-attack (potentially within a separate social engineering attack). It is worth noting attackers may not even need to obtain the physical item but can simply take a photograph or commit the information to memory for use in a later attack. The most common misplaced sensitive items are as follows [7]: Laptops, Mobile Phones, USB Drives, Sensitive Documents, Written Passwords, Company ID Cards.

2.2. Efficacy of VR For Learning

A persistent and prevalent issue with current education systems is student engagement [8]. Traditional methods of learning are confined to a combination of written and auditory comprehension. This form of learning lends itself to lack of student engagement [9], a driving factor in rates of academic failure and dissatisfaction. Virtual reality technology has the capability to provide its users with a level of immersion conducive to engagement and interest. As an example, Costa and Melotti [10] found that archaeology exhibits that contained virtual reality elements showed a massive spike in public interest and engagement.

Another prominent issue that can be addressed within VR is the lack of perceived relevancy of learning material. Students may perceive a disconnect between the information in front of them and its 'real-world' applications. Forms of learning in which the learner is provided with a 'real-world' feel have been described as '*situated*' learning [11], where the disparity between the learning material and its real-world application is minimized. A case study [12] compared traditional textbook-based learning with VR education using 'zSpace' – an immersive educational company utilizing VR. Students using zSpace reported higher satisfaction and enjoyment than those students learning through traditional methods. The test results also showed that the zSpace group performed significantly better in all topic exams than the traditional learning group.

2.3. VR Cyber Security Training Simulations

The following simulations best highlight common shortfalls of cyber training simulations.

2.3.1. KIPS Power Station Simulation

'KIPS (Kaspersky Interactive Protection Simulation) Power Station VR' [13] is a cyber-security strategy game developed within virtual reality that mimics the real-world operations of a power plant as closely as possible. Players are divided into teams of 2-4, and each must devise a cybersecurity strategy by selecting from available proactive and reactive resources such as network segmentation and anti-virus installations. At the end of each round the scores of the teams are calculated and displayed, where a team's score reflects the accuracy of their decision making. KIPS strives for realism, and in doing so limits its relevancy. Its forced-multiplayer feature combined with its 2+ hour gameplay loop discourages frequent plays, and therefore limits one's ability to 'train' using it. Players are also limited in their environmental interaction – simply being allowed to arrange cards, impacting relevancy and engagement.

2.3.2. OneBonsai Training Simulator

OneBonsai's 'Cyber Security Awareness VR' is a cyber awareness training simulator [14] that aims to make players aware of cyber threats within a corporate (office) setting. Players can move around the office and scan various objects around the room i.e., confidential documents, whiteboards etc. A tablet will display information about focused items and give the player options to deal with the item/information about the security risk that the item poses. Unlike KIPS, OneBonsai's simulation is highly generic, but perhaps to the point of contrivance, which may impact relevancy (but perhaps less so than KIPS). Its simple, short and concise gameplay may enhance replayability on one hand, yet harm it by virtual of its negligible challenge. Player

movement is also restricted to joystick only, which lends itself to nausea (motion sickness) for those inexperienced with Virtual Reality applications.

3. Design

VirSec's design followed an iterative approach, with progressive adjustments being made upon the testing specified in Section 5. The following subsections outline VirSec's broader functionality, as well as some other platform considerations.

3.1. Requirements

VirSec's simulation and training requirements have been gathered through reviewing literature on attack data [4], and the shortfalls of existing VR simulations [13,14] as discussed in Section 2.3.

Table 1
VirSec Requirements

Requirement Name	Description
Utilization of Immersion	Objects within environments should be grabbable and fully interactable i.e. throwable, placeable. Transitions between game states should also be immersive i.e. triggered with environmental rather than UI interactions.
Malicious Email Identification Simulation	Players should play an email handling simulation in which they can train to improve speed and accuracy of malicious email identification.
Sensitive Item Identification Simulation	Players should be able to play an item disposal simulation in which they must correctly identify and dispose of the sensitive items amongst a group of both non-sensitive and sensitive items.
Branching Path Gameplay Flow	Players actions/performance within individual simulation should affect future game states for a particular gameplay loop.

3.2. Development Platforms

Four development platforms have been considered based on usage: Unity3D, Unreal Engine, Godot Engine and CryEngine. Community support generally holds the most importance when attempting to implement a novel application, as one must draw from existing skillsets to learn quickly and efficiently. Unity3D maintains the highest number of active users and therefore a more comprehensive support network, whilst also offering a free edition unlike CryEngine. Godot Engine is also offered for free but has a far smaller community. Unity3D also has far more comprehensive support for VR and AR devices, with libraries such as the XR interaction toolkit [15]. VirSec therefore opts for implementation within Unity3D.

3.3. Simulations

Malicious emails often have detectable indicators [16], giving malicious email detection viability as a training simulation, as trainees will be able to hone their detections abilities in a situated learning environment. The format is appropriate as it naturally allows for many email types and ‘weapons of influence’ (section 2.1) to be considered at once (email inboxes) without simulations becoming too contrived.

VirSec’s email simulation will take place on a realistic computer setup and screen. Once the simulation is entered, the user will be greeted with a realistic computer desktop screen, which they can interact with to open an email inbox.

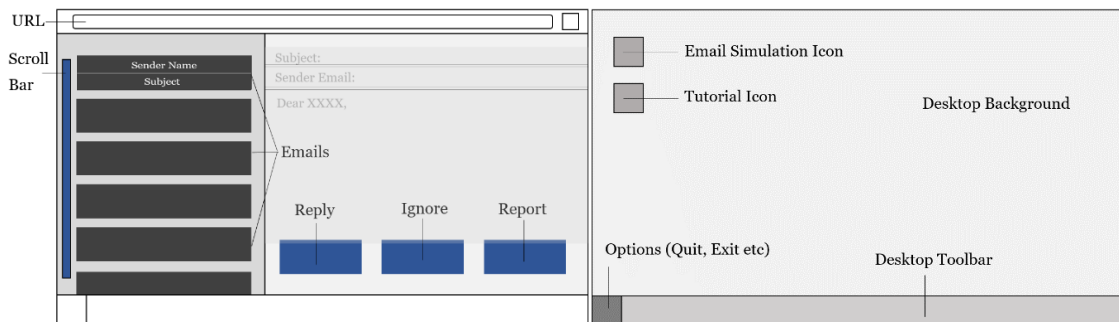


Figure 1: Email Simulation Inbox (Left), Email Simulation Desktop Screen (Right).

Emails within the inbox can be categorized as follows:

- **Benign (Unimportant)** – Emails that pose no threat to the user and should therefore be ignored (can also be replied to).
- **Benign (Important)** – Emails that pose no threat to the user yet are important emails, and so should be replied to.
- **Malicious** – Malicious emails that pose a threat to the user and the user alone.
- **Critically Malicious** – Malicious emails that pose a threat to the organization the user works for via the user’s corporate credentials (Phishing and Social Engineering) as well as malware attached to emails and within links.

The inclusion of such variation is to more closely mimic email variations in real-world inboxes; most corporate emails will fall into the 4 categories presented. The variation also provokes much more thought from the user, adding an element of difficulty that makes the user think laterally. Scores for correct/incorrect choices will reflect the severity of the error.

The Sensitive Item Identification Simulation (Section 3.1) will take place within a company break room to enhance relevancy and placing players within a situated learning environment. Users will spawn within the room and will be able to traverse the space looking for objects. Users will be prompted to dispose of sensitive objects, i.e. ID cards, by physically throwing them away, providing education to counter the ‘trashing’ attack [17]. Score will be deducted for incorrect answers and augmented for correct answers.

3.4. Immersive Branching Path Gameplay

Immersion is the key distinguisher between VirSec (and other VR simulators) and traditional forms of cyber security awareness training. It is important to note that immersion is not imparted on a VR simulation by default; immersion lies in an effective utilization of VR's capabilities and intelligent immersion-centric design choices to make the user feel as though they are performing a real-world task. VirSec forgoes immersion-breaking user interfaces – instead showing a small 'hint texts' to explain items (Figure 3).

The logical gameplay flow in existing implementations of VR cyber awareness trainers [Section 2.3] remains consistent across multiple play instances, but VirSec's gameplay flow will be branching path in nature. Players will traverse the gameplay tree (Figure 2) differently with decisions they make within individual simulations. Users will spawn in the main room and be able to transition to the 'Home PC' to view a tutorial or straight to the office PC for the email simulation. The number of emails handled determines the next stage – if they handle enough, they go to the break room, otherwise they transition to the boss' office (note that the quality of email handling has not been factored in yet). Major errors in the previous simulation will bring users to the quick time emergency breach simulation (Figure 7), in which they must respond quickly and accurately to a multiple-choice breach question. If users in the **boss's office** did not make a major error in email handling, they progress to the sensitive item identification simulation. If users at the **break room** did not make a major error, then progress to an ending. Once users complete either their sensitive item or breach simulation, they progress to the ending – where they are presented with the 'name' of their unique ending, the path they took, and the score they achieved.

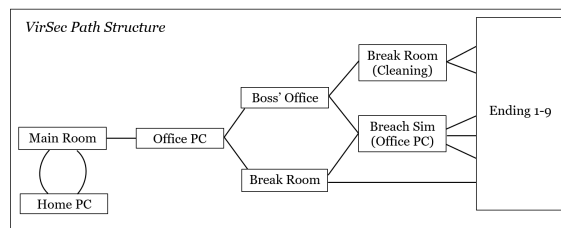


Figure 2: VirSec Branching Path Structure.

4. Implementation

4.1. User Interaction/Movement

The movement and user interaction within VirSec makes heavy use of Unity's XR Interaction toolkit [15] - a unity package to streamline the process of handling VR and AR (Augmented-Reality) head and controller inputs. Disparities in rotational and lateral head movement between the player and the player's perspective often induce nausea [18] in users - particularly if they're not conditioned for VR usage. VirSec employs a teleportation method to completely remove disparities in lateral head movement by using a combination of Unity's XR Interaction tools to create a teleportation ray incident from the player's left hand.

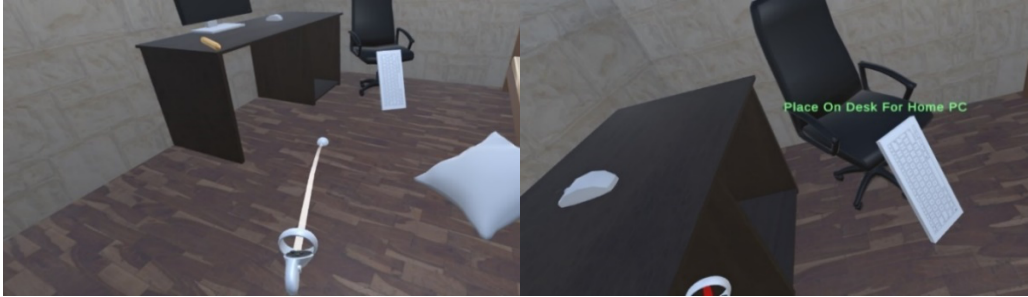


Figure 3: Before teleportation (Left), After teleportation (Note the ‘hint text’ mentioned in section 3.4) (Right).

VirSec further utilizes the XR interaction toolkit to allow objects to be picked up with users’ right hands. Players use object handling and collision to transition between rooms and simulations, as well as dispose of items in the sensitive item identification simulation. Sources for all non-native assets used in VirSec can be found in Appendix B.

4.2. Transitional Spaces



Figure 4: Home Room (Left), Boss’s Office (Right).

VirSec forgoes an immersion breaking main menu interface for a home room from which users can: view controls written on a whiteboard (Figure A.5); pick up and touch a key to the front door to transport to the office; throw a pillow onto a bed to quit the application (go to sleep); and place a keyboard onto a table (start working on your PC), which initiates a perspective zoom into the computer monitor – fading into the home PC simulation which displays an introductory simulation context on an interactable desktop (Figure A.1). The ‘office’ and the ‘break room’ (Figure 5) are both transitional spaces *as well as* simulations. Users can walk inside the office before placing a keyboard onto the desk to begin the email simulation. The break room functions as both a space for the sensitive item identification simulation in which the room will be populated with objects (Figure A.2), as well as a transitional space after the email simulation (which appears tidy).



Figure 5: Office Room (Left), Break Room (Right).

4.3. Malicious Email Simulation

Upon transition to the email simulation from the office room, users' perspectives will travel toward the PC monitor with a fade-in to maintain immersion. Users will then be greeted with a realistic and interactable desktop (Figure 6) where they have options to start the email simulation, open the tutorial, or interact with a menu button (Figure A.3). Upon starting the simulation, the browser window will open (as well as an icon in the toolbar) with an already (randomly) populated inbox (Figure 6). The email pool contains an even ratio of all email types; inboxes include **all** emails in the email pool (easily adjusted).



Figure 6: Email Simulation Desktop (Left), Email Simulation Browser Window (Right).

As in section 3.3, users can navigate through emails using the scroll bar and can select emails by aiming their interaction laser and using their respective 'interact' input – opening the email contents. They can choose to reply (takes 1 second), ignore (instant) or report (will be prompted to select a report type – either phishing, malware or financial). The number of emails handled will be displayed for the user; users will have 2 minutes to handle as many emails as they can. They must do so as accurately as possible. Once 2 minutes is up, the number of handled emails is saved for their gameplay loop, and they progress to the appropriate transitional space (Section 4.2 and 4.4).

4.4. Secondary Simulations & Endings

Users who handle < 15 emails progress to the boss's office (Figure 4), where appropriate dialogue will appear (Figure A.4) to indicate their transition to the cleaning simulation. The break room will transform from a transitional space to the sensitive item identification simulation (Figure A.2), where they must correctly identify and dispose of sensitive items by physically throwing them in a trash bin. Players can dispose the following: ID card, written password, sensitive documents, flash drive, as well as 4 benign items. Users are given 1 minute to dispose item and

are penalized for throwing away benign items/leaving sensitive items **after** the simulation, and rewarded for disposing of sensitive items. Users have a *50%* chance to cause a ‘major breach’ if they replied to a **malicious** email, and a *100%* chance if they replied/ignored a **critically malicious** email. If a major breach has been caused, a user’s third stage in their gameplay flow will always be the emergency response simulation (Figure 7). All 9 unique gameplay tree traversals are named and will be displayed (Figure 9) along with their score, providing replay incentive to both achieve all endings, as well as a higher score. The path the player took through the simulations will also be shown on the ending panel.



Figure 7: Emergency Breach Simulation (Left), Ending Example (Right).

5. ‘Debug Log’ Testing

Email content is input via CSV file, which includes both visible content and meta information (email type, handling information) to instantiate email inbox entries, as well as allow scripts to determine the accuracy (or inaccuracy) of player inputs. It is critical that the simulation identifies correct email handling, as well as the severity of incorrect email handling i.e. if simply to deduct score or trigger a major breach. All score updates and general simulation logic are handled by a few central scripts (Figure D.1), in which a Unity3D ‘Debug.Log’ function can be used to print events as they happen (Appendix E) - which can be used to test for correct simulation function throughout. Object collisions play a huge part in VirSec’s gameplay by facilitating transitions between game states. Correct console outputs for all collision tests can be observed below:

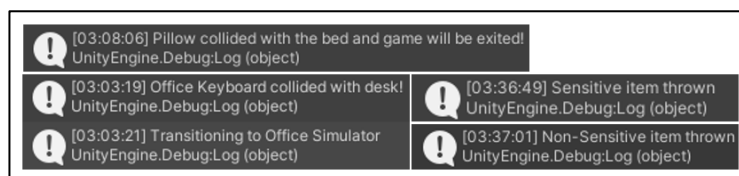


Figure 8: Collision Tests Console Outputs

The emergency breach simulation, having only two outcomes (correct and incorrect answers), can be exhaustively tested (Figure 9). The email simulation has been selectively tested with the following disparate cases: **Incorrectly replying to a normal malicious email; Incorrectly ignoring a critically malicious email; Correctly ignoring a benign unimportant email; Correctly reporting a critically malicious email (including type).**

The console (Figure 9) correctly outputs the corresponding behaviors (note the 'Breach Made' console output is caused by ignoring a critically malicious email).

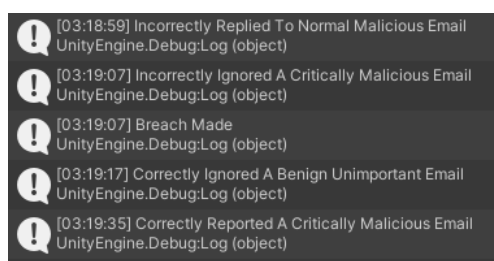


Figure 9: Email Simulation Testing Console Outputs.

6. Conclusion

VirSec is modular in nature. The email simulation lends itself to easy extension – both in type and quantity. The sensitive item identification simulation can be augmented by simply adding more candidate items, and scenarios can be added freely to the emergency breach simulation. VirSec facilitates the addition of new gameplay tree nodes (simulations and intermediary rooms); one could create arbitrary simulations and append them somewhere in the gameplay loop - adding new transitions and endings accordingly. This allows for virtually infinite simulation extensions, with each new one exponentially increasing the possible unique paths and endings one could take through the experience. An addition of a score tracking and/or achievement dashboard would perhaps give users a more tangible incentive for repeat playthroughs – e.g., graphing players' progress over time to incentivize progression. Score tracking information could also be used to give players tailored guidance for improvements in their simulation performance, to provide direction for those struggling, and allow high-performing players to hone their abilities even further. An online leaderboard component could add a further competitive element; users would practice for top scores in both individual simulations and general playthroughs, creating an even stronger replay incentive.

VirSec stands as a pillar of example for what can be done within our means and can be seen as a prototype for novel education, not just in cyber security, but also for other academic areas in which learning methods have stagnated. Whilst virtual reality technology remains a novelty for many, the sands are beginning to shift as hardware developments begin to offer affordable and more portable alternatives. It is time for pedagogy to begin exploring and leveraging advanced technologies for the benefit of both individuals and corporations. Cyber threats are ever evolving; it would seem foolish for our education *on them* to not follow suit.

References

- [1] S. Hasham, S. Joshi, and D. Mikkelsen, "Financial crime and fraud in the age of cybersecurity," McKinsey & Company, 2019.
- [2] S. Al-Janabi and I. Al-Shourbaji, "A study of cyber security awareness in educational environment in the middle east," Journal of Information & Knowledge Management, vol. 15, no. 01, p. 1650007, 2016.

- [3] K. Dorfmüller-Ulhaas and D. Schmalstieg, "Finger tracking for interaction in augmented environments," in Proceedings IEEE and ACM International Symposium on Augmented Reality, IEEE, Oct. 2001, pp. 55-64.
- [4] A. Bendovschi, "Cyber-attacks—trends, patterns and security countermeasures," *Procedia Economics and Finance*, vol. 28, pp. 24-31, 2015.
- [5] V. Bolden-Barrett, "Despite new technologies, 95% of companies still use email as Main Communication Tool," *HR Dive*, URL: <https://www.hrdiver.com/news/despite-new-technologies-95-of-companies-still-use-email-as-main-communic/445490/> (accessed Apr. 3, 2024).
- [6] M. Workman, "Gaining access with social engineering: An empirical study of the threat," *Information Systems Security*, vol. 16, no. 6, pp. 315-331, 2007.
- [7] "ArcGIS dashboards," URL: <https://colpolice.maps.arcgis.com/apps/dashboards/60499304565045b0bce05d2ca7e1e56c>, [Accessed: Jul. 15, 2013]
- [8] E. Hu-Au and J. J. Lee, "Virtual reality in education: a tool for learning in the experience age," *International Journal of Innovation in Education*, vol. 4, no. 4, pp. 215-226, 2017.
- [9] Ö. Delialioğlu, "Student engagement in blended learning environments with lecture-based and problem-based instructional approaches," *Journal of Educational Technology & Society*, vol. 15, no. 3, pp. 310-322, 2012.
- [10] N. Costa and M. Melotti, "Digital media in archeological areas, virtual reality and hyper-tourism," *Sociology Mind*, vol. 2, no. 1, pp. 53-61, 2012.
- [11] J. P. Gee, "Situated language and learning: A critique of traditional schooling," Psychology Press, 2004.
- [12] A. Aljumaiah and Y. Kotb, "The impact of using zSpace system as a virtual learning environment in Saudi Arabia: A case study," *Education Research International*, vol. 2021, pp. 1–12, Dec. 2021. doi:10.1155/2021/2264908
- [13] "Kaspersky Interactive Protection Simulation Virtual Reality," URL: https://media.kaspersky.com/en/enterprise-security/KIPS-VR_Product_Leaflet_Web_A4_EN.pdf, [Accessed: Jul. 20, 2021]
- [14] "Cybersecurity awareness VR for companies," OneBonsai, URL: <https://onebonsai.com/vr-training/cybersecurity-awareness-training-in-vr/>, [Accessed: Jul. 21, 2023]
- [15] "XR Interaction Toolkit: XR interaction toolkit: 2.4.3," XR Interaction Toolkit | 2.4.3, URL: <https://docs.unity3d.com/Packages/com.unity.xr.interaction.toolkit@2.4/manual/index.html>, [Accessed: Aug. 03]
- [16] R. Amin, J. Ryan, and J. van Dorp, "Detecting targeted malicious email," *IEEE Security & Privacy*, vol. 10, no. 3, pp. 64-71, 2011.
- [17] [1] "Trashing: From dumpster diving to data dumps," *Social Engineering*, pp. 69–88, Mar. 2022. doi:10.7551/mitpress/12984.003.0008
- [18] C. Regan, "An investigation into nausea and other side-effects of head-coupled immersive virtual reality," *Virtual Reality*, vol. 1, no. 1, pp. 17-31, 1995.

Appendices

A. Additional Simulation Images



Figure A.1: Home PC simulation text.



Figure A.2: Populated Break Room for Sensitive Item Identification.



Figure A.3: Email Simulation Tutorial.



Figure A.4: Boss's Office Dialogue.

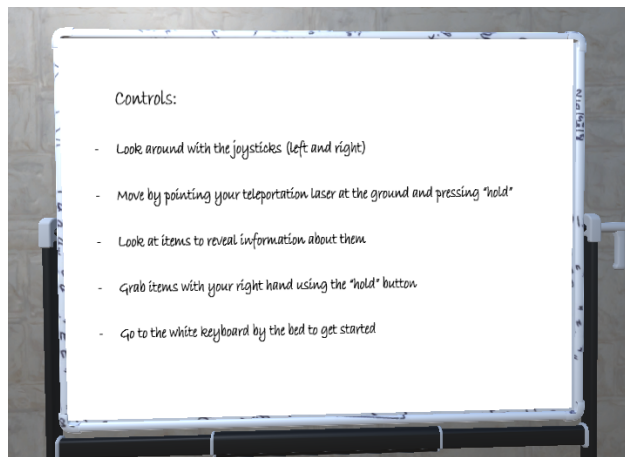


Figure A.5: Home Room Whiteboard.

B. Asset Resources

“CGTrader”, URL: <https://www.cgtrader.com/>

“TurboSquid”, URL: <https://www.turbosquid.com/>

“Poly Haven”, URL: <https://www.polyhaven.com/>

C. Simulation Scoring

The scores below were set intuitively, and reward players for identifying the exact nature of emails and handling them appropriately. Score change potential is greatest with the most malicious emails i.e. replying to the most dangerous emails incur the highest penalty, whilst (correctly) reporting them provide the greatest reward. Players will incur a 100 point penalty for causing a breach, but can make up 40 points by correctly handling it.

Table 2

Email Simulation Scoring

	Replied	Ignored	Reported	Correct Report Type
Benign (Unimportant)	+5 score	+10 score	-5 score	+15 score
Benign (Important)	+10 score	-20 score	-15 score	+15 score
Malicious (Normal)	-30 score	-10 score	+10 score	+15 score
Malicious (Critical)	-50 score	-30 score	+20 score	+15 score

Sensitive Item Identification Simulation scoring:

Sensitive Item Thrown: **+10 Score**

Non-Sensitive Item Thrown/Left: **-10 Score**

Emergency Response Simulation scoring:

Breached Caused: **-100 Score**

Correct Breach Answer: **+40 Score**

D. Object/Script Diagrams

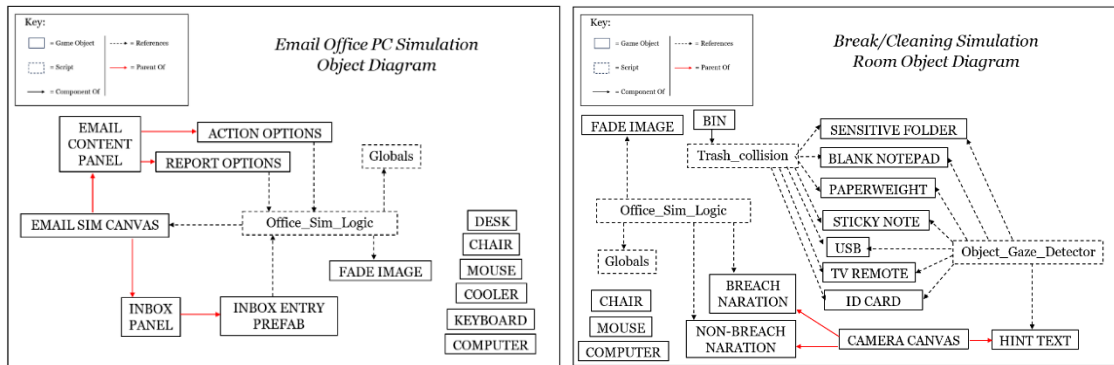


Figure D.1: Object/Script Structure Diagrams

E. Testing Code Snippets

```

else if (currentMethod == "3" && currentImportance == "c")
{
    Debug.Log("Incorrectly Ignored A Critically Malicious E
if (Random.value < 0.5f)
{
    Debug.Log("Breach Made");
    Globals.severe_error = true;
}
}
    
```

Figure E.1: Debug.Log Email Handling Example

```

if (collision.gameObject.CompareTag("Office_Keyboard"))
{
    Debug.Log("Office Keyboard collided with desk!");
    key.transform.position = new Vector3(-4.075f, 4.603f, 2.921f);
    Globals.chosen_office_sim = true;
}
    
```

Figure E.2: Debug.Log Object Collision Example