Cyber Play

Final Report (01/10/2024)

MSC Computing and IT Management

STUDENT: ROBERT KENNARD (0941023)

SUPERVISOR: DR CATHERINE TEEHAN

MODERATOR: DR YULIA CHERDANTSEVA

Abstract

The Cyber Play project, developed in collaboration with Bridgend College's STEAM Academy, is an interactive educational theatre experience designed for pre-GCSE students in Years 9 and 10. This 45-minute production focuses on teaching key topics such as online safety, cybersecurity, and cyber forensics. By allowing the audience to influence the storyline, the project promotes active engagement and learning through participation.

Aligned with the Welsh Digital Competence Framework (DCF), Cyber Play is supported by structured classroom resources, including lesson plans and follow-up activities. These ensure that the learning objectives extend beyond the theatre, reinforcing critical thinking and responsible online behaviour.

The project leverages the Twine platform to create an interactive storyline that responds to audience input. This fusion of theatre and digital technology raises awareness of cybersecurity issues and promotes understanding of online safety and ethics among young learners.

Acknowledgements:

I would like to express my deepest gratitude to my partner, Mirna Amoedo, whose unwavering strength and encouragement have been a constant source of inspiration, even while facing a cancer diagnosis this year. Her resilience has been truly inspiring.

I extend my sincere thanks to Dr. Catherine Teehan, my supervisor, for her invaluable guidance, and support throughout the development of this project.

Lastly, I wish to acknowledge Bridgend College's STEAM Academy for the opportunity to work on this innovative project and Cardiff University for their academic support.

Table of Contents

Table of Images

Appendix

Introduction

The Cyber Play project aims to create an interactive, narrative-driven educational tool using Twine to teach cybersecurity concepts to pre-GCSE students. Complemented by classroom materials, including a scheme of work, lesson plans, and resources, the project is designed to support educators in delivering comprehensive and engaging cybersecurity education. Its primary goal is to enhance students' digital competence and equip them with the skills needed to navigate the increasingly complex digital landscape.

The project addresses the Digital Competence Framework (DCF) in the Curriculum for Wales, which emphasises online safety, cyber threat recognition, and responsible data handling (Welsh Government 2020). Aligned with the Principles of Progression in Science and Technology, Cyber Play fosters problem-solving, resilience, and deeper conceptual understanding by connecting learning to real-world cybersecurity scenarios.

Current resources often fail to engage students effectively, being static or outdated (TeachComputing.org 2024). This project fills that gap by providing a more immersive, interactive approach. Twine was selected for its non-linear storytelling capabilities, allowing students to make decisions that impact the narrative. The play covers phishing, malware, and network traffic analysis, offering students the chance to collect clues, interact with suspects, and solve cybersecurity challenges.

Mini-games, such as terminal simulations and timed challenges, enhance engagement and skill development.

The 8-week scheme of work, lesson plans, and resources extend learning, encouraging deeper exploration of cybersecurity topics through scenario-based activities and critical reflection. This structured curriculum provides continuity and practical application of cybersecurity skills.

By combining storytelling with game-based learning, Cyber Play makes complex topics like phishing and data protection accessible and engaging, equipping young learners with essential skills for navigating the digital world securely.

Background

Research

Digital Competence Framework (DCF) and AoLE Science & Technology

The Digital Competence Framework (DCF) is a key part of the Curriculum for Wales, focusing on online safety, cyber threat recognition, responsible data handling, and ethical digital technology use. Despite its importance, many current educational resources remain static and fail to engage students in meaningful ways (TeachComputing.org 2024), leading to difficulty in internalising and applying concepts.

The Area of Learning and Experience (AoLE) for Science and Technology highlights the need for practical digital skills and problem-solving (Hwb [no date]), further reinforcing the significance of digital literacy. Cyber Play addresses this gap by aligning with both the DCF and AoLE, providing students with an interactive, narrative-driven experience that transforms passive learning into active participation. By simulating real-world cybersecurity scenarios like phishing detection and network traffic analysis, students can apply theoretical knowledge in practical settings, fostering critical thinking and decision-making.

Cyber Play contributes to the broader educational goals of the Wales National Mission and the Curriculum for Wales, focusing on lifelong learning, active citizenship, and employment readiness.

Game-based Learning

Game-based learning (GBL) is a proven educational approach that enhances engagement and motivation among learners. The interactive nature of games offers a platform for problem-solving and critical thinking skills, which are essential in cybersecurity education. Cyber Play uses GBL principles by incorporating interactive challenges which encourage students to actively explore cybersecurity concepts. By allowing students to make decisions, face challenges, and learn from their mistakes within a game environment, we ensure that abstract topics become tangible and relatable.

Cyber Play ensures students are not only thinking critically but are also emotionally invested and engaged in the learning process. This aligns with research showing

that GBL can foster higher levels of engagement, promote resilience through safe failure, and encourage learners to take an active role in their education (Plass et al., [no date]).

Storytelling and Narrative Structure in Cyber Play

Storytelling is a powerful method for conveying complex information, transforming abstract concepts into real-life scenarios. Cyber Play uses interactive storytelling to immerse students in cybersecurity challenges where they actively participate, role-play, and make decisions that directly impact the narrative. This method fosters a deeper understanding of cybersecurity principles by allowing students to experience the consequences of their actions, aligning with constructivist theory (Educational Technology, 2021), which emphasises learning through active, contextualised knowledge construction.

The non-linear narrative structure of Cyber Play differentiates it from traditional linear teaching methods. Students navigate branching paths, make decisions, and face real-time consequences. This flexibility encourages critical thinking and cognitive engagement as they explore multiple cybersecurity strands. Student experience is shaped by the choices they make, which mirrors real-world decision-making in cybersecurity.

While Cyber Play loosely follows elements of the 7-point story structure (Art of Narrative 2022), it intentionally avoids a strict adherence to this framework due to its semi-random, non-linear nature. Instead the game allows students to influence the story's progression, reinforcing the game-based learning approach where exploration and critical thinking are central.

Beyond cybersecurity, the storytelling approach promotes cross-curricular skills such as literacy, numeracy, and social interaction, aligning with the goals of the Curriculum for Wales (Hwb, [no date]). A key feature is the “failure by design” approach, where students are encouraged to take risks, make mistakes, and learn from them in a safe environment. This enhances resilience, fostering deeper, more meaningful learning outcomes.

Literature Review

Introduction

In today's digital age, cybersecurity education is crucial, especially for younger students who frequently engage with online platforms. This literature review examines how key methodologies, social engineering concepts, game-based learning (GBL), and story-based learning (SBL), can be effectively integrated into cybersecurity education. The review also explores their alignment with the Digital Competence Framework (DCF) and Routes for Learning (RfL), laying the foundation for Cyber Play.

Social Engineering in Cybersecurity Education

Social engineering is a critical and evolving threat in cybersecurity, exploiting human vulnerabilities to bypass technical defences. According to Wang, Sun, and Zhu (2021), social engineering "poses a serious security threat to infrastructure, user, data, and operations of cyberspace," with attacks becoming more sophisticated and harder to detect. The origins of social engineering trace back to the Phreak phase (1974-1983), where techniques like pretexting were used to deceive individuals into divulging sensitive information.

Today, social engineering encompasses tactics such as phishing, blagging, and shoulder surfing. Phishing, one of the most widespread methods, tricks individuals into revealing personal information by posing as trustworthy through seemingly legitimate emails or websites. Wang et al. (2021) emphasise that "the success rate

and efficiency of social engineering attacks are increasing," driven by advancements in machine learning that exploit open-source intelligence.

Blagging (pretexting) creates fabricated scenarios to deceive individuals into providing confidential information. Shoulder surfing, a more direct attack, involves physically observing someone entering sensitive data, such as a password or PIN. This technique highlights the need for physical security awareness, an often-overlooked aspect of cybersecurity. Name generator attacks, common on social media, gather personal information through quizzes or surveys, particularly targeting younger users.

To address these threats, Cyber Play integrates social engineering scenarios into its narrative, offering students practical, hands-on experience in identifying and responding to these threats. This approach not only reinforces theoretical knowledge but prepares students for real-world cybersecurity challenges.

Game-Based Learning (GBL)

Game-based learning (GBL) is an effective educational strategy that promotes learning objectives through engaging gameplay. According to Marques and Pombo (2021), "GBL leverages the engaging nature of games to make education interactive and enjoyable." In Cyber Play, GBL is used to raise motivation by incorporating challenges that promote problem-solving and critical thinking, keeping students actively involved in the narrative.

GBL is particularly powerful because it uses failure as a learning tool. Traditional classrooms may discourage participation due to fear of failure, but games provide a

safe space for students to take risks and experiment without serious consequences (Plass et al., no date). This model encourages mastery and resilience, concepts integral to Cyber Play.

GBL also helps reduce anxiety often associated with assessments. Marques and Pombo (2021) note, "Games can reduce stress and fear tied to knowledge assessments, making learning more enjoyable." This makes GBL ideal for teaching complex subjects like cybersecurity.

Finally, GBL's flexibility allows content to be adapted to diverse learning styles, ensuring all students benefit regardless of their prior knowledge or experience with digital technologies.

Story-Based Learning (SBL)

Story-based learning (SBL) engages students by using narrative to enhance understanding, grounded in constructivist principles where knowledge is actively constructed (Türkben & Karaca, 2018). This approach is particularly effective for teaching abstract concepts, providing memorable contexts.

Research shows that SBL improves student engagement and retention of information. As Theroux (2020) notes, "Positive student feedback about the use of stories…showed the effectiveness of this teaching strategy." By incorporating SBL, students can internalise cybersecurity concepts through active participation and reflection.

SBL also allows students to explore complex scenarios in a safe environment, where they experience the consequences of their decisions and learn from mistakes. This reinforces both engagement and the practical application of cybersecurity skills.

In Cyber Play, SBL creates a narrative-driven experience, immersing students in real-world cybersecurity scenarios. This deepens their understanding of cybersecurity challenges and develops the skills they need to navigate them.

Digital Competence Framework (DCF) and Routes for Learning (RfL)

The Digital Competence Framework (DCF) integrates essential digital skills into education, focusing on digital literacy, online safety, and information management. Cyber Play aligns with the DCF by teaching students how to navigate the digital world safely and defend against cyber threats.

The DCF's core strands, citizenship, interactions and collaboration, producing, and data and computational thinking (Welsh Government 2020), are enhanced by Cyber Play through hands-on experiences with cybersecurity scenarios. The citizenship strand, in particular, is addressed as students engage with scenarios involving ethical digital behaviour and cybersecurity breaches, fostering informed digital citizenship.

Cyber Play also incorporates the Routes for Learning (RfL) framework to ensure inclusivity for students with significant learning difficulties. By adapting the project to align with RfL principles, the narrative and interactive elements can be tailored to

meet diverse learning needs. Adjustments in complexity ensure that all students, including those with additional needs, can comprehend and engage with cybersecurity concepts.

Integrating both the DCF and RfL frameworks, Cyber Play becomes an inclusive tool for teaching critical skills, making it adaptable for mainstream and diverse learners alike.

Problem

Challenges in Teaching Cybersecurity Concepts

The integration of digital technologies has heightened the need for effective cybersecurity education, but teaching these concepts presents challenges. Terms like "phishing" and "social engineering" are abstract and distant from students' everyday experiences, making them difficult to grasp. Traditional, passive teaching methods, lectures and textbooks, fail to engage students or provide hands-on learning opportunities.

Cyber Play addresses this by using gamification to enhance engagement. Features like a clue-tracking system reward students for identifying cybersecurity concepts, promoting a sense of achievement. This aligns with motivational theories, suggesting gamification boosts engagement and persistence.

The Digital Competence Framework (DCF) presents another challenge, particularly for pre-GCSE students at progression steps 3 and 4. These students are still developing foundational digital literacy and critical thinking skills, making advanced cybersecurity topics difficult to grasp. Cyber Play addresses this by scaffolding instruction to make cybersecurity concepts accessible, aligning with the broader goals of the Curriculum for Wales, which emphasises digital competence and cross-curricular skills. These include responsible online behaviour and understanding digital footprints, essential for developing capable learners.

Identifying the Target Audience

Cyber Play is designed for students in Years 9-10, a key stage where their digital independence increases, making them more vulnerable to cyber threats like phishing, malware, and social engineering. As they engage more with social media, online gaming, and other platforms, these risks become more pronounced.

At this age, students are forming complex online behaviours and digital identities, making it essential to teach them cybersecurity concepts that protect them and encourage responsible behaviour. They are cognitively ready to grasp the real-world implications of cyber threats but still benefit from engaging, practical learning methods that make these concepts accessible.

Cyber Play leverages this by offering an interactive, narrative-driven experience, presenting real-world cybersecurity challenges in a game-like format. This helps students not only understand these threats but also apply practical strategies to protect themselves and others.

Approach

Methodologies

The Lean Canvas model guided the development of Cyber Play, helping to define educational goals, engagement strategies, and execution plans. Further details of this framework are provided in the appendix.

Problem

Cybersecurity education often relies on passive, lecture-based methods, leading to disengagement and poor retention. Students struggle to connect theoretical knowledge with practical, real-world applications.

Solution

Cyber Play offers a gamified, narrative-based solution. It immerses students in real-world scenarios, enabling active engagement and hands-on learning, rather than passive information absorption.

Unique Value Proposition

Cyber Play provides an interactive learning environment where students make critical decisions and experience real-world consequences, offering both theoretical and practical knowledge.

Key Metrics

Success can be evaluated through engagement (post-play surveys and observations), knowledge retention (surveys), and long-term behavioural changes (follow-up surveys assessing digital habits).

Customer Segments

Targeting Year 10 students, Cyber Play appeals to educators seeking innovative, interactive tools that align with curriculum goals and foster digital literacy.

Channels

The project is adaptable to both live school performances and classroom activities, offering flexibility based on educational needs.

Cost Structure and Revenue Streams

Initially developed as a free resource, Cyber Play has future potential in the EdTech sector. Development costs were minimal, relying on tools like Twine and Mentimeter, making it scalable.

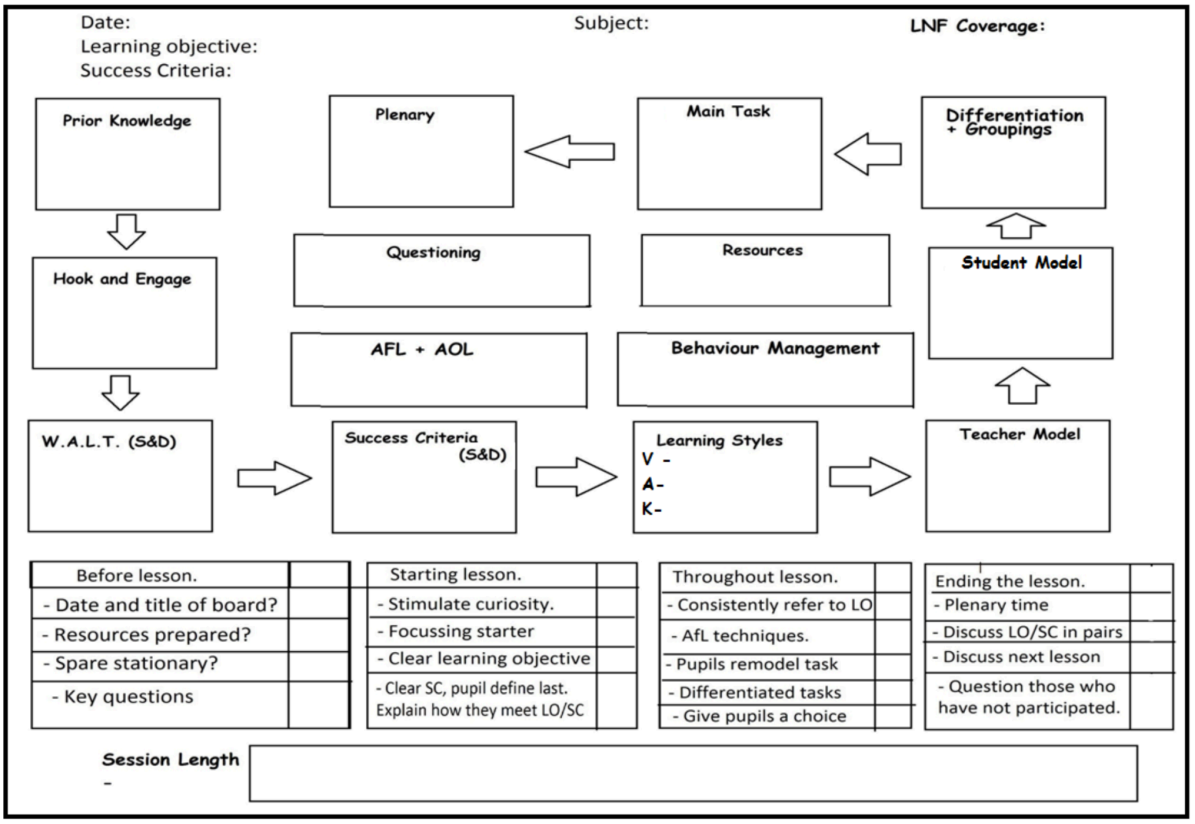
7-Stage Story Structure

The design of Cyber Play follows a 7-stage story structure but is set apart by its semi-random, non-linear format. Unlike traditional narratives, the play consists of short, interactive branches where students actively engage in real-time cybersecurity scenarios. These problem-solving activities challenge students to think critically and make quick decisions, simulating the fast-paced nature of real-world cybersecurity.

The lessons are guided by the "RoadMap for an Outstanding Lesson," a proven teaching framework developed by Pencoed Primary School and one I've successfully used since 2015. This framework ensures consistency, structure, and effectiveness, creating a cohesive learning experience. My own teaching, evaluated as

"Outstanding," and Pencoed Primary School's strong feedback from Ofsted highlight the impact of this approach.

The play targets Year 10 students, who are expected to have a basic understanding of cybersecurity from the Digital Competence Framework (DCF). Cyber Play pushes students to apply this foundational knowledge in dynamic scenarios where their decisions directly influence the narrative, turning them into active participants.



Roadmap to an outstanding lesson, Pencoed Primary School

Phishing, Network Analysis, and Malware Lessons:

Each branching path, covering phishing, malware, or network traffic analysis, serves as a mini-lesson integrated into the broader narrative to maintain engagement. Rather than immediate evaluation, the focus is on exploring the consequences of different decisions.

Phishing Lesson: Students encounter a phishing email scenario, identifying suspicious elements and exploring the consequences of actions like clicking on links or reporting emails, deepening their understanding of phishing techniques.

Network Traffic Analysis Lesson: Students analyse traffic logs to detect suspicious activities, reinforcing network security concepts and the importance of monitoring unauthorised access.

Malware Lesson: In a simulated malware outbreak, students make decisions on how to contain the infection and protect data, mirroring real-world cybersecurity responses and applying their knowledge dynamically.

Mr. Luddite is vital for the play as he acts as the voice of exposition when the Task Force are speaking in technical terms, Luddite’s exposition is designed to bring the dialogue down to a Year 10 level. Mini-plenary points, acting as AFL moments, inspired by the "RoadMap for an Outstanding Lesson" check for overall understanding, allowing the narrative to flow while prompting reflection on key concepts. This is repeated in the Powerpoints and resources.

Twine Application

Cyber Play was developed using Twine, an open-source tool for building interactive, non-linear narratives. Twine's flexibility enabled the creation of branching narrative paths that align with the play’s emphasis on critical thinking and decision-making. Its structure mirrors the real-world complexity of cybersecurity situations, where a single decision can lead to vastly different outcomes.

Twine’s browser-based functionality made the play easy to implement in classroom environments, where software installations might be limited. Its integration ensured a seamless experience for both students and educators, supporting the interactive and scenario-based learning approach of the play.

Application of the Approach

Cyber Play is designed to facilitate scenario-based learning through interactive lessons embedded within the narrative. These modules present real-time problem-solving exercises where students assess situations, weigh options, and make decisions based on their understanding of cybersecurity.

The play emphasises critical thinking over rote knowledge. Students face choices that mimic real-world cybersecurity challenges, such as handling phishing attacks or responding to malware infections. Each decision encourages students to apply their knowledge in dynamic, real-world scenarios. Reflective moments prompt students to consider the reasons behind correct or incorrect choices.

After the play, classroom activities revisit these cybersecurity concepts through scenario-based learning and portfolio-building exercises. The scheme of work aligns with the themes introduced in Cyber Play, allowing students to explore these topics in a structured setting. Teachers act as moderators, guiding discussions and group activities, emphasising student-driven exploration and problem-solving over conventional worksheets and lectures.

Survey Techniques

The survey methodology for Cyber Play and its classroom lessons was designed to assess both immediate engagement and long-term learning outcomes. Given the real-world scenarios presented in the play, surveys were tailored to capture insights into how students processed and applied cybersecurity knowledge.

Immediate Feedback Surveys to be conducted after each play session (see appendix), collecting qualitative data on engagement, learning outcomes, self-reported confidence in applying knowledge, and the effectiveness of decision-making. These surveys also allowed for open-ended suggestions for improvement.

Pre- and Post-Lesson Surveys focused on evaluating students' knowledge retention and understanding. A pre-survey gauged existing knowledge, while a post-survey measured how well students retained the information and their confidence in applying what they learned.

Long-Term Follow-Up Surveys to be conducted several weeks later to evaluate retention of core concepts, behavioural changes (such as improved password practices and phishing detection), ongoing confidence in handling real-world cybersecurity threats, and continued interest in the subject.

Teacher Feedback plays a crucial role, providing insights into how students engaged with content, how they applied concepts in class, and offering recommendations for improvement.

This staggered approach to surveys ensures meaningful data can be collected on how well students engage with the material, apply their knowledge, and adjust their behaviour. Classroom follow-up lessons, focusing on critical thinking and portfolio-building activities, reinforced the outcomes of Cyber Play.

Ethical Considerations in Cybersecurity Education

The incorporation of social engineering techniques in educational settings raises important ethical concerns, particularly in line with frameworks like the ACM Code of Ethics (ACM 2018) and the BCS Code of Conduct (BCS 2023). While Cyber Play aims to educate students about cybersecurity threats, care must be taken to ensure simulations of attacks do not cause unnecessary distress and that data is handled responsibly.

In line with GDPR (European Union 2016) and the ACM’s principle of avoiding harm, data collected during Cyber Play sessions will be securely stored and promptly

deleted. This respects participants' privacy, as outlined by the ACM’s guidelines on responsible data collection and storage. The use of real-world scenarios, such as mimicked phishing attacks, is carefully designed to educate students without causing undue anxiety. Ethical codes from both the ACM and BCS emphasise the need to minimise harm, ensuring that students are aware they are participating in a controlled, safe environment.

The BCS Code of Conduct requires the protection of private information from misuse, which Cyber Play ensures through secure storage and the timely deletion of data. Future iterations of the play will strengthen this ethical framework by providing educators with clear guidelines, including debriefing sessions to encourage reflection on the ethical aspects of cybersecurity.

Design

Narrative Structure and Engagement

The play unfolds across several key stages, each focusing on a distinct cybersecurity topic, including phishing, malware, and network traffic analysis. Each branch of the narrative offers unique challenges that encourage the audience to think critically and solve problems.

Key Stages of the Play:

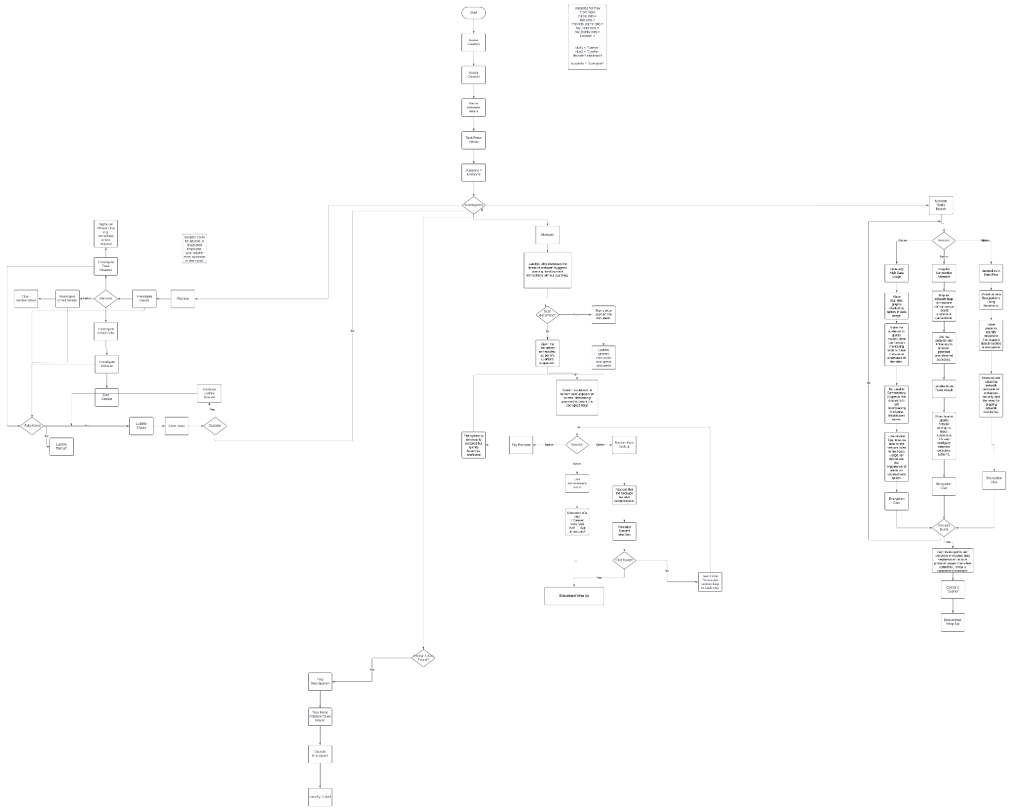
1. Introduction and Avatar Creation: The play begins with an interactive avatar creation process, subtly teaching the audience about the risks of sharing personal information online. The task force enters, announcing a security breach, with everyone a suspect.
2. Branching Investigations: The audience uncovers an initial clue, a Caesar Cipher, which unlocks three investigation paths:
    - Phishing: Examining suspicious emails for signs of phishing attempts.
    - Malware: Investigating an attack, where decisions about backups, and ransom payments must be made.
    - Network Traffic Analysis: The audience analyses traffic logs and identifies anomalies, racing against a timer to stop a data breach.
3. Dynamic Decision-Making: Each branch requires the audience to make decisions that influence the outcome of the investigation. Correct decisions lead to clues, while incorrect choices may delay progress or lead to false leads. This mechanic encourages critical thinking and problem-solving.

4. Decryption and Final Puzzle: After gathering sufficient clues, the final puzzle is unlocked—a Cipher that, once decrypted, reveals the identity of the perpetrator of the cyberattack.
5. Resolution and Educational Wrap-Up: The play concludes with the task force summarising the key cybersecurity lessons learned, reinforcing the importance of online safety.

See Appendix for the full outline of the play as used during the design phase.

Cyber Play flowchart

The flowchart served as a foundational tool for designing and implementing Cyber Play, guiding the development of branching narratives, decision points, and interactive elements. This visual roadmap mapped out each investigative path, phishing, malware, and network traffic analysis, and their corresponding consequences, ensuring a cohesive structure. By clearly outlining how decisions would influence the narrative, the flowchart allowed for a logical progression that mirrored real-world cybersecurity scenarios. As the project evolved, the flowchart helped in managing the complexity of the branching paths and ensuring that each pathway delivered educational value, culminating in a meaningful learning outcome. Although the project expanded beyond the initial flowchart, adding new branches and interactive elements like mini-games, the core framework it established remained crucial in organising the project.



Cyber Play Flowchart

Lesson Design and Integration with DCF

The design of the lessons followed a scenario-based, portfolio-building approach, with each lesson building on the narrative structure outlined by the flowchart. The formative assessments embedded within Cyber Play allow students to reflect on their decisions and apply critical thinking. These assessments are not limited to testing factual knowledge but are designed to evaluate students' ability to navigate complex cybersecurity scenarios.

In alignment with the Digital Competence Framework (DCF), the follow-up lessons extend beyond the interactive play, providing structured opportunities to revisit and deepen students' understanding of cybersecurity concepts. These lessons are detailed in the scheme of work and focus on critical engagement with real-world

digital safety practices. Hands-on activities such as scenario-based exercises enable students to develop practical cybersecurity skills, ensuring that knowledge retention and real-world application are emphasised. The overall goal of the lessons is to foster digital competence while supporting the Principles of Progression by encouraging independent learning, critical thinking, and problem-solving.

Implementation

Implementation Overview

The implementation of Cyber Play is divided into five key focus areas: Introduction, Voting, Malware, Phishing, and Network Traffic. Additionally, the play features General Implementation, Styling, and Lesson Resources. Each section plays a critical role in engaging students through immersive, real-time scenarios designed to challenge their problem-solving and critical thinking skills.

The Introduction familiarises students with the setting and key suspects, while the Voting system lets the audience direct the investigation. The Malware, Phishing, and Network Traffic branches offer distinct cybersecurity challenges, each incorporating interactive elements. The play concludes by evaluating the audience's grasp of cybersecurity concepts.

General Implementation

Story Background

Cyber Play was developed using Twine’s Harlowe engine due to its simplicity for creating interactive, non-linear narratives. However, as development progressed, Harlowe's limitations in managing complex variables and interactive elements became evident. By that stage, over 100 pages of content had been developed, making a transition to a more advanced engine, like SugarCube, impractical.

To address these limitations, custom JavaScript was integrated to manage more sophisticated interactions that Harlowe couldn’t handle. This allowed for the continuation of core features. While Harlowe presented constraints, its ease of use supported rapid early-stage prototyping, making it valuable for initial development despite its technical limitations.

General Overview of StoryInit in Cyber Play

The StoryInit node in Cyber Play plays a crucial role in initialising global variables that track the player's progress and decisions. These variables, such as $phishing_completed, clue discovery, and suspect identification, ensure player actions persist across the branching narrative. By setting these variables upfront, the game can dynamically adapt the storyline based on player interactions.

In Twine’s Harlowe engine, StoryInit manages task completion, switching variables like $phishing_completed from false to true when the player successfully identifies a phishing attempt. This impacts future scenarios, making them more responsive to player outcomes.

Arrays like viperWormStories[] further enhance the narrative, adding dynamic content related to cyber threats and increasing immersion.

Code snippets embedded in the dissertation illustrate how these variables are initialised and managed, ensuring the game remains responsive to player choices.

```
(set: $cluesFound to 0)
(set: $foundClues to (array:)) <!-- An array to track found clues -->

(set: $clue1_found to false) <!-- Clue 1: Caesar Cipher -->
(set: $clue2_found to false) <!-- Clue 2: Suspicious IP Address -->
(set: $clue3_found to false) <!-- Clue 3: USB Device -->
(set: $clue4_found to false) <!-- Clue 4: Encryption Tools -->
(set: $clue5_found to false) <!-- Clue 5: Fake Phishing Email -->
(set: $clue6_found to false) <!-- Clue 6: Unusual Login Attempts -->
(set: $clue7_found to false) <!-- Clue 7: Compromised Files -->
(set: $clue8_found to false) <!-- Clue 8: First Pet Name -->

(set: $clue9_found to false) <!-- Clue 9: Strange Software Installed -->
(set: $clue10_found to false) <!-- Clue 10: Anonymous Email -->
(set: $clue11_found to false) <!-- Clue 11: Favorite Hobby -->
(set: $clue12_found to false) <!-- Clue 12: Decryption Key (Shift of 3) -->
(set: $clue13_found to false) <!-- Clue 13: Hidden Message in Source Code -->
)
(set: $clue14_found to false)

(set: $suspectsFound to 0) <!-- Initialize suspects found count -->
(set: $suspect1_found to false) <!-- Suspect 1: Alex Johnson -->
(set: $suspect2_found to false) <!-- Suspect 2: Jamie Parker -->
(set: $suspect3_found to false) <!-- Suspect 3: Emily Davis -->
(set: $suspect4_found to false) <!-- Suspect 4: Thomas Reed -->
(set: $suspect5_found to false) <!-- Suspect 5: Sarah Lee -->
(set: $suspect6_found to false) <!-- Suspect 6: Robert Brown -->
(set: $suspect7_found to false) <!-- Suspect 7: Luddite -->
(set: $suspect8_found to false) <!-- Suspect 8: EVERYONE -->
```

StoryInit Code Snippet for Variable Initialization

```
(set: $viperWormStories to (a:
    "**BREAKING NEWS!** Scientists warn that **ViperWorm 2.0** doesn't just destroy computers—it's evolved to **hack your brainwaves** and turn you into a mindless zombie! Experts recommend wearing a **tinfoil hat** at all times to block the virus from controlling your mind.",
    "Security experts are in **shock** as the **ViperWorm virus** has unleashed an animated **snake emoji** that **slithers across your screen** and eats all your important files! It even hisses every time it gobbles up a document. Once your data is eaten, the snake vanishes, leaving only chaos behind.",
    "In its **latest mutation**, ViperWorm has found a way to turn your entire computer into a **real snake**! Users have reported their laptops **shedding their casings** and slithering away. If your computer is feeling scaly, DO NOT approach! Experts advise locking your devices in terrariums.",
    "The latest version of ViperWorm has started creating **wormholes** on infected computers, **sucking up all data** and transporting it to another dimension. Once your files are gone, they're gone for good! No firewall can stop it, as it seems to transcend time and space."
))
```

Viperworm Array

TestSuspectNode

```
<!-- StoryInit to map the suspectNum to the correct suspect with some encrypted values -->
(if: $suspectNum is 1)[
  (set: $perp to "Doha Mrkqvrq") <!-- Alex Johnson encrypted -->
  (set: $perpRole to "Frpsxwhu Whfkqlfldq") <!-- Computer Technician encrypted -->
  (set: $perpDOB to "01/05/1980") <!-- Date of Birth -->
  (set: $perpPetName to "Rex")
  (set: $perpMaidenName to "Taylor")
  (set: $perpFavoriteColor to "Blue")
  (set: $perpLoginTime to "Late Nights")
  (set: $perpHobby to "Programming")
  (set: $perpCipherKey to 3) <!-- Caesar's Cipher decryption number -->
  (set: $perpHackerName to "ShadowByte") <!-- Hacker Name -->
]
(else-if: $suspectNum is 2)[
  (set: $perp to "Ofrnj Ufwpjw") <!-- Jamie Parker encrypted -->
  (set: $perpRole to "Xdxyjr Firnsnxywfytw") <!-- System Administrator encrypted -->
  (set: $perpDOB to "12/11/1975") <!-- Date of Birth -->
  (set: $perpPetName to "Milo")
  (set: $perpMaidenName to "Clark")
  (set: $perpFavoriteColor to "Red")
  (set: $perpLoginTime to "Evenings")
  (set: $perpHobby to "Gaming")
  (set: $perpCipherKey to 5) <!-- Caesar's Cipher decryption number -->
  (set: $perpHackerName to "NetPhantom") <!-- Hacker Name -->
]
```

Initialising Suspects

The TestSuspectNode manages suspect information, assigning encrypted personal characteristics to each suspect, including names, roles, and clues that players must decrypt. The node creates dynamic suspect profiles to engage players in solving the mystery.

Variables such as $perp, $perpRole, and $perpCipherKey are initialised to represent encrypted data, for example:

(set: $perp to "Doha Mrkqvrq") <!-- Alex Johnson encrypted -->

(set: $perpRole to "Frpsxwhu Whfkqlfldq") <!-- Computer Technician encrypted -->

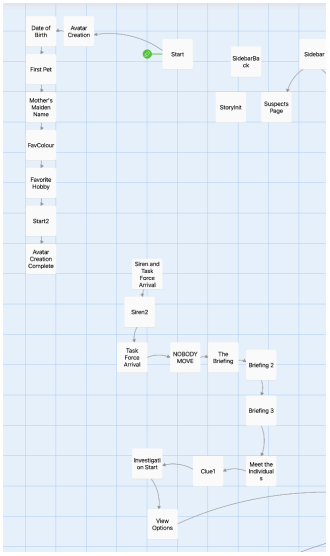
(set: $perpCipherKey to 3) <!-- Caesar's Cipher decryption key -->

This setup allows players to decrypt clues like names or roles. Each suspect has a unique cipher key:

(set: $perpCipherKey to 5) <!-- Different cipher key for another suspect -->

Initially, I considered using arrays or dictionaries for efficient data storage, but the limitations of Twine's Harlowe engine, particularly its difficulty in integrating with advanced data structures, led to reliance on individual conditions. While less scalable, this method proved reliable for the current project scope and maintains narrative flexibility.

Introduction



Introductory Nodes in Twine

The play begins with students expecting a standard cybersecurity awareness assembly. This mundane introduction lulls the audience into a sense of familiarity before the narrative takes an unexpected turn.

Avatar Creation Process

To enhance audience participation, the actors invite viewers to create avatars using an in-game questionnaire. Originally, Mentimeter was planned for data collection, but technical challenges with Twine integration led to this alternate approach. The questionnaire gathers personal details like name, date of birth, pet’s name, mother’s maiden name, favourite colour, hobby, and a chosen number.

Inspired by TeachComputing.org (TeachComputing.org 2024)., these questions mirror real-world security practices, highlighting how personal information is often

exploited in phishing scams. Audience responses are stored as variables and used to personalise "Suspect 7," representing the audience within the narrative.

```
<p class="speech"><b>Emma Smith:</b> "Lastly, what's your favorite hobby?"
</p>
{
  <!-- Input for the favorite hobby -->
  (input-box: bind $userHobby)
}
{
  <!-- Submit button to validate input -->
  (link-repeat: "Submit")[
    (if: $userHobby is not "")[
      (set: $suspect7Hobby to $userHobby) <!-- Store the hobby in
suspect7Hobby variable -->
      (show: ?nextLink) <!-- Reveal the link to the next passage --
>
    ]
    (else:)[
      (alert: "Please enter your favorite hobby.")
    ]
  ]
}
```

Initialising Character 7

```
(else-if: $suspectNum is 7)[
  <!-- Suspect 7: Audience Member (Details assigned at the
beginning of the play) -->
  (set: $perp to $userName) <!-- Name entered by the audience -->
  (set: $perpRole to "Audience Member") <!-- A generic role for
the audience -->
  (set: $perpDOB to $userDOB) <!-- Date of Birth entered by the
audience -->
  (set: $perpPetName to $userFirstPet) <!-- Pet name entered by
the audience -->
  (set: $perpMaidenName to $userMotherMaidenName) <!-- Mother's
maiden name entered by the audience -->
  (set: $perpFavoriteColor to $userFavoriteColor) <!-- Favorite
color entered by the audience -->
  (set: $perpLoginTime to "Unknown") <!-- Optional, can set this
to another question response -->
  (set: $perpHobby to $userHobby) <!-- Hobby entered by the
audience -->
  (set: $perpCipherKey to 7) <!-- Caesar's Cipher decryption
number (from the number entered by the audience) -->
  (set: $perpHackerName to "Audience4Lyfe") <!-- Hacker Name -->
]
```

Setting Character 7 Variables

Purpose of Avatar Creation

1. **Engagement**: Creating avatars makes the play more immersive.
2. **Cybersecurity Lesson**: This process subtly demonstrates the risks of sharing personal data, modelling tactics used in phishing and social engineering.

Perpetrator choice

After avatar creation, participants select a number between 1 and 8, which is stored in the variable $suspectNum. This variable assigns one of eight possible perpetrators, each with a unique backstory, adding an element of variability to each playthrough. Due to technical constraints, the play is currently limited to these 8 suspects.While live polling tools like Mentimeter can display real-time information directly into platforms like Zoom or PowerPoint, dynamically transferring this data into Twine presented a significant challenge.In future iterations, a proprietary system could be developed to seamlessly transfer real-time polling data directly into Twine. This would allow for more variation in suspects with more Audience Members being potentially assigned as the perpetrator.

```
<h1>Pick a random number.</h1>
<p>Pick a number between 1 and 8:</p>
{
  <!-- Input box to get the user's number -->
  (input-box: bind $userNum)
}
{
  <!-- Submit button to validate input -->
  (link-repeat: "Submit")[
    (if: $userNum is not "")[
      (if: (num: $userNum) >= 1 and (num: $userNum) <= 8)[
        (set: $suspectNum to (num: $userNum)) <!-- Convert to a
number and store it in $suspectNum -->
        (show: ?nextLink) <!-- Reveal the link to the next passage
-->
      ]
      (else:)[
        (alert: "Please enter a valid number between 1 and 8.")
      ]
    ]
    (else:)[
      (alert: "Please enter a number.")
    ]
  ]
}
{
  |nextLink)[[[Continue to Avatar Creation Complete->Avatar Creation
Complete]]]
}
```

Selecting a Perpetrator Code Snippet

Each number corresponds to a different character profile, the controlled randomness ensures diverse outcomes while preventing complexity. The chosen number influences which perpetrator's details are revealed.

Notably, $suspectNum applies to all perpetrators except Suspect 7, representing the audience, which is handled uniquely in subsequent sections.

Implementing Caesar Cipher to Encrypt User Name in Twine

To simulate hacker activity and introduce basic encryption, a Caesar Cipher was implemented to encrypt the user's name early in the play. This encryption uses the scrambled name as a narrative clue, enhancing the storyline by giving the impression that a hacker is manipulating information in real-time.

In the TestSuspectNode, the cipher-encrypted names of other characters have been manually inserted, each with predetermined scrambled names and decryption keys.

However, for Suspect 7, the audience member chosen through their number selection, a dynamic script was required to scramble their name. This script takes the user input from the avatar creation process and encrypts their name with a Caesar Cipher shift of 7.

The scrambled name appears as a clue during the investigation, but the audience do not immediately recognise it. This dynamic encryption was specifically designed for Suspect 7, while the other suspects follow pre-encoded paths.

JavaScript Code for Encryption

Twine’s Harlowe language doesn't natively support JavaScript, so a workaround using *window.harloweVariables* allowed manipulation of Harlowe variables. This enabled encryption and the use of the scrambled name as a variable within the story.

```
// JavaScript tab
window.harloweVariables = State.variables; // Create a global
reference to Harlowe variables
```

Harlowe Global Variables

```
function caesarCipherEncrypt(str, shift) {
    return str.split('').map(char => {
        if (char.match(/[a-z]/i)) {
            const base = char.charCodeAt(0) < 97 ? 65 : 97;
            const encryptedChar = String.fromCharCode(((char.charCodeAt(0) - base + shift) % 26) + base);
            return encryptedChar;
        }
        return char; // Non-letter characters remain unchanged
    }).join('');
}

// Automatically encrypt the user's name when the passage loads
const inputString = window.harloweVariables.userName; // Get the Harlowe variable
const encryptedString = caesarCipherEncrypt(inputString, 7);

// Display the output
document.getElementById('output').innerHTML = encryptedString;

// Store the result back into a Harlowe variable
window.harloweVariables.encryptedName = encryptedString; // Store it in a Harlowe variable
```

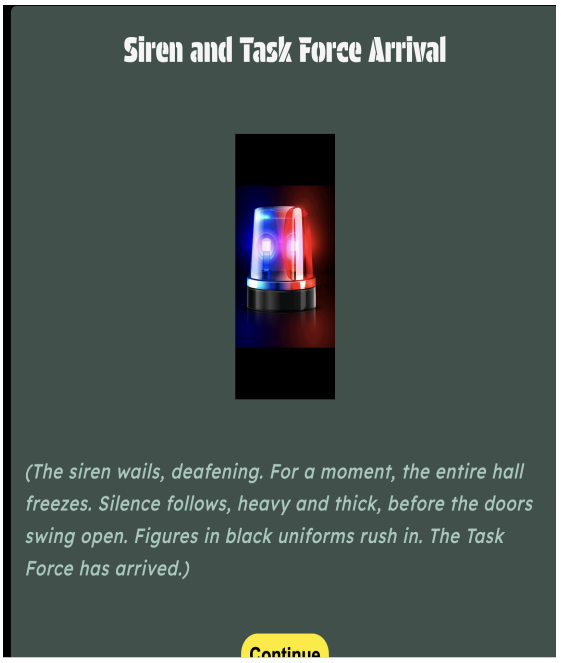
Cipher Encryption Code

This method takes the input from the original avatar creation, stores it in a Harlowe Variable and allows it to be accessed through JavaScript. This then converts it to a JavaScript variable before adding it to the story at selected places.

Implementation of the Sidebar and Task Force Arrival

The arrival of the task force, marked by a siren video, signals a key shift in *Cyber Play* from a routine assembly to an intense cybersecurity investigation. Due to Twine's limitations with local media, the video was hosted externally on Wix and linked to the play. This approach allowed seamless multimedia integration, heightening the immersive experience.

```
<h1>Siren and Task Force Arrival</h1>

<div style="display: flex; justify-content: center; align-items: center;">
  <video class="siren" id="sirenVideo" width="560" height="315" controls autoplay>
    <source src="https://video.wixstatic.com/video/27b368_91943f947fa847ce8dfe7069aef467c1/1080p/mp4/file.mp4" type="video/mp4">
    Your browser does not support the video tag.
  </video>
</div>

<p class="s_direction">(The siren wails, deafening. For a moment, the entire hall freezes. Silence follows, heavy and thick, before the doors swing open. Figures in black uniforms rush in. The Task Force has arrived.)</p>

[[Continue->Siren2]]

(display: "SidebarBack")
```



Siren and Task Force Arrival Code and Visual

Sidebar System Overview

The Sidebar provides real-time updates, displaying suspects and clues as they are uncovered. It serves as a progress tracker, helping the audience stay engaged with the investigation by:

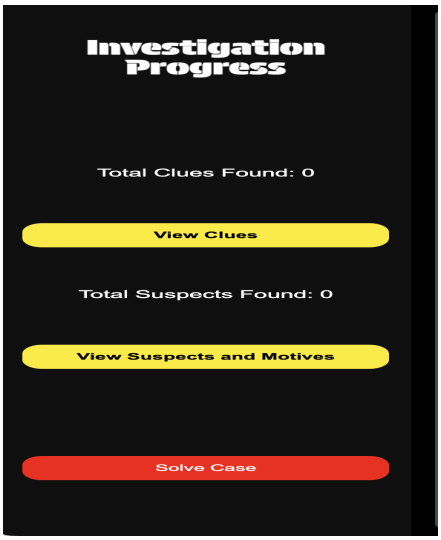
- Displaying discovered clues and suspects.
- Tracking the total number of clues.
- Offering detailed information about each clue.
- Indicating when sufficient evidence has been gathered to solve the case.

The Sidebar updates automatically. For example, when "Clue 1" (a Caesar Cipher) is discovered, the code increments the clue counter and refreshes the display, keeping the audience involved as the investigation unfolds.

```
<!-- Check and update the clue variable -->
(if: $clue1_found is not true)[
 (set: $clue1_found to true)
 (set: $cluesFound to $cluesFound + 1)
]
```

Incrementing Sidebar Clues

Sidebar Code Example for Clues and Suspects




```
<!-- Display total clues found -->
<p>Total Clues Found: (print: $cluesFound)</p>

<ul>
  (if: $clue1_found is true)[<li>Caesar Cipher found in hacker's message.</li>]
  (if: $clue2_found is true)[<li>Suspicious IP Address found in logs.</li>]
  (if: $clue3_found is true)[<li>Email Header Clue - 'Trust me, this is safe.'.</li>]
  (if: $clue4_found is true)[<li>Encryption tools found on the compromised machine.</li>]
  (if: $clue5_found is true)[<li>Hackers Profession Found.</li>]
  (if: $clue6_found is true)[<li>Login attempts at unusual hours.</li>]
  (if: $clue7_found is true)[<li>Found hackers favourite colour.</li>]
  (if: $clue8_found is true)[<li>Hackers First Pet name found</li>]
  (if: $clue9_found is true)[<li>Found Hackers mothers maiden name.</li>]
  (if: $clue10_found is true)[<li>Anonymous email traced back to the hacker.</li>]
  (if: $clue11_found is true)[<li>Favorite Hobby used as a personal security question.</li>]
  (if: $clue12_found is true)[<li>Decryption Key used to decode the message.</li>]
  (if: $clue13_found is true)[<li>Hidden message "Olssv dvysk" found in the source code, awaiting decryption.</li>]
  (if: $clue14_found is true)[<li>Found Hackers online name.</li>]
   (if: $clue15_found is true)[<li>Hackers scrambled email found</li>]
  <!-- Other clues here -->
</ul>

(display: "SidebarBack")
(display: "Sidebar")
```

```
<ul>
  (if: $suspect1_found is true)[<li><b>Alex Johnson</b>: Computer Technician, frustrated with IT policies. His night shift gave him access to key systems.</li>]
  (if: $suspect2_found is true)[<li><b>Jamie Parker</b>: System Administrator, seeking more control over system access. His role granted him insider knowledge.</li>]
  (if: $suspect3_found is true)[<li><b>Emily Davis</b>: Headteacher, frustrated with budget cuts affecting IT infrastructure. She might have sought control over limited resources.</li>]
  (if: $suspect4_found is true)[<li><b>Thomas Reed</b>: Deputy Headteacher, believed IT resources were being mismanaged. His position gave him administrative access.</li>]
  (if: $suspect5_found is true)[<li><b>Sarah Lee</b>: IT Support Staff, wanted better infrastructure. Her role allowed her to install critical software.</li>]
  (if: $suspect6_found is true)[<li><b>Robert Brown</b>: Librarian/Media Specialist, wanted more control over school media. He could access the media network.</li>]
  (if: $suspect7_found is true)[<li><b>Luddite</b>: Anti-technology advocate, aiming to disrupt all tech systems. His anti-tech stance made him a prime suspect.</li>]
  (if: $suspect8_found is true)[<li><b>EVERYONE</b>: Everyone is a suspect! A coordinated effort might have been behind this attack.</li>]
</ul>

(display: "SidebarBack")
```

Sidebar Overview

This real-time update system maintains engagement and a sense of progression as the audience uncovers more clues.

Sidebar Templates and the "Solve Case" Button

The sidebar is implemented as a reusable template using Twine's Harlowe macro (display: sidebar), allowing it to appear across multiple passages without duplicating code.The sidebar includes a Solve Case button, which activates based on the number of clues found.

- Red (disabled): Less than or equal to 3 clues.
- Orange (enabled): Medium difficulty (4-6 clues).
- Green (enabled): Easier difficulty (more than 6 clues).

This dynamic button adds control over the investigation’s pacing, heightening narrative tension as clues are gathered.

```
<!-- Solve Case Button with color and status change -->
{
  (if: $cluesFound <= 3)[
    <!-- Disable the button if less than 4 clues are found -->
    <button class="solve" style="background-color: red; cursor:
not-allowed;">Solve Case</button>
  ]
  (else-if: $cluesFound > 3 and $cluesFound <= 6)[
    <!-- Link to Gatekeeper Node with orange color for medium
difficulty -->
    <button class="solve" style="background-color: orange;
cursor: pointer;">[[Solve Case ->Gatekeeper Node]]</button>
    <p style="color: orange; font-size: 0.8em;">Hard</p>
  ]
  (else-if: $cluesFound > 6)[
    <!-- Link to Gatekeeper Node with green color indicating
readiness -->
    <button class="solve" style="background-color: green;
cursor: pointer;">[[Solve Case ->Gatekeeper Node]]</button>
    <p style="color: green; font-size: 0.8em;">Ready to solve!</p>
  ]
}
```

Solve Button Implementation

Back Button (SidebarBack Template)

To enhance user navigation, I implemented a Sidebar Back button, allowing the audience to return to previously viewed passages seamlessly. This feature was added for stylistic reasons, ensuring smoother navigation and a more intuitive experience. The back button is triggered when there are multiple pages in the user's navigation history, and it directs the user to the last visited passage. If no previous pages are available, a message informs the user that there is no page to return to.

The following code snippet demonstrates how the back button works:

```
<div id="back-sidebar">
  <!-- Back Button using the (history:) macro to navigate to the
last visited passage -->
  (if: (history:)'s length > 1)[
    (link-goto: "Go Back", (history:)'s last)
  ]
  (else:)[
    <p>No previous page to go back to.</p>
  ]
</div>
```

Sidebar Back Implementation

Meet the Individuals Node: Interactive Introduction of Suspects

Meet the Individuals

The Meet the Individuals node is a key moment where the audience is introduced to suspects in the cybersecurity breach. Each suspect has a unique backstory and an alibi, offering insight into their potential involvement. This interaction builds both the narrative and audience engagement by encouraging critical thinking about who may be responsible.

Technical Overview

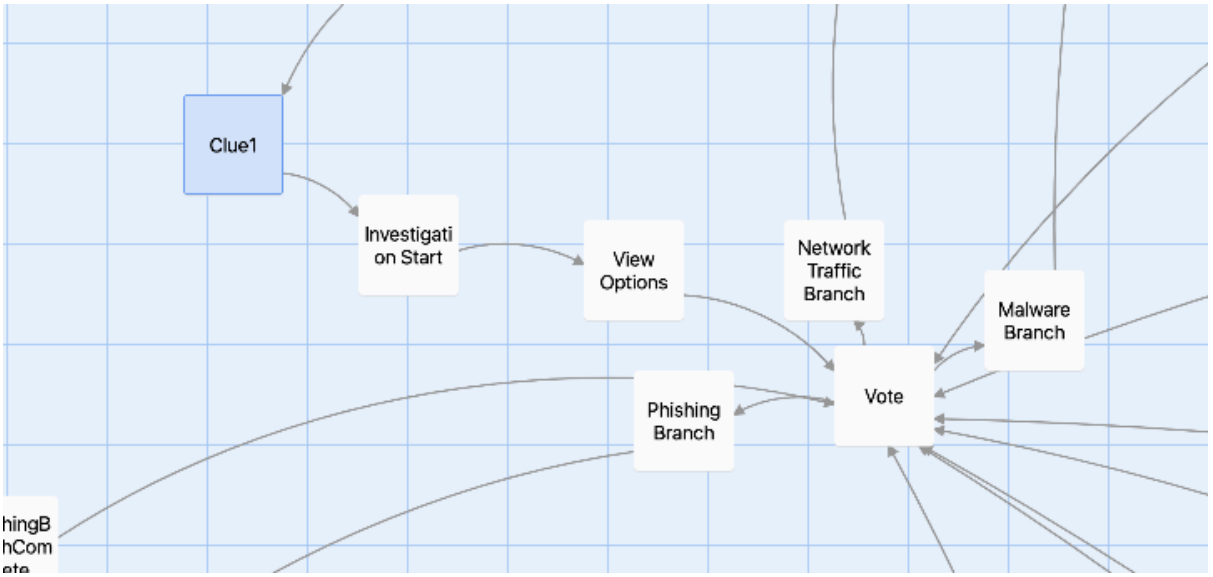
Using JavaScript, suspects are revealed one at a time. Initially, only the first suspect is visible; clicking the screen hides the current suspect and shows the next. After all suspects are introduced, the narrative continues with a dialogue from the Task Force Commander. Each suspect's details, name, job title, and backstory, are housed in separate elements, with display properties adjusted dynamically.

This structure ensures smooth, engaging progression as suspects are introduced, allowing the audience to analyse each one before moving forward.

```
<script>
      let currentIndividual = 1; // Start at Individual 1

      document.getElementById('clickableArea').addEventListener('click', function() {
          if (currentIndividual <= 7) {
              // Hide the current individual
              document.getElementById(`individual${currentIndividual}`).style.display = 'none';

              // Show the next individual
              currentIndividual++;
              if (currentIndividual <= 7) {
                  document.getElementById(`individual${currentIndividual}`).style.display = 'block';
                  document.getElementById(`individual${currentIndividual}`).style.zIndex = '1'; // Ensure it's on top
              } else {
                  // Show the Task Force Commander dialogue after the last individual
                  document.getElementById('taskForceDialogue').style.display = 'block';
              }
          }
      });

      // Initially display the first individual
      document.getElementById('individual1').style.display = 'block';
  </script>
```

Displaying each suspect in Meet the Individuals

Discovery of Clue and Branch Choices



First Clue: Hacker's Message - Implementation

The First Clue: Hacker's Message introduces the audience to the play's first cybersecurity puzzle, a Caesar Cipher. This clue is semi-random, with the shift number determined by the suspect number selected by the audience earlier in the play.

Caesar Cipher Randomisation

The number tied to each suspect, based on the audience's earlier choice, dictates the shift for the Caesar Cipher. The variable $suspectNum is used to assign the correct shift number for the clue.

- For example, if the audience chose suspect 1, the cipher shift is 3.

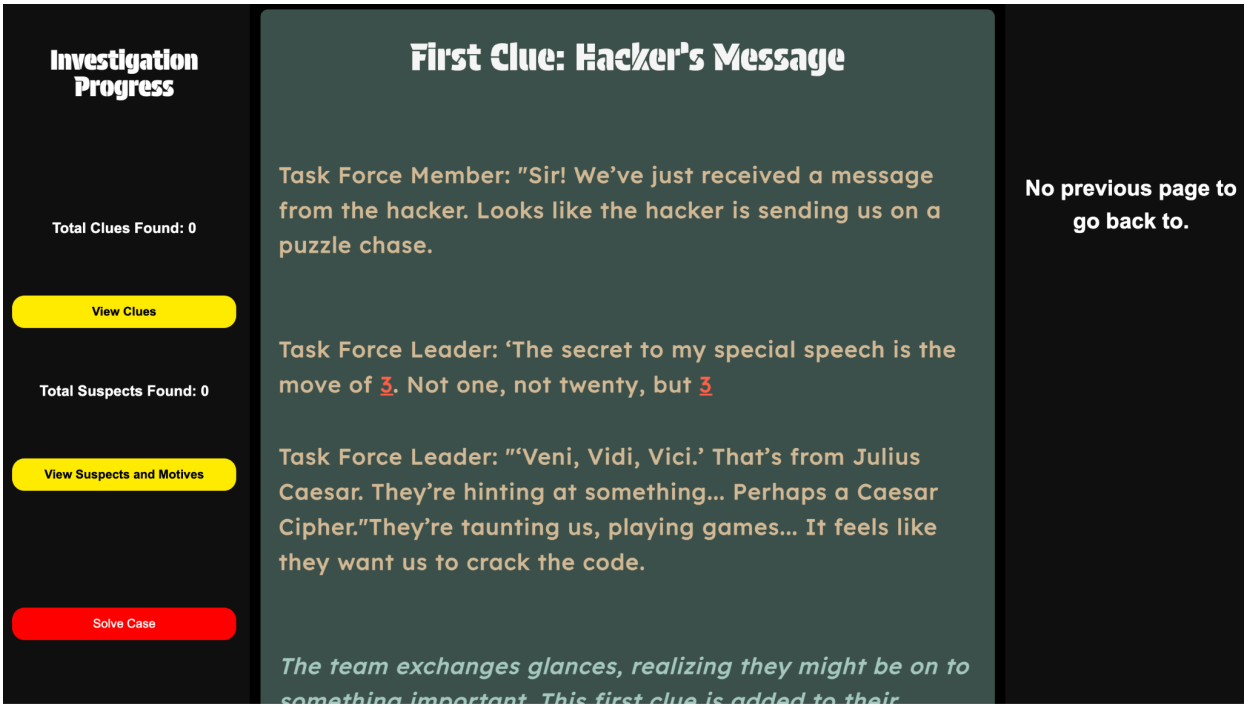
- If suspect 7 (representing the audience member) is chosen, the shift is 7, aligning with their avatar creation choice.

```
(if: $suspectNum is 1)[3]
(else-if: $suspectNum is 2)[5]
(else-if: $suspectNum is 3)[4]
(else-if: $suspectNum is 4)[2]
(else-if: $suspectNum is 5)[7]
(else-if: $suspectNum is 6)[6]
(else-if: $suspectNum is 7)[(print: 7)]
(else-if: $suspectNum is 8)[8]
(else:)[3]
```

Setting the Cipher Number

If no input is provided, the default shift is set to 3.

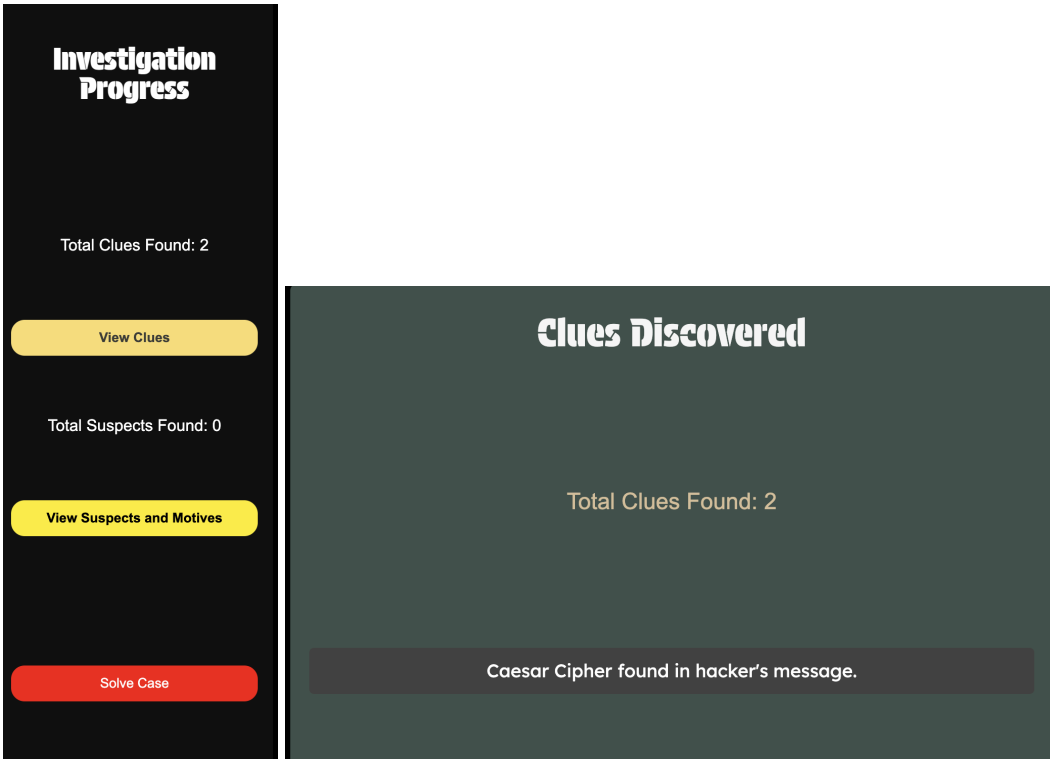
The clue is introduced as a cryptic message from the hacker, with the task force leader hinting at the use of a Caesar Cipher by referencing Julius Caesar's famous quote. The cipher shift is clearly explained, directly connecting it to the audience's earlier decision during avatar creation.



Displaying the Clue

Once the clue is introduced, it’s added to the investigation progress, with the sidebar dynamically updating to reflect newly discovered clues. The clue is tracked using the $clue1_found variable, which increments the total number of clues.

The audience can review discovered clues at any time by accessing the sidebar, the dynamic update works by checking to see if $clueX_found is true and then uncovering the individual divs in the sidebar.



Updating Sidebar and Clues Page

View Options Node

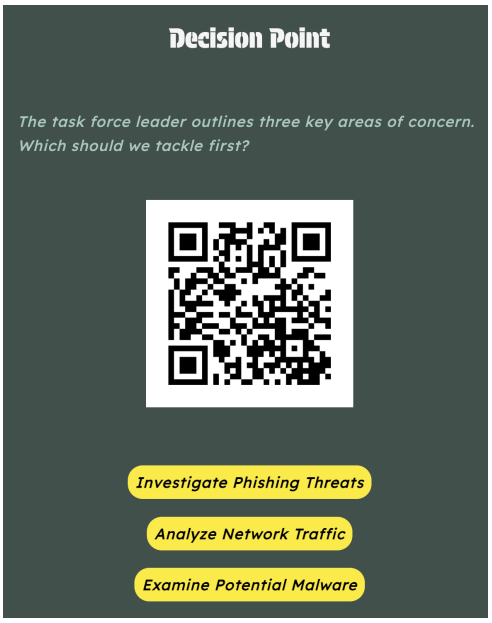
The View Options node structures the decision-making process. Similar to earlier sections, key details are presented sequentially, encouraging the audience to carefully consider their choices. The node combines JavaScript and Twine variables to reveal paragraphs one by one, presenting the three investigative paths (Phishing, Network Traffic, and Malware). The choices are hidden until all details have been reviewed, enhancing immersion and thoughtful decision-making.

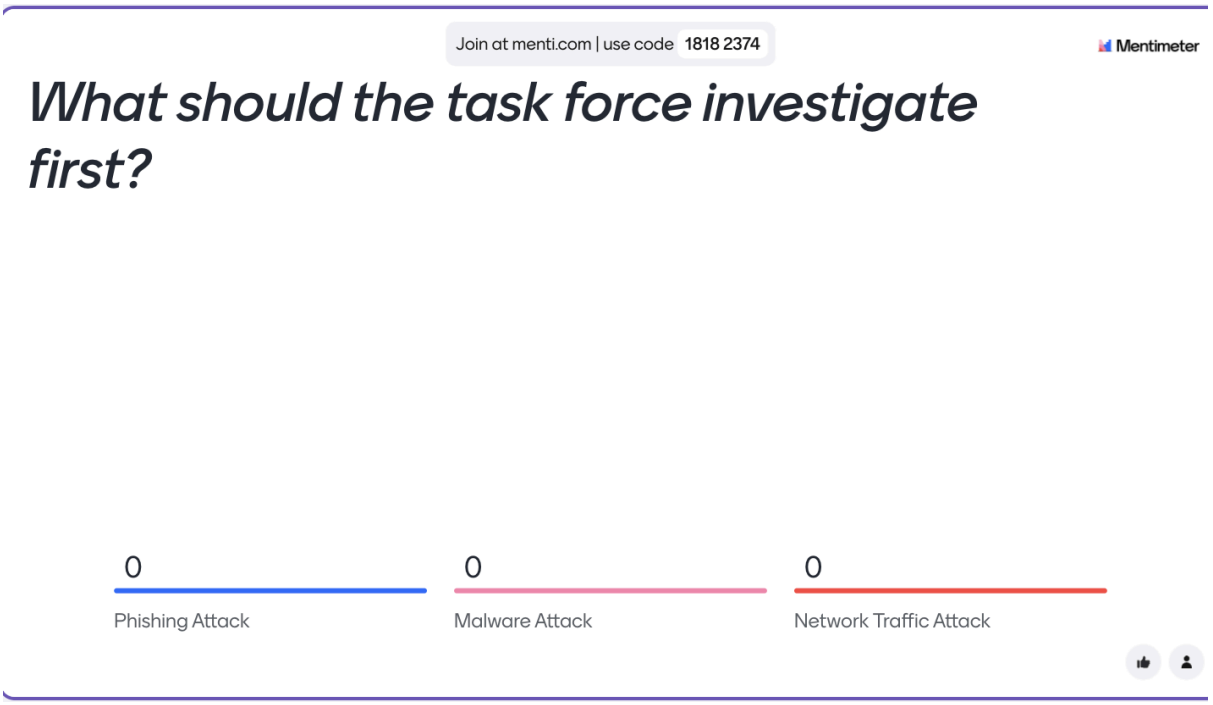
JavaScript controls the pacing, ensuring the audience moves through the options in sequence, similar to the Meet the Individuals section. Each option is displayed only after the previous one has been clicked through. The code ensures that the “Vote” link appears only after all options have been presented, keeping the flow smooth and logical.

```
<script>
    let currentText = 1; // Start with the first paragraph

    document.getElementById('clickableArea').addEventListener('click', function() {
        if (currentText <= 6) { // Ensure we stop before the last text
            // Hide the current paragraph
            document.getElementById(`text${currentText}`).style.display = 'none';

            // Show the next paragraph
            currentText++;
            if (currentText <= 6) {
                document.getElementById(`text${currentText}`).style.display = 'block';
                document.getElementById(`text${currentText}`).style.zIndex = '1'; // Ensure it's on top

                // Hide the instruction after the last click
                if (currentText === 6) {
                    document.getElementById('clickForNext').style.display = 'none'; // Hide "Click for next..."
                    document.getElementById('voteLink').style.display = 'block'; // Show the vote link
                }
            }
        }
    });

    // Initially display the first paragraph
    document.getElementById('text1').style.display = 'block';
</script>

<style>
    /* Add matching styling for "Click for next..." */
    .instruction {
        text-align: center;
        margin-top: 20px;
        color: #d4c5a6; /* Matching text color */
        font-style: italic;
    }
```

Meet the Individuals Code Snippet

Vote Node



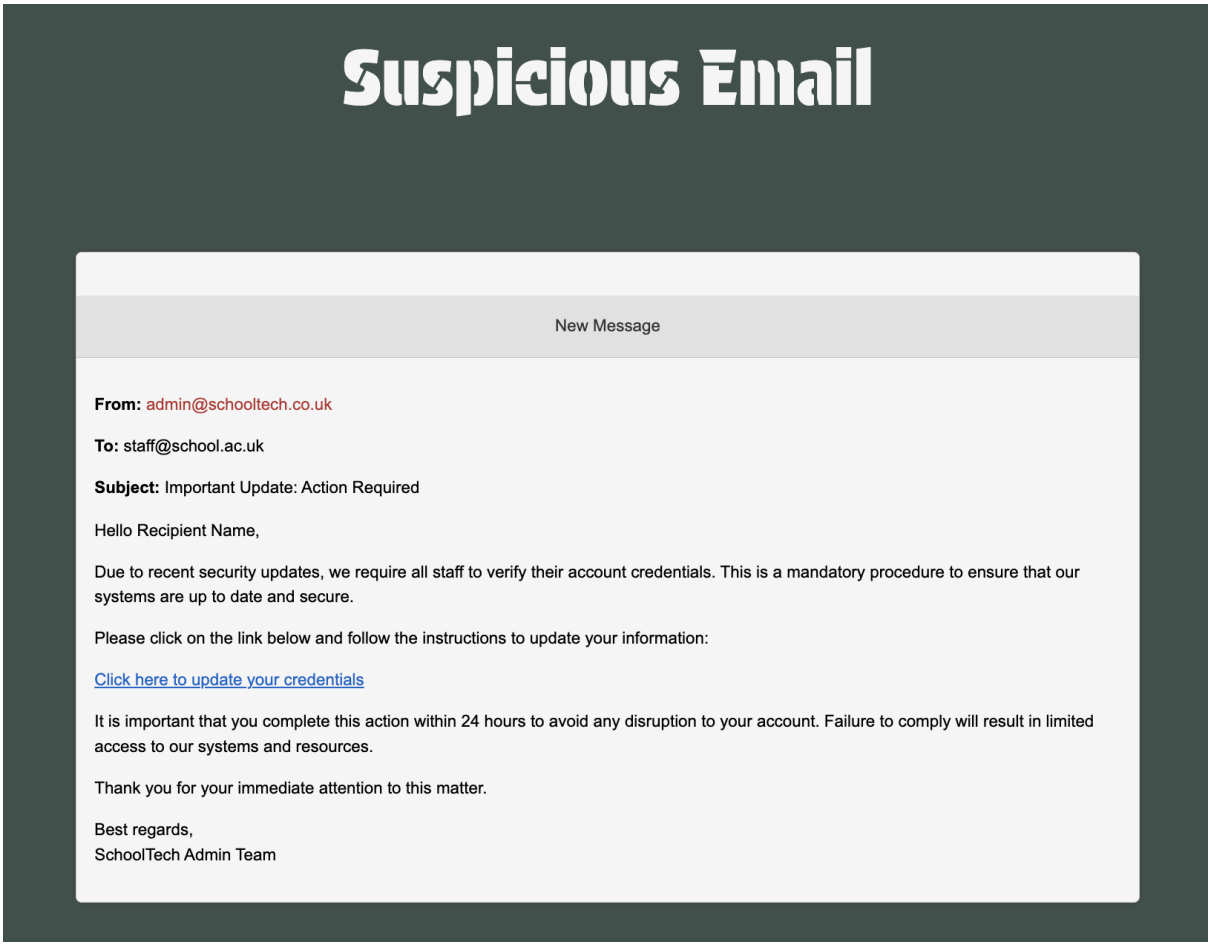


Voting and Mentimater Visual

The Vote Node allows the audience to decide which investigative path to follow (Phishing, Network Traffic, or Malware) using Mentimeter. Participants scan a QR code to cast votes in real-time, adding an interactive element to the play. A task force

member manually switches Mentimeter slides based on the audience's choice, which can cause slight delays due to the branching nature of the story. Once voting concludes, the play proceeds along the selected branch.

Phishing Branch



Suspicious Email Resource within Cyber Play

In the Phishing Branch of Cyber Play, participants are presented with a **Suspicious Email** interface that mimics a real inbox. This mock email contains typical red flags found in phishing scams, such as a deceptive sender address (admin@schooltech.co.uk) and an urgent request for credential verification. The

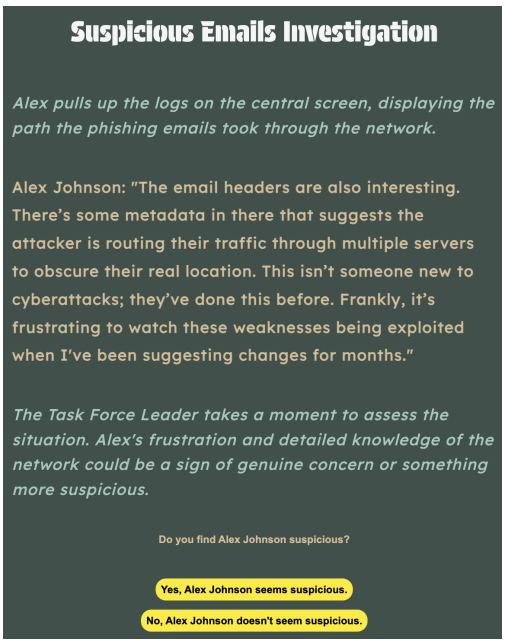
purpose is to teach students how to spot phishing scams through hands-on interaction.

The email interface is built using a simple HTML structure with CSS classes that simulate a real email client. The sender's email is set up to display subtle clues that it is suspicious, while the link, styled like a typical phishing link, uses a javascript:void(0); call to ensure it doesn't redirect anywhere.

The audience is engaged by task force members who lead them through an analysis of the email. Key suspicious elements, such as the sender's address and the fake link, are highlighted to teach participants how to critically assess potential phishing emails.

Suspect Alex Johnson

The audience meets Alex Johnson, a Computer Technician and potential suspect. He offers technical insights into phishing emails, discussing metadata and email routing. However, Alex's frustration with the school's IT policies introduces ambiguity, leaving the audience uncertain about his involvement in the attack.



Is Alex Johnson a suspect?

After Alex's introduction, the audience is prompted to decide whether they find his behaviour suspicious. This decision is captured using conditional logic:

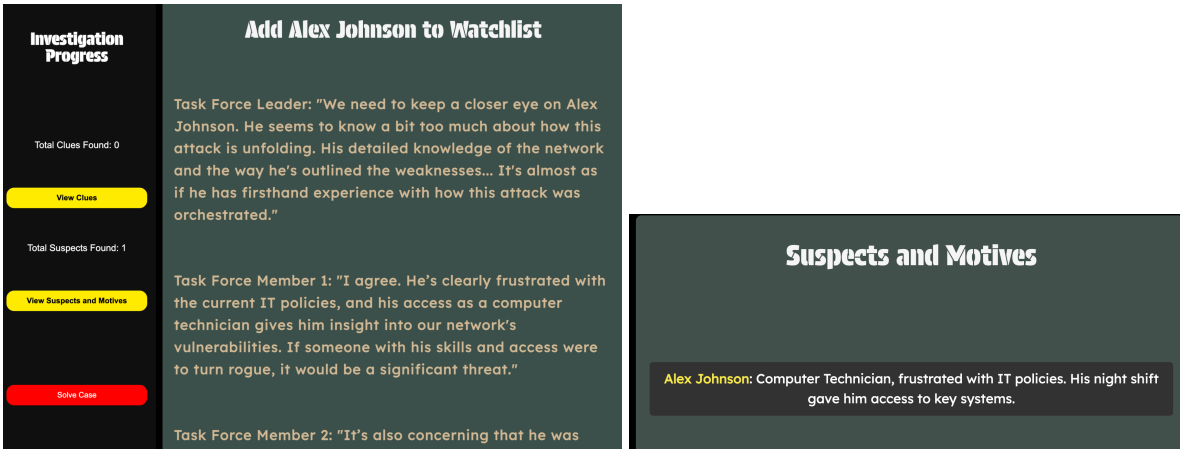
<!-- Set the suspect variable to true if Alex is marked as suspicious -->

(set: $suspect1_found to true)

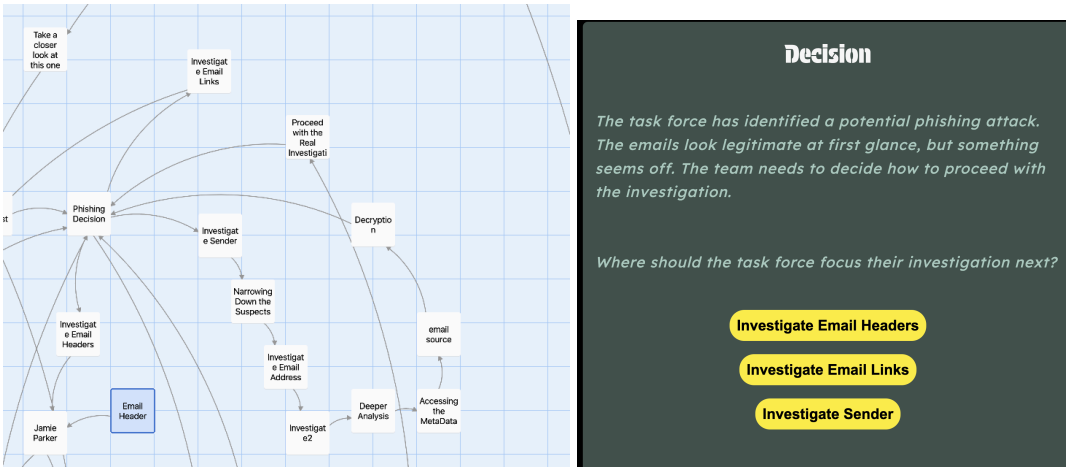
(set: $suspectsFound to $suspectsFound + 1)

If the audience selects "Yes," the variable $suspect1_found is set to true, marking Alex as a suspect. This also increments the global variable $suspectsFound to keep track of how many suspects have been identified, which is displayed in the Sidebar that tracks the investigation's progress.

If the audience chooses "No" (i.e., they do not find Alex suspicious), the variable is not triggered, and the story continues without adding Alex to the suspect list.



Adding Alex Johnson to the Suspects List

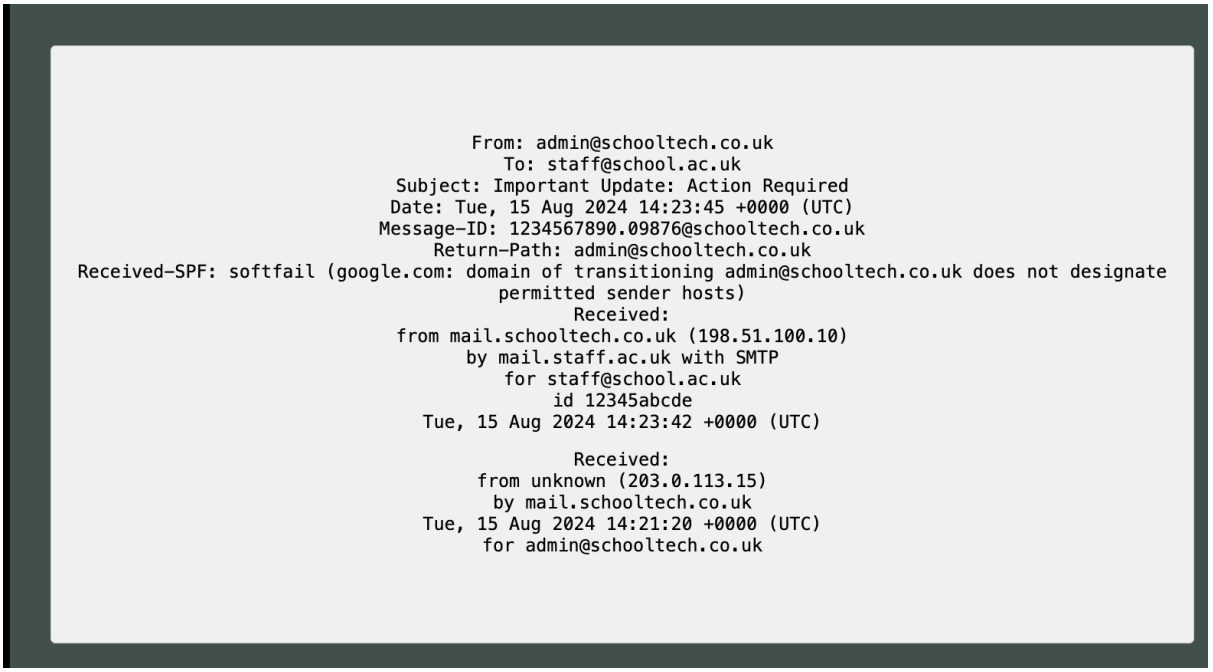


Phishing Branch Decision Point

Exploring the Email Headers

The audience is presented with three investigative paths: headers, links, and sender information. Choosing to investigate the email headers provides a detailed lesson on

the type of information found in headers and how attackers obscure their location by routing traffic through multiple servers. This reinforces the play's educational objectives by illustrating real-world phishing techniques.



Email Headers

Diversion into Fake News

Choosing the email headers path leads to a diversion involving Mr. Luddite, where the narrative branches into the Fake News Route. Mr. Luddite tries to convince the audience that the attack isn't phishing but instead a new malware, ViperWorm.

- Dynamic Dialogue: If Jamie Parker was previously marked as a suspect, he supports Mr. Luddite's theory, attempting to derail the investigation. If Jamie is not a suspect, he takes a more pragmatic stance, refocusing the investigation on the evidence. This was implemented using a simple if/else statement, and checking against the suspect found variable

```
<!-- Check if Jamie Parker is a suspect -->
{
  (if: $suspect2_found is true)[
    <!-- If Jamie Parker is a suspect -->
    <p class="s_direction">Jamie Parker smirks, clearly entertained by Luddite's outburst. He leans back in his chair, speaking with a mix of sarcasm and disdain.</p>

    <p class="speech"><b>Jamie Parker:</b> "You know, Luddite might be onto something for once. *Viperworm*, huh? Sounds like exactly the kind of thing our outdated systems wouldn't catch. Maybe we should all listen to the 'insider'."</p>

    <p class="s_direction">He glances at the task force leader with a hint of defiance.</p>

    <p class="speech"><b>Jamie Parker:</b> "After all, we're just following the same old protocol here, aren't we? Maybe it's time for some outside-the-box thinking."</p>

    <p class="s_direction">His tone grows colder, revealing his frustration with the current investigation's direction.</p>

    <p class="speech"><b>Task Force Leader:</b> "Jamie, enough. We can't get sidetracked by every theory. Focus on the evidence."</p>

    <p class="speech"><b>Jamie Parker:</b> "Evidence... right. Because evidence has been so effective at stopping this so far."</p>

    <p class="s_direction">He turns back to his screen, muttering under his breath as he begins typing furiously.</p>
  ]
  (else:)[
    <!-- If Jamie Parker is not a suspect -->
    <p class="s_direction">Jamie Parker sighs, rubbing his temples before stepping in to address Luddite's claim.</p>

    <p class="speech"><b>Jamie Parker:</b> "Luddite, while the idea of *Viperworm* is... intriguing, there's no solid evidence pointing to that right now. We need to focus on what we can prove."</p>

    <p class="s_direction">He turns to the task force leader, nodding in agreement with the current line of investigation.</p>

    <p class="speech"><b>Jamie Parker:</b> "If we start chasing every rumor or theory, we'll end up wasting time and resources. Let's stick with the clues we've gathered so far."</p>

    <p class="s_direction">He sits back down, his demeanor calm and focused as he resumes his work.</p>

    <p class="speech"><b>Task Force Leader:</b> "Exactly. We can't afford to get distracted by speculation. We need to stay on track."</p>
  ]
}

[[Proceed to Vote->Vote for Attack]]
```

Dynamic Dialogue Harlowe Code

The audience is prompted to vote on whether to investigate ViperWorm or continue with the phishing investigation. If they choose ViperWorm, the story diverts into the Fake News Route, where they encounter a series of fake news stories about the virus.

The fake news stories are presented using a randomised array. Each time the audience explores the ViperWorm/Fake News Path, they are shown a different fake news story, ensuring variability and unpredictability. These exaggerated and humorous stories, such as claims that ViperWorm can control thoughts through smartphones, highlight the role of misinformation in cyberattacks.

Randomisation is implemented through a Twine macro that generates a random index to select a story from a predefined array, ensuring the audience encounters different stories each time.

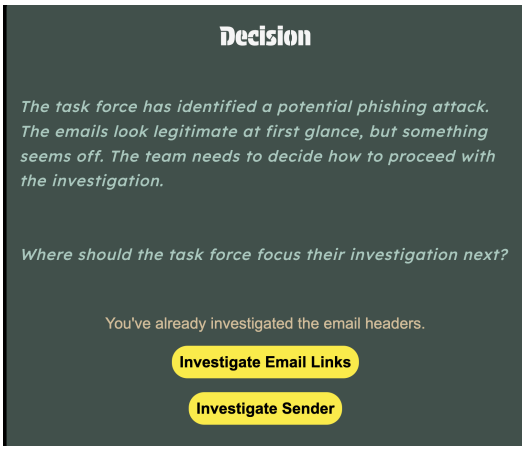
```
<h1>Viperworm News Article</h1>
{
<!-- Define the array of fake news stories directly in the passage -->
(set: $viperWormStories to (a:
    "ViperWorm 2.0: Experts claim it can fry your microwave and break your fridge!<br>
Tech Alarm Network - Breaking News<br>
In a shocking turn of events, cybersecurity experts are warning about <strong>ViperWorm 2.0</strong>, a new mutation of the already dangerous virus. According to reports, ViperWorm has evolved beyond attacking computers—it's now
capable of <strong>frying household appliances</strong>, including microwaves and refrigerators!<br>
'Once ViperWorm 2.0 infects your home network, it spreads rapidly,' said Dr. Jen Hacker, a leading cybersecurity expert. 'We've seen it <strong>overheat microwaves</strong> to dangerous levels, causing them to break down or even
explode. And don't even get me started on what it's doing to fridges—food spoilage and more!'<br>
Experts urge everyone to unplug all smart appliances until further notice.",

    "ViperWorm now capable of controlling your thoughts through your smartphone!<br>
<strong>World Tech News Flash</strong><br>
In an alarming new development, researchers have discovered that the infamous <strong>ViperWorm</strong> has evolved to <strong>control human thoughts</strong> through smartphones! Using highly advanced mind-hacking techniques,
ViperWorm can take over a person's decision-making process just by infecting their phone.<br>
Victims report suddenly feeling compelled to share personal information online, make strange purchases, or even text embarrassing secrets to their contacts.<br>
'It feels like my brain was hijacked,' said one victim. 'I ordered 100 pizzas without realizing it!'<br>
Experts advise turning off all smartphones until a patch can be released to protect users from mind control.",

    "ViperWorm attacks pets! Beware of infected cats and dogs!<br>
<strong>Breaking: PetVirus Reports</strong><br>
Cybersecurity experts have issued an urgent warning: <strong>ViperWorm</strong> is no longer just a threat to humans and computers—it's now targeting our beloved pets. Reports indicate that once a household device is infected,
<strong>ViperWorm</strong> can somehow spread to nearby cats, dogs, and even hamsters.<br>
'My cat started acting really strange,' said one victim. 'It kept pawing at my computer, like it was trying to hack into my email!'<br>
Pets infected with ViperWorm may display erratic behavior, such as excessive typing, attempting to chew on USB cables, or incessantly knocking over smart devices. No animal is safe!",

    "New study suggests ViperWorm can spread via Bluetooth earbuds!<br>
<strong>Tech Alert News Bulletin</strong><br>
A new study has revealed a startling finding: the <strong>ViperWorm virus</strong> may be spreading via Bluetooth earbuds. Scientists have found that once ViperWorm infiltrates a device, it can hop from phone to phone through
Bluetooth connections—starting with <strong>wireless earbuds</strong>.<br>
'We found that anyone within a 10-meter radius of infected earbuds is at risk,' said Dr. Soundwave from the Institute of Wireless Infections. 'The virus can travel through the airwaves at incredible speeds, infecting anyone who's
listening to music or taking a call.'<br>
To prevent infection, experts recommend turning off Bluetooth on all devices and using <strong>wired</strong> headphones.",

    "Authorities warn: ViperWorm can steal your online shopping passwords!<br>
<strong>Consumer Safety Network</strong><br>
Officials are urging everyone to be cautious while shopping online this week as the <strong>ViperWorm virus</strong> has been detected in multiple major e-commerce websites.<br>
'ViperWorm is intercepting passwords and personal details when people log into online shopping accounts,' warned a representative from CyberSafe Inc. 'People need to be extremely careful, as ViperWorm can instantly take control of
your entire shopping cart, racking up thousands of dollars in purchases without your knowledge.'<br>
Authorities recommend avoiding online shopping entirely until further notice. 'Consider going back to in-person shopping until we have this under control,' experts suggest."
))

<!-- Generate a random index number between 1 and 5 (since we know the array has 5 items) -->
(set: $randomIndex to (random: 1, 5))

<!-- Select the story based on the generated index -->
(set: $selectedStory to $viperWormStories's ($randomIndex))
}
```

ViperWorm Fake News Stories in an Array

Closing the Investigation Path

Once the audience completes this route, the variable $investigateEmailHeadersCompleted is set to true, preventing them from returning to this path. They are then redirected to choose from the remaining options.

```
<p>[[Phishing Decision]]</p>

(display: "Sidebar")
(display: "SidebarBack")

(set: $investigateEmailHeadersCompleted to true)
```



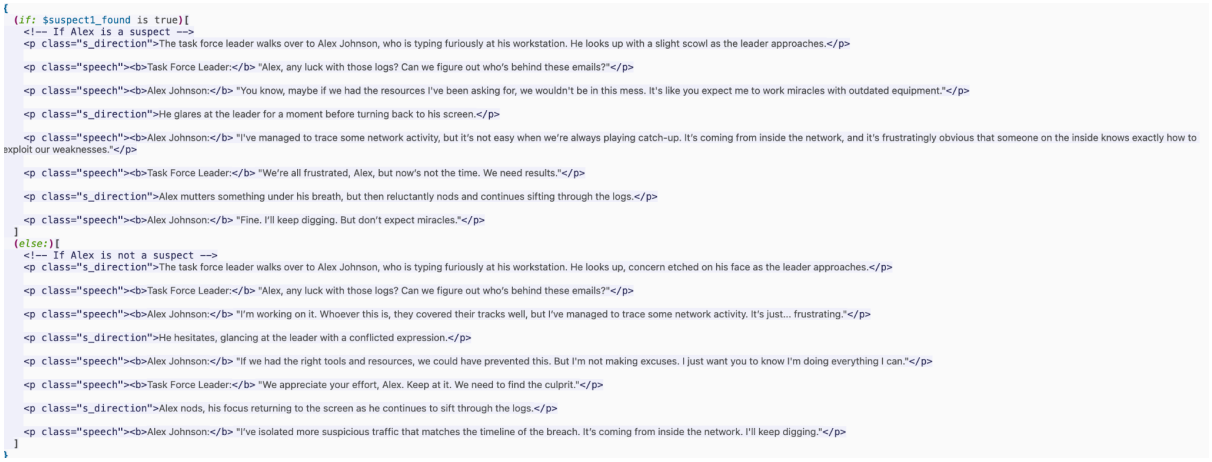
Closing a branch

Investigating the Sender

If the audience chooses to Investigate the Sender, they are guided through an analysis of the sender information from the phishing email. This path focuses on assessing the email's legitimacy and interacting with Alex Johnson, whose dialogue shifts based on whether he was flagged as a suspect earlier in the play.

The investigation turns to Alex Johnson:

- If Alex is a Suspect: He becomes defensive and frustrated, repeatedly pointing out the school's poor cybersecurity. His agitation and hints about an insider exploiting network weaknesses raise further suspicion about his involvement.
- If Alex is Not a Suspect: Alex is composed and professional, focusing on helping the task force. He acknowledges the sophistication of the attacker in covering their tracks and expresses concern about limited resources, but remains cooperative.



```
{
  (if: $suspect1_found is true)[
    <!-- If Alex is a suspect -->
    <p class="s_direction">The task force leader walks over to Alex Johnson, who is typing furiously at his workstation. He looks up with a slight scowl as the leader approaches.</p>

    <p class="speech"><b>Task Force Leader:</b> "Alex, any luck with those logs? Can we figure out who's behind these emails?"</p>

    <p class="speech"><b>Alex Johnson:</b> "You know, maybe if we had the resources I've been asking for, we wouldn't be in this mess. It's like you expect me to work miracles with outdated equipment."</p>

    <p class="s_direction">He glares at the leader for a moment before turning back to his screen.</p>

    <p class="speech"><b>Alex Johnson:</b> "I've managed to trace some network activity, but it's not easy when we're always playing catch-up. It's coming from inside the network, and it's frustratingly obvious that someone on the inside knows exactly how to exploit our weaknesses."</p>

    <p class="speech"><b>Task Force Leader:</b> "We're all frustrated, Alex, but now's not the time. We need results."</p>

    <p class="s_direction">Alex mutters something under his breath, but then reluctantly nods and continues sifting through the logs.</p>

    <p class="speech"><b>Alex Johnson:</b> "Fine. I'll keep digging. But don't expect miracles."</p>
  ]
  (else:)[
    <!-- If Alex is not a suspect -->
    <p class="s_direction">The task force leader walks over to Alex Johnson, who is typing furiously at his workstation. He looks up, concern etched on his face as the leader approaches.</p>

    <p class="speech"><b>Task Force Leader:</b> "Alex, any luck with those logs? Can we figure out who's behind these emails?"</p>

    <p class="speech"><b>Alex Johnson:</b> "I'm working on it. Whoever this is, they covered their tracks well, but I've managed to trace some network activity. It's just... frustrating."</p>

    <p class="s_direction">He hesitates, glancing at the leader with a conflicted expression.</p>

    <p class="speech"><b>Alex Johnson:</b> "If we had the right tools and resources, we could have prevented this. But I'm not making excuses. I just want you to know I'm doing everything I can."</p>

    <p class="speech"><b>Task Force Leader:</b> "We appreciate your effort, Alex. Keep at it. We need to find the culprit."</p>

    <p class="s_direction">Alex nods, his focus returning to the screen as he continues to sift through the logs.</p>

    <p class="speech"><b>Alex Johnson:</b> "I've isolated more suspicious traffic that matches the timeline of the breach. It's coming from inside the network. I'll keep digging."</p>
  ]
}
```

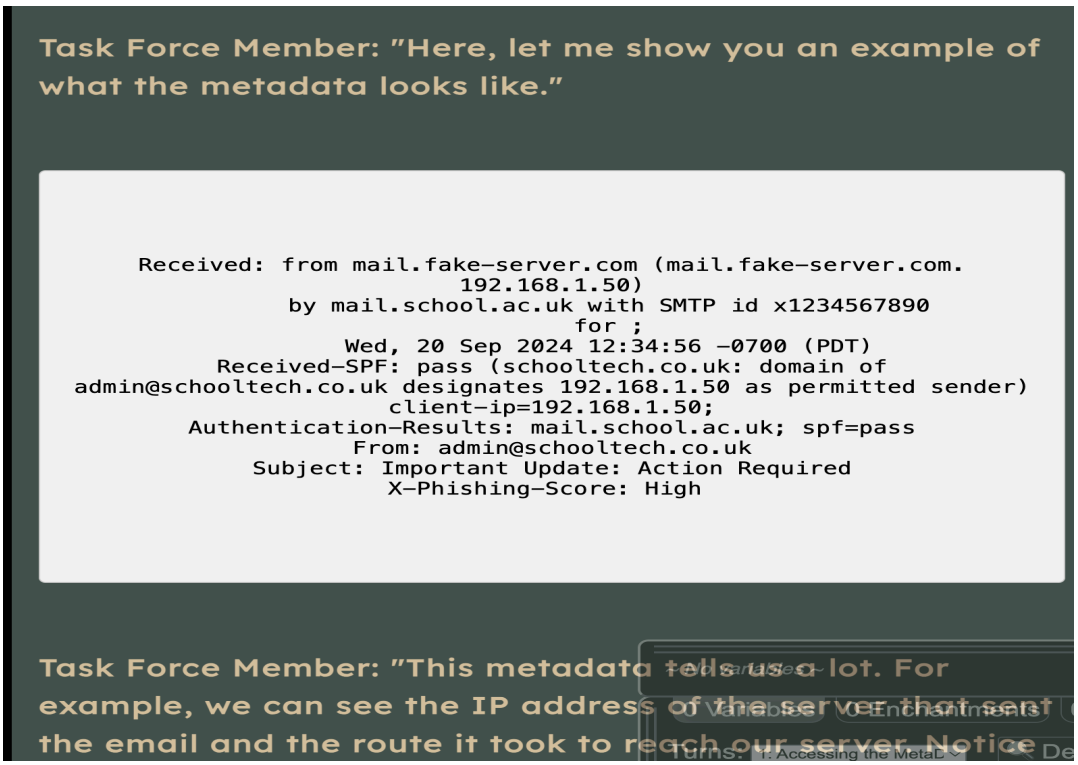
Dynamic Dialogue 2

This branching dialogue is controlled using Twine's conditional logic, checking the status of $suspect1_found to determine Alex's behaviour, allowing the investigation to proceed accordingly.

Exploring the Email Metadata

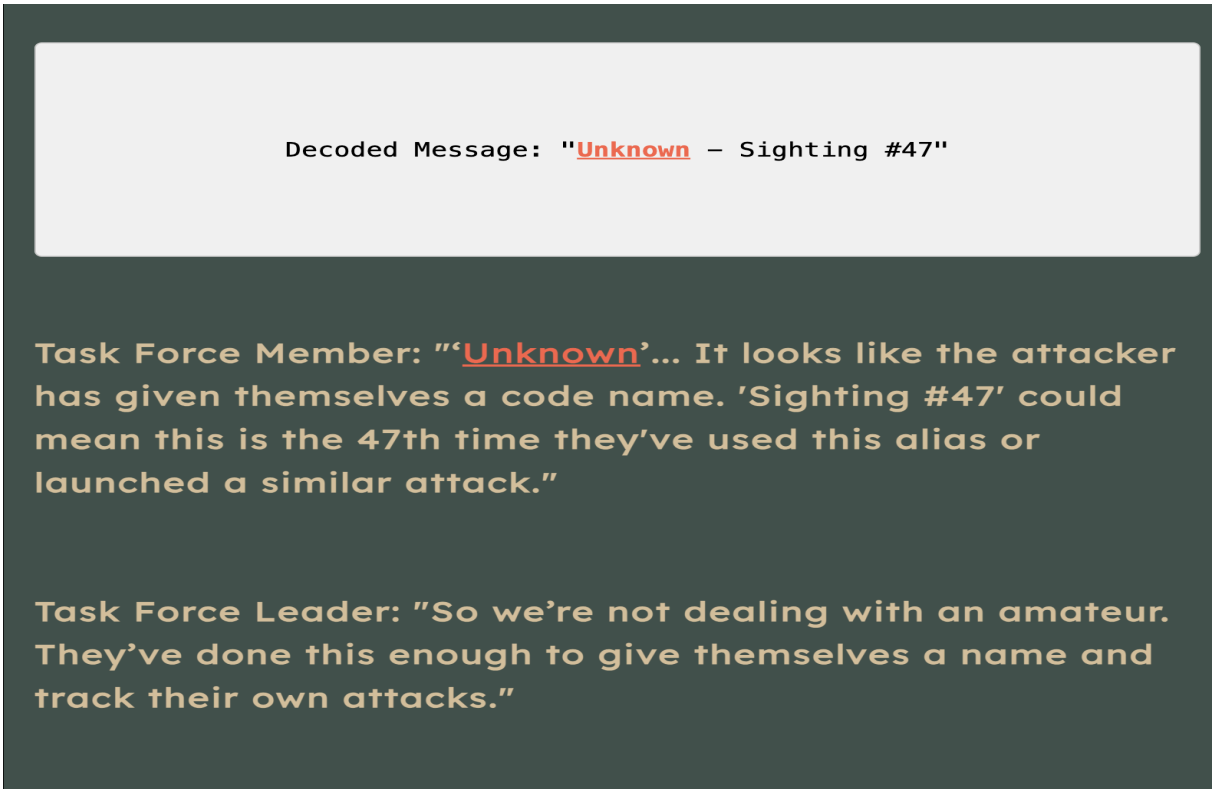
The investigation shifts to the email metadata, with the Task Force Member guiding the audience through its technical details. This serves as a mini-lesson in how email metadata aids cybersecurity investigations, covering key points:

- Server Path: The audience learns how the email travelled through the network, noting that it was sent from an external server (mail.fake-server.com).
- SPF Check: Although the SPF (Sender Policy Framework) check passes, indicating the email is authorised to send from that domain, the audience is reminded that attackers can manipulate these systems.
- X-Phishing-Score: This hidden metadata value flags the email as a high-risk phishing attempt, emphasising that users would need to examine the source code.The metadata investigation reinforces the sophistication of the attacker and encourages the task force to dig deeper.



Discovering a Clue: Decrypting the Hidden String

In Investigate Sender, the audience uncovers a hidden string in the email metadata revealing the hacker’s online alias. This clue suggests the attacker is not a casual perpetrator, but a seasoned hacker. The alias is dynamically revealed based on the suspect the audience has chosen at the beginning of the play.



Discovering the Hackers Online Identity (Default Value Selected)

```
<div class="decrypted-message" style="width: 100%; overflow:
auto; color: black; background-color: #f4f4f4; border: 1px solid
#ccc; padding: 10px; border-radius: 5px;">
  <pre style="white-space: pre-wrap; word-wrap: break-word; font-
size: 0.9em;">
Decoded Message: "<span class='clue'>{
  (if: $suspectNum is 1)[ShadowByte]
  (else-if: $suspectNum is 2)[NetPhantom]
  (else-if: $suspectNum is 3)[DataMistress]
  (else-if: $suspectNum is 4)[CipherScribe]
  (else-if: $suspectNum is 5)[CodeSorceress]
  (else-if: $suspectNum is 6)[MediaGhost]
  (else-if: $suspectNum is 7)[Audience4Lyfe]
  (else-if: $suspectNum is 8)[TechNemesis]
  (else:)[Unknown]
}</span> - Sighting #47"
  </pre>
</div>
```

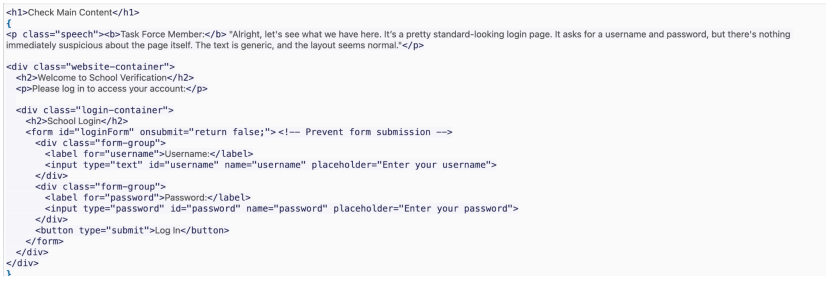
Code for the Hackers Identity

At the end of the metadata inspection, the clue flag $clue14_found is updated, and the sidebar reflects the new discovery. With the sender investigation complete, the audience is presented with the remaining choices. The path is marked as completed, ensuring it cannot be revisited.

Investigating Links

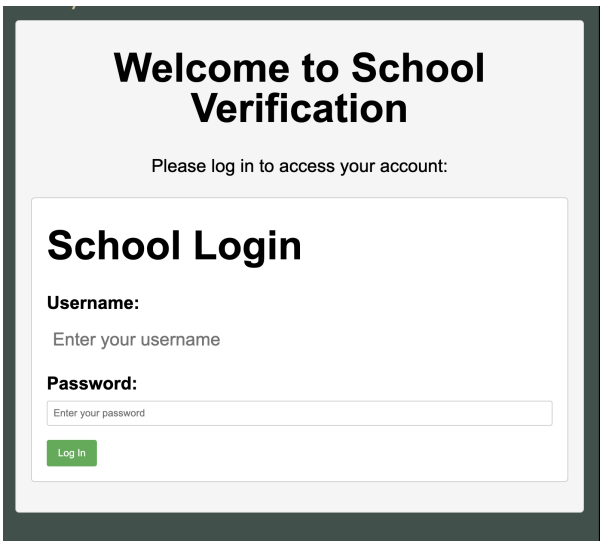
The audience is presented with a fake login page that is intentionally designed to look harmless at first glance, mimicking a typical phishing website. The page is built to reinforce the lesson that phishing websites often appear legitimate, with no obvious signs of malicious intent on the surface

The fake login page is structured using HTML elements within Twine, styled to appear like a genuine login portal for a school verification system.



```
<h1>Check Main Content</h1>
{
<p class="speech"><b>Task Force Member:</b> "Alright, let's see what we have here. It's a pretty standard-looking login page. It asks for a username and password, but there's nothing
immediately suspicious about the page itself. The text is generic, and the layout seems normal."</p>

<div class="website-container">
  <h2>Welcome to School Verification</h2>
  <p>Please log in to access your account:</p>

  <div class="login-container">
    <h2>School Login</h2>
    <form id="loginForm" onsubmit="return false;"><!-- Prevent form submission -->
      <div class="form-group">
        <label for="username">Username:</label>
        <input type="text" id="username" name="username" placeholder="Enter your username">
      </div>
      <div class="form-group">
        <label for="password">Password:</label>
        <input type="password" id="password" name="password" placeholder="Enter your password">
      </div>
      <button type="submit">Log In</button>
    </form>
  </div>
</div>
```

Fake Login Form: The form contains fields for a username and password, but the onsubmit="return false;" attribute is used to block any form submissions, as this is a mock-up designed purely for educational purposes. This ensures the audience remains focused on the analysis rather than interacting with functional forms.



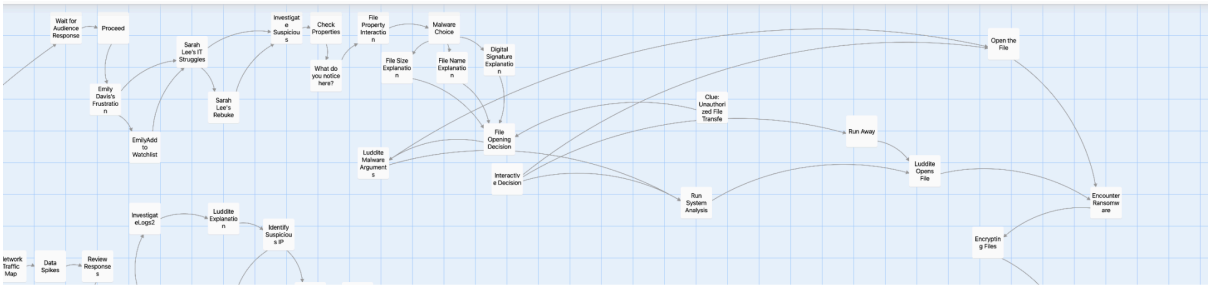
Code and Visualisation of Login Box

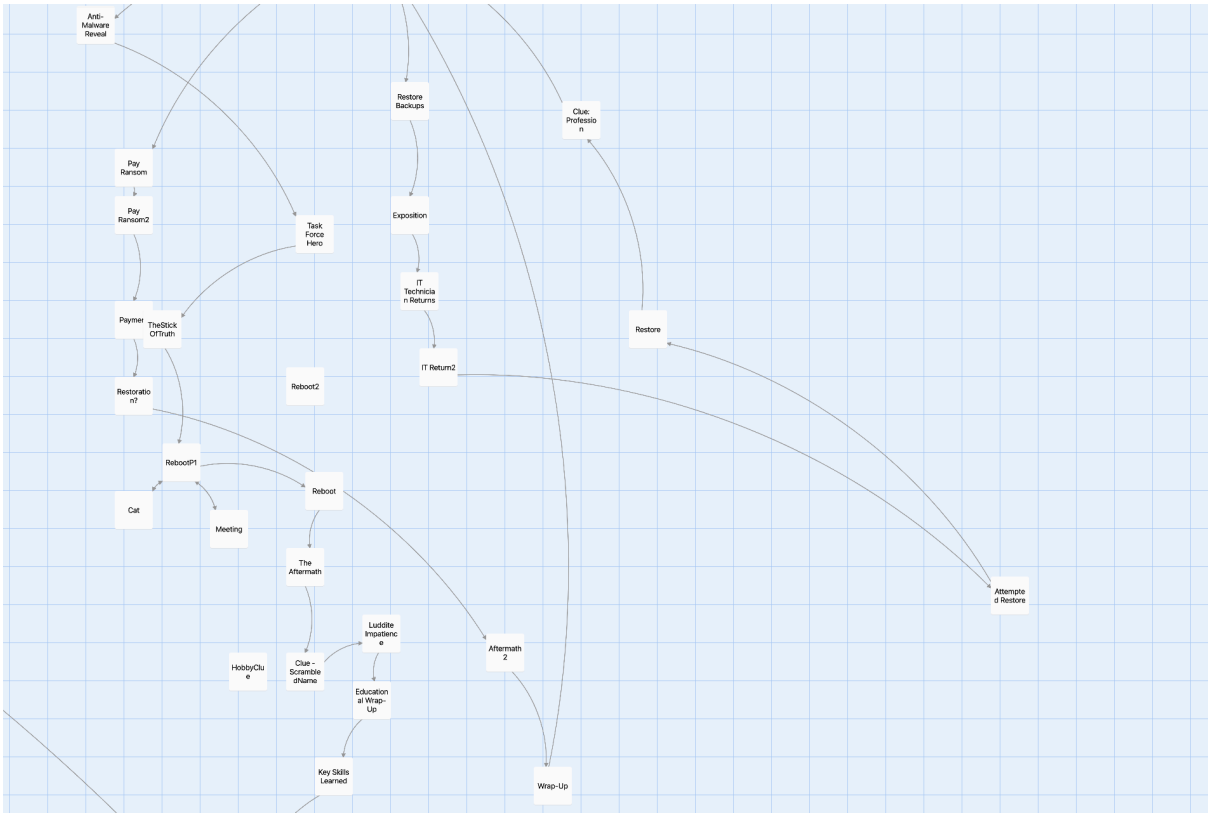
The audience engages with this content through dialogue provided by the Task Force Leader and Task Force Member. They analyse the fake page and point out that it has no immediate red flags, encouraging the audience to think critically about how even legitimate-looking websites can be deceptive.

Wrapping Up the Phishing Investigation

Once all parts of the phishing investigation, headers, links, and sender, are completed the variable $checkedMainContent is set to true and the audience is redirected to the main vote node, where the phishing option is no longer selectable. This allows the investigation to shift focus to other aspects of the case, continuing the story's progression.

Malware Branch



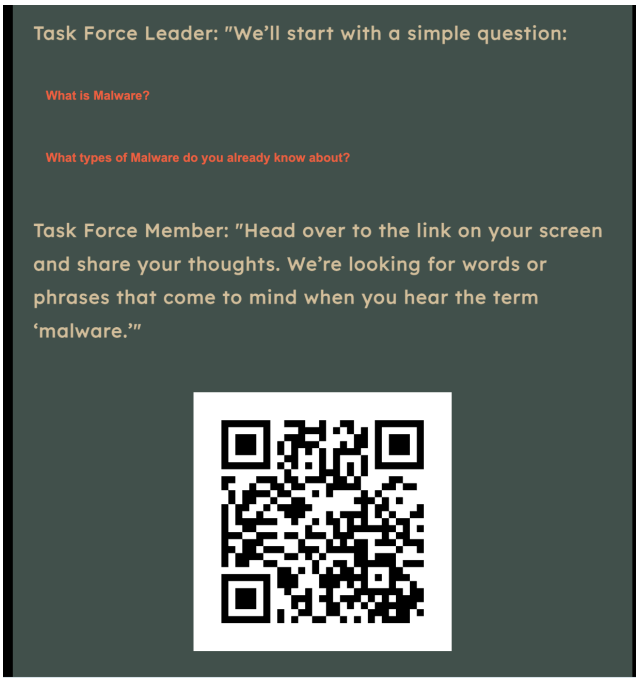


Malware Branch

Malware Branch: Introduction and Audience Engagement

The Malware Branch opens with the Task Force Leader introducing malware and assessing the audience's knowledge. To prompt reflection, the Task Force Leader encourages the audience to consider their understanding of malware. A QR code is displayed, allowing participants to scan and respond via a Mentimeter poll. This

interactive poll aligns with established pedagogical practices, integrating inquiry-based learning and reinforcing the play's educational objectives.



Malware Branch Appearance

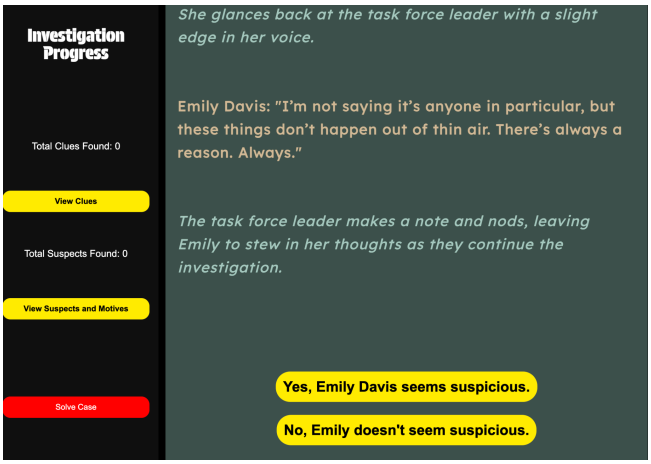
Mentimeter Visuals

Malware Branch: Emily Davis and Sarah Lee

In the Malware Branch, the audience interacts with both Emily Davis, the Headteacher, and Sarah Lee, the IT support staff. These interactions are influenced by the player's decisions, particularly whether or not Emily Davis is marked as a suspect. This branching narrative is achieved through the use of variables and conditional logic to dynamically adjust the dialogue and story progression.

Emily Davis' Suspect Status

When the audience first interacts with Emily Davis, they are presented with dialogue options that allow them to assess her behaviour. If the player finds her suspicious, her suspect status is updated and stored in a variable.




```
(set: $suspectsFound to $suspectsFound + 1)
<!-- Set the variable for "Emily Davis" to true -->
(set: $suspect3_found to true)
```

Suspect Emily Davis

Dynamic Dialogue with Sarah Lee

Based on whether Emily Davis has been flagged as a suspect, the dialogue with Sarah is dynamically altered. If Emily is a suspect, she interjects during the conversation, blaming Sarah for mishandling the IT systems. This branching dialogue creates a more immersive and responsive narrative experience.

```
<!-- Check if Emily Davis is a suspect -->
{
  (if: $suspect3_found is true)[
    <p class="s_direction">Emily Davis interjects, her voice sharp.</p>

    <p class="speech"><b>Emily Davis:</b> "If Sarah had been more diligent about maintaining the systems, we might not be in this situation. She's been aware of these issues for months!"</p>

    <p class="s_direction">Sarah looks taken aback by the accusation, feeling the weight of the blame.</p>
  ]
}

<p>
  {
    (if: $suspect3_found is true)[
      [[Sarah Lee's Rebuke->Sarah Lee's Rebuke]]
    ]
    (else:)[
      [[Investigate Suspicious Document->Investigate Suspicious Document]]
    ]
  }
</p>
```

Dynamic Dialogue 3

In this code, the conditional logic checks the value of $suspectEmilyDavis. If she is marked as a suspect, her dialogue is triggered, adding tension and shifting blame onto Sarah. Otherwise, the conversation proceeds without Emily's interference.

Investigating the Malware File Properties

Investigating the Malware File Properties

The Task Force shifts focus to a suspicious file, ImportantDocument.exe, believed to be part of the malware attack. The audience is tasked with analysing the file properties, mirroring cybersecurity professionals.

The file appears harmless, but its properties reveal key suspicious elements:

- It's an executable (.exe) mislabeled as a "document."
- It lacks a digital signature, and the publisher is unknown.
- The file attempts to connect to an external IP address (192.168.1.45), typical of malware communication.

After reviewing these details, the Task Force Leader asks the audience to provide observations on what makes the file suspicious. Using Mentimeter, the audience offers real-time feedback, which is then discussed in a group setting.

File Properties Visual

Luddite's Reckless Decision

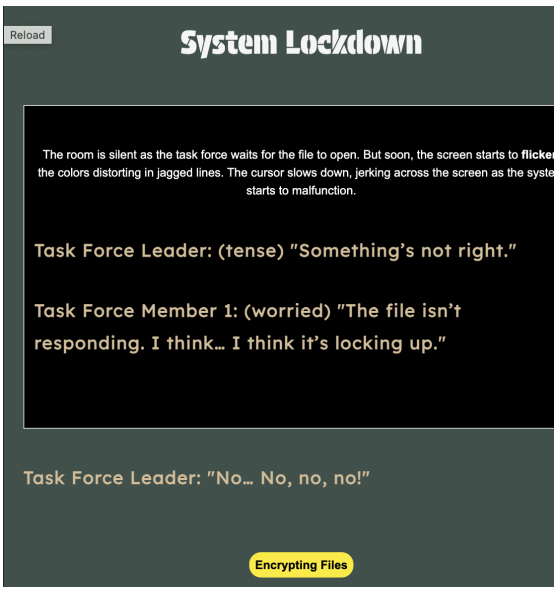
The audience encounters a critical moment when Mr. Luddite suggests opening a suspicious file. This serves as a key educational moment where the Task Force

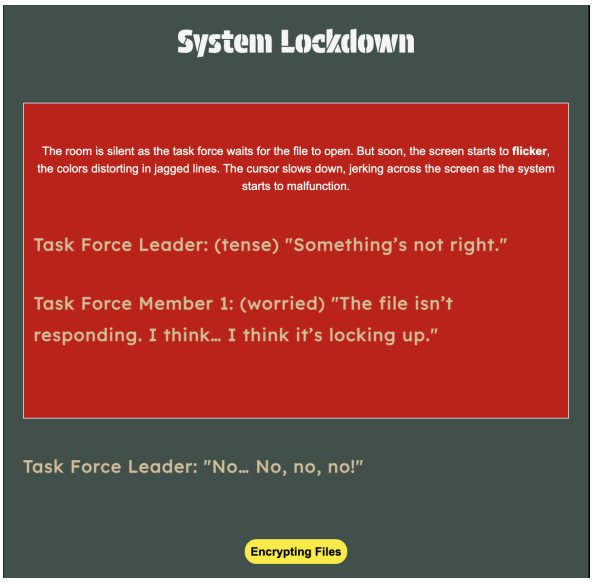
Leader explains the risks of running unverified executables, emphasising best practices in cybersecurity. Despite the warnings, Mr. Luddite ignores protocol and opens the file, triggering a simulated ransomware attack.

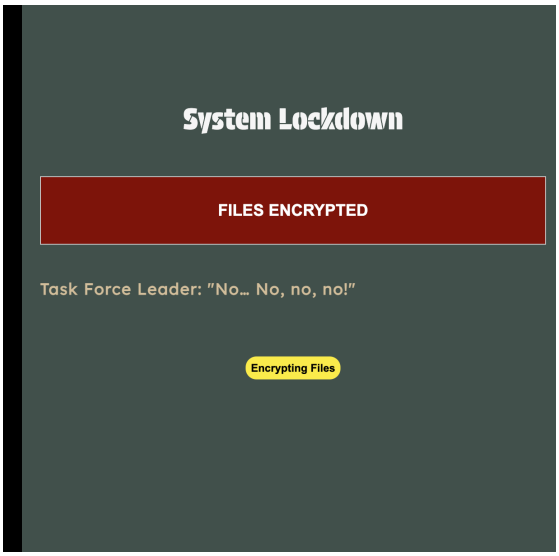
CSS animations simulate the system’s breakdown after the suspicious file is opened. Initially, the screen begins to flicker. The flickering is created with the @keyframes flicker animation, where the opacity of the screen fluctuates rapidly, giving the appearance of a glitching system.

After a few seconds of flickering, the colour transition starts, turning the background from black to red. This is achieved through the @keyframes colorTransition animation, which visually conveys the system's failure and the ransomware attack.

JavaScript timers play a crucial role in pacing the interaction, using setTimeout() functions to control when the flickering stops and when the final message, "Files Encrypted," appears on the screen.







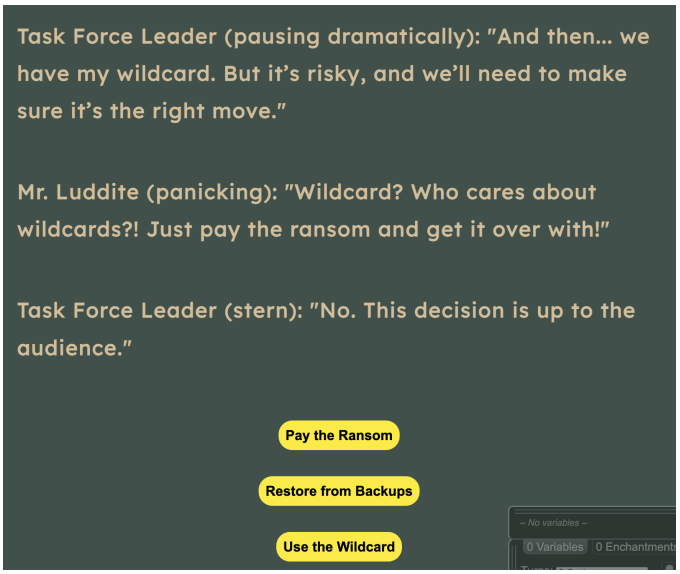
Simulating the Lockdown Visual

```
<style>
    @keyframes flicker {
        0% { opacity: 1; }
        25% { opacity: 0.5; }
        50% { opacity: 1; }
        75% { opacity: 0.5; }
        100% { opacity: 1; }
    }

    @keyframes colorTransition {
        0% { background-color: black; color: white; }
        50% { background-color: red; color: white; }
        100% { background-color: darkred; color: white; }
    }

    #screen {
        animation: flicker 0.1s infinite;
    }
</style>

<script>
    // Simulate flickering and color transition
    setTimeout(() => {
        document.getElementById('screen').style.animation = 'none'; // Stop flickering
        document.getElementById('screen').style.animation = 'colorTransition 2s forwards'; // Start color transition

        // Show the "Files Encrypted" message after the transition
        setTimeout(() => {
            document.getElementById('screen').innerHTML = "<p style='font-size: 36px; font-weight: bold; text-align: center; color: white;'>FILES ENCRYPTED</p>";
        }, 2000); // Show message after 2 seconds of color transition
    }, 3000); // Flicker for 3 seconds before starting the color transition
</script>
```

Code Snippet: Simulating the System Lockdown

Ransomware Decision Point

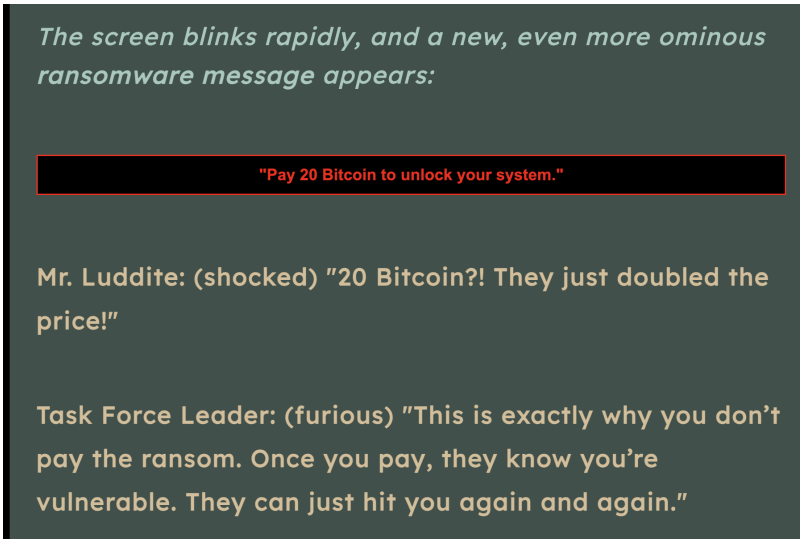
Participants are faced with three choices: pay the ransom, restore from backups, or use a wildcard option. Each decision mirrors real-world cybersecurity scenarios, emphasising decision-making under pressure and highlighting the consequences of each course of action.



Ransomware Pinch Point

Paying the Ransom (The Bad Choice)

The task force initially experiences a false sense of security as the system appears to be restored after paying the ransom.



Paying the ransom consequence

However, the system's brief recovery is a false flag, and the worsening situation is emphasised through dialogue and visual cues. This reinforces the core lesson: paying ransomware demands only leads to further exploitation and exacerbates the problem.

No clues are offered in this branch, as it represents the wrong choice, driving home the point that paying ransomware demands is not a viable strategy in real-world cybersecurity.

Restoring from Backups

Choosing to restore from backups highlights the importance of regular maintenance. The task force interacts with the IT Technician, Alex Johnson, who brings an outdated floppy disk for restoration, humorously emphasising the need for up-to-date IT resources. If Alex Johnson has been flagged as a suspect, his dialogue becomes more aggressive, reflecting frustration. If not, his demeanour is more humorous.

The dynamic dialogue system for Alex Johnson is managed by a conditional statement that checks whether he has been added to the suspect list. This is controlled by the **$suspect1_found** variable, which tracks whether the audience previously flagged Alex during the Phishing Branch. Depending on this variable’s state, Alex's dialogue alters to reflect either frustration (if he's flagged as a suspect) or humour (if not flagged).

```
<h1>IT Technician Returns with the Floppy Disk</h1>

<!-- Check if Alex Johnson is a suspect -->
{
  (if: $suspect1_found is true)[
    <p class="speech"><b>Alex Johnson:</b> (aggressively) "Yeah, I told you it wouldn't work! Nobody ever listens to me around here!"</p>
  ]
  (else:)[
    <p class="speech"><b>IT Technician:</b> (nervously, barely audible) "It's... it's my first day."</p>
  ]
}

<p class="speech"><b>Mr. Luddite:</b> (laughing in disbelief) "A floppy disk?! Please tell me you're joking."</p>

<p class = "s_direction">The task force stares in stunned silence at the floppy disk, then slowly turn to the technician.</p>

<p class="speech"><b>Task Force Member 1:</b> (trying to hold back laughter) "This is what we have to work with?"</p>

<p class="speech"><b>Task Force Leader:</b> (grimacing) "It's all we've got. Let's give it a shot."</p>

<p>[[Attempted Restore]]</p>

<p>(display: "Sidebar")</p>
<p>(display: "SidebarBack")</p>
```

Alex Johnson Dynamic Speech

Restoring from backups leads to the discovery of scrambled metadata containing a clue about the hacker's profession. The message changes based on the audience's path and requires decoding later in the play.

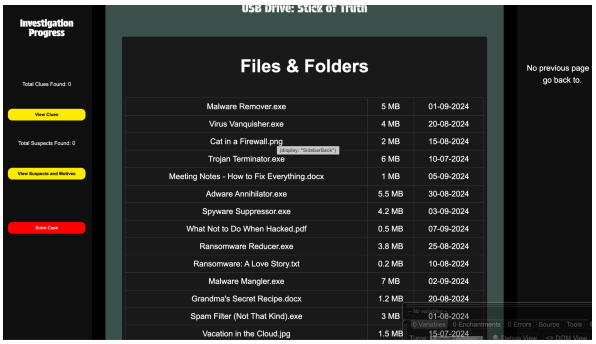
```
<h1>Clue: Hackers Profession</h1>

<p class="speech"><b>Task Force Member:</b> "There's <strong>some</strong> good news Sir! While you were doing that i've been going over the  metadata in the system logs. We have found a clue about the hacker's profession! It's scrambled but...if we can unscramble it!"</p>

<p class="speech"><b>Task Force Leader:</b> "That's a significant lead. If we can identify the hacker's professional role, it might narrow down our list of suspects."</p>

<p class="speech"><b>Task Force Member:</b> "Analyzing the techniques and the type of access used, we've pinpointed their role."</p>

<p class="s_direction">
  The hacker's professional role is revealed as <span class="clue">{
  (if: $suspectNum is 1)[Frpsxwhu Whfkqlfldq] <!-- Computer Technician -->
  (else-if: $suspectNum is 2)[Xdxyjr Firnsnxywfytw] <!-- System Administrator -->
  (else-if: $suspectNum is 3)[Liehxiegliv] <!-- Headteacher -->
  (else-if: $suspectNum is 4)[Fgrwva Jgcfvgcejgt] <!-- Deputy Headteacher -->
  (else-if: $suspectNum is 5)[PA Zbwwvya] <!-- IT Support -->
  (else-if: $suspectNum is 6)[Rohxgxogt/Skjog Yvkiogroyz] <!-- Librarian/Media Specialist -->
  (else-if: $suspectNum is 7)[School Student] <!-- Audience Member -->
  (else-if: $suspectNum is 8)[Ivbq-Bmkpvwtwog lldwkibm] <!-- Anti-Technology Advocate -->
  (else:)[Unknown]
}</span>.

</p>
[[Continue]]

(if: $clue5_found is not true)[
  (set: $clue5_found to true)
  (set: $cluesFound to $cluesFound + 1)
]
```

Hackers Profession Clue Code

Anti-Malware Reveal

the audience interacts with a file explorer on the "Stick of Truth," a USB drive containing a mix of legitimate and humorous files. The correct choice is selecting any of the .exe files, which reinforces the importance of recognising file types and using the appropriate tools to tackle malware.

The audience selects files from the list, and based on the file type (.exe, .png, .docx), different actions are triggered. This interaction is managed using JavaScript, where clicking on a file type shows a relevant message and additional links. Selecting an .exe file correctly advances the scene and reveals the next step in the investigation.



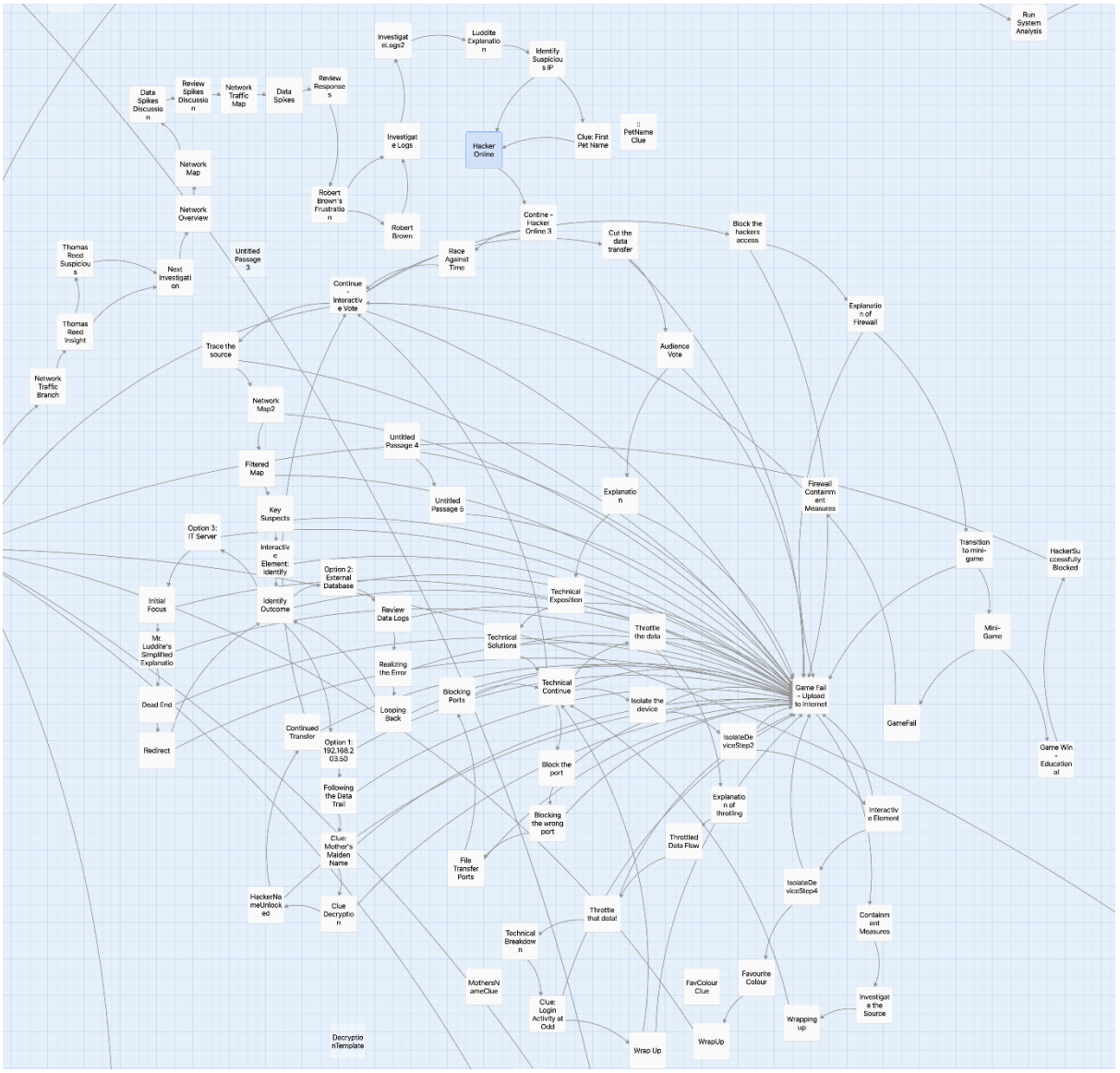
Anti Malware tools on the Stick of Truth

After choosing the correct file, the fourth clue—the hacker’s scrambled name—appears. This clue is generated using the Caesar cipher function from previous sections.

```
<p class="s_direction">
  The hacker's scrambled name is <b><span class="clue">{
    (if: $suspectNum is 1)[Doha Mrkqvrq] <!-- Alex Johnson
encrypted -->
    (else-if: $suspectNum is 2)[Ofrnj Ufwpjw] <!-- Jamie Parker
encrypted -->
    (else-if: $suspectNum is 3)[Iqmpc Hezmw] <!-- Emily Davis
encrypted -->
    (else-if: $suspectNum is 4)[Wkrpdv Uhhh] <!-- Thomas Reed
encrypted -->
    (else-if: $suspectNum is 5)[Zhyho Sll] <!-- Sarah Lee
encrypted -->
    (else-if: $suspectNum is 6)[Xuhkxz Hxuct] <!-- Robert Brown
encrypted -->
    (else-if: $suspectNum is 7)[<p id="output"></p>] <!--
Reference to user input for Suspect 7 -->
    (else-if: $suspectNum is 8)[Rwvibpiv Tcllqbm] <!-- Jonathan
Luddite encrypted -->
    (else:)[Unknown]
  }</span></b>.
</p>
```

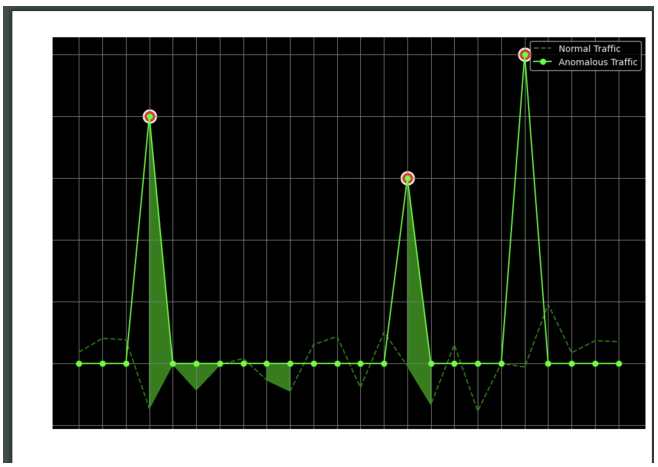
Hackers Scrambled Name Clue

Network Traffic Analysis



Network Traffic Branch Overview

The Network Traffic Node is the most technically complex, simulating a network attack where the hacker uploads sensitive documentation to the internet. This branch uses realistic network traffic behaviour to educate students on recognising anomalies and understanding real-time threats.



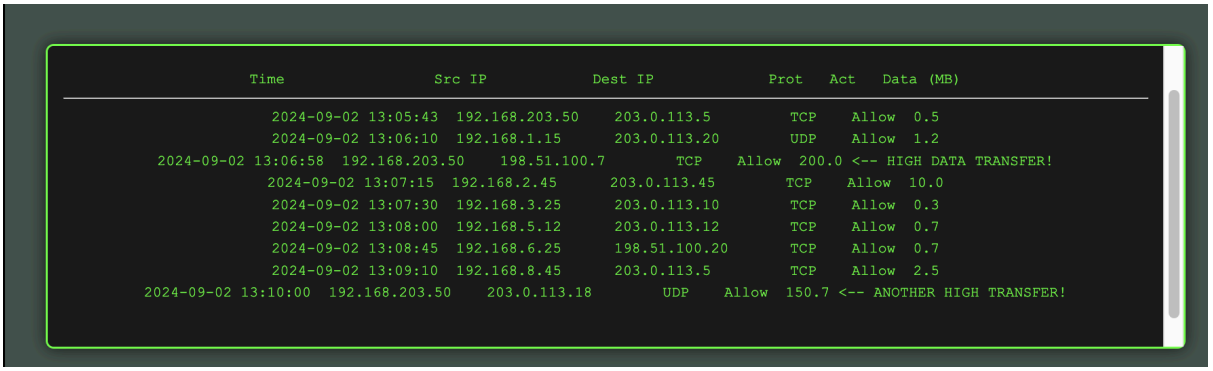
Simulating Suspicious Traffic Spikes

This branch introduces Thomas Reed (Deputy Headteacher) and Robert Brown (Librarian/Media Specialist). Both suspects have access to critical systems and resources, and again their dialogue dynamically changes based on earlier decisions.

Network Traffic Branch

Students analyse network traffic logs to identify a suspicious IP address, enhancing their cybersecurity awareness by simulating real-world data exfiltration scenarios.

The audience reviews a log of data transfers between internal and external IP addresses, identifying which IP shows malicious behaviour, such as high upload rates. Correctly identifying the suspicious IP (192.168.203.50) unlocks the next clue, "First Pet Name", contributing to the hacker’s identity investigation.



Network Traffic Log

Log Structure

The logs are presented in a table format with fields:

- Time: Timestamp for each entry.
- Src IP: Source IP address initiating the data transfer.
- Dest IP: Destination IP address receiving the data.
- Prot: Protocol used (TCP, UDP).
- Act: Firewall action (Allow/Deny).
- Data (MB): Amount of data transferred, with unusually high transfers indicating potential malicious activity.

The logs are stored in an array (logEntries), and the addLogEntry() function appends them to the display at randomised intervals (1 to 3 seconds) using setTimeout(). This gradual, unpredictable log addition simulates real-time network activity. The container scrolls automatically to mimic live network monitoring tools, keeping new entries visible.

```
<p class="speech"><b>Task Force Leader:</b> "These logs are like the digital fingerprints of every device on the network. If someone's been moving large amounts of data, the logs will show us when, where, and how."</p>

<div class="log-container">
  <pre class="network-logs" id="logs">
Time          Src IP        Dest IP         Prot  Act  Data (MB)
------------------------------------------------------------------------------------------
  </pre>
</div>

[[Continue->Luddite Explanation]]

<script>
// Define the log entries array globally
const logEntries = [
    "2024-09-02 13:05:43  192.168.203.50    203.0.113.5         TCP    Allow  0.5",
    "2024-09-02 13:06:10  192.168.1.15      203.0.113.20        UDP    Allow  1.2",
    "2024-09-02 13:06:58  192.168.203.50    198.51.100.7        TCP    Allow  200", // Potential large data transfer
    "2024-09-02 13:07:15  192.168.203.50    203.0.113.45        TCP    Allow  5.0",
    "2024-09-02 13:07:30  192.168.203.50    203.0.113.10        TCP    Allow  0.3",
    "2024-09-02 13:08:00  192.168.203.50    203.0.113.12        TCP    Allow  15.7", // Potential large data transfer
    "2024-09-02 13:08:45  192.168.1.25      198.51.100.20       TCP    Allow  0.7",
    "2024-09-02 13:09:10  192.168.203.50    203.0.113.5         TCP    Allow  10.5", // Potential large data transfer
    "2024-09-02 13:10:00  192.168.203.50    203.0.113.18        UDP    Allow  2.3"
];

// Function to add a new log entry to the logs
function addLogEntry() {
    const logsElement = document.getElementById('logs');
    if (logsElement && logEntries.length > 0) {
        const newLog = logEntries.shift(); // Get the next log entry
        logsElement.textContent += '\n' + newLog; // Append the new log entry

        // Scroll to the bottom of the logs to show the new entry
        const logContainer = document.querySelector('.log-container');
        logContainer.scrollTop = logContainer.scrollHeight;

        // Schedule the next log update at a random interval (1 to 3 seconds)
        const nextInterval = Math.random() * 2000 + 1000; // Random between 1000ms and 3000ms
        setTimeout(addLogEntry, nextInterval);
    }
}

// Start adding logs after a short delay, only if the logs element is present
if (document.getElementById('logs')) {
    setTimeout(addLogEntry, 1000); // Start after 1 second
}
</script>
```

Network Log Code

Clue: First Pet Name

The hacker used a pet name Unknown as part of their security setup. This is a test placeholder to show that the clue system is working.

Task Force Member: "Sir! While combing through the user logs, we found a password recovery prompt. It's asking for the name of the user's first pet. A bit old-school, but it looks like our hacker is relying on traditional security questions."

```
{<p class="s_direction">
  (if: $suspectNum is 1)[The hacker used the pet name <span class="clue">Rex</span> as part of their security setup.]
  (else-if: $suspectNum is 2)[The hacker used the pet name <span class="clue">Milo</span> as part of their security setup.]
  (else-if: $suspectNum is 3)[The hacker used the pet name <span class="clue">Buddy</span> as part of their security setup.]
  (else-if: $suspectNum is 4)[The hacker used the pet name <span class="clue">Max</span> as part of their security setup.]
  (else-if: $suspectNum is 5)[The hacker used the pet name <span class="clue">Lucy</span> as part of their security setup.]
  (else-if: $suspectNum is 6)[The hacker used the pet name <span class="clue">Oscar</span> as part of their security setup.]
  (else-if: $suspectNum is 7 and $suspect7FirstPet is not "")[The hacker used the pet name <span class="clue">(print: $suspect7FirstPet)</span> as part of their security setup.] <!-- Reference to user input -->
  (else-if: $suspectNum is 8)[The hacker used the pet name <span class="clue">Shadow</span> as part of their security setup.]
  (else:)[The hacker used a pet name <span class="clue">Unknown</span> as part of their security setup. This is a test placeholder to show that the clue system is working.]
</p>
}
```

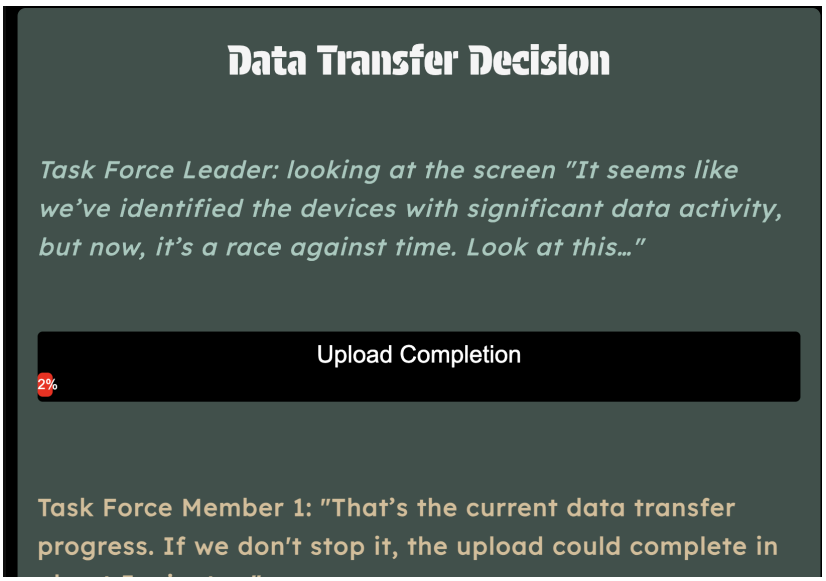
Uncovering the Clue

Data Transfer Decision: A Real-Time Challenge

In this critical scenario, students must race against the clock to stop a data upload and prevent sensitive school information from being leaked. This section simulates a

real-world network attack, utilising a dynamically updating progress bar and multiple decision points to create an urgent, high-pressure experience.

The upload progress is represented by a JavaScript-powered progress bar, which updates continuously. The timer is initiated as soon as the scene begins, and it controls the speed at which the data upload progresses. If the students fail to act within the time limit, the branch is locked, simulating the failure to prevent the data breach.



Upload Bar Visual

```
<script>
      // Ensure global harloweVariables is accessible
      if (!window.harloweVariables.timerProgress) {
          window.harloweVariables.timerProgress = 0; // Initialize if not set
      }

      // Initialize the timer progress from Harlowe variable, or 0 if not set
      let progress = window.harloweVariables.timerProgress;

      // Adjust timeRemaining for 300 seconds (5 minutes)
      let timeRemaining = 300 * (1 - progress / 100); // Total time: 300 seconds

      const updateProgressBar = () => {
          document.getElementById('progressBar').style.width = `${progress}%`; // Update progress bar width
          document.getElementById('progressBar').textContent = `${Math.floor(progress)}%`; // Update text inside the bar
      };

      // Function to hide all other links except the fail link
      const hideOtherLinks = () => {
          // Select all Twine links and hide them, but keep the fail link visible
          document.querySelectorAll('tw-link, tw-enchant').forEach(link => {
              if (link.closest('#failLink') === null) { // Ensure we don't hide the fail link
                  link.style.display = 'none';
              }
          });
      };

      // Call this function to start the timer
      const startTimer = () => {
          const timerInterval = setInterval(() => {
              if (timeRemaining > 0) {
                  timeRemaining--;
                  progress = ((300 - timeRemaining) / 300) * 100; // Calculate progress from 0% to 100%
                  updateProgressBar();

                  // Update the Harlowe variable
                  window.harloweVariables.timerProgress = progress; // Persist progress
              } else {
                  clearInterval(timerInterval); // Stop the timer when it reaches 100%
                  progress = 100;
                  updateProgressBar();

                  // Hide all other links and show the fail link
                  hideOtherLinks();
                  document.getElementById('failLink').style.display = 'block';
              }
          }, 1000);
      };

      // Start the timer automatically
      startTimer();
  </script>
}
```

JavaScript Code for Progress Bar

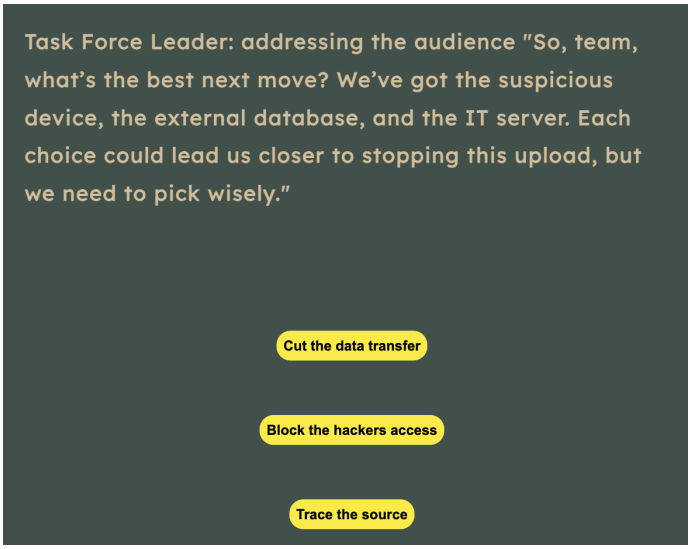
Key Technical Elements:

1. **Timer Setup:** The timer counts down from 300 seconds, updating the visual display by counting to 100% to reflect the urgency of the situation. This timer is a global variable that persists across all nodes within the Network Traffic Branch.

2. **Progress Bar Mechanism:** The progress bar advances incrementally, tied to the timer. The data upload percentage increases proportionally as time passes, simulating the real-world progression of a network breach.

Decisions: Multiple Pathways to Success or Failure

Students are offered multiple strategies to stop the data leak. Failure leads to branch lockout and missed clues, while success reveals critical information. This turns cybersecurity into a high-stakes game, where time management and strategy are essential.



Options to stop the upload

Post-Breach Briefing: Consequences and Reflections

If students fail to stop the upload, the post-breach dialogue emphasises the importance of vigilance and planning in cybersecurity. Mr. Luddite reacts to the failure:

- Mr. Luddite: "I… I can’t believe it! It's out there, all of the data’s out there, and you couldn’t stop it."

The Task Force Leader refocuses on resilience and learning:

- Task Force Leader: "No one person can stop every attack, and no system is foolproof. What matters now is what we do next."

This dialogue reinforces that cybersecurity is an ongoing process, and even failures provide valuable learning opportunities. The team shifts focus to containment measures, giving students a realistic view of the post-breach phase.

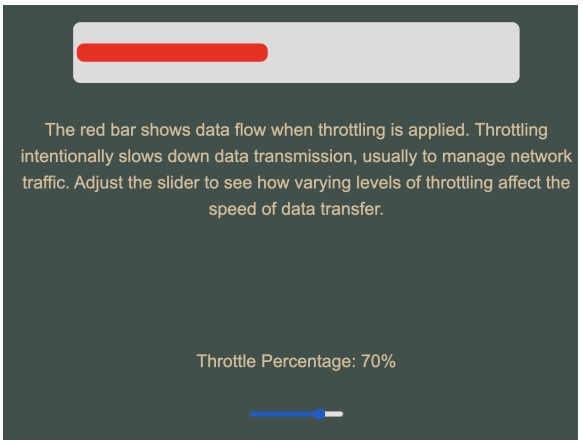
Throttled Data Flow Mini-Game

The Throttled Data Flow mini-game tasks students with managing data flow by adjusting a slider to simulate throttling.

The progress bar reflects real-time changes in data flow speed based on the selected throttle percentage. Using JavaScript, the throttle is controlled by an input slider, with higher throttle percentages slowing the data transfer. This teaches students how throttling impacts network traffic and introduces a way to slow down (but not stop) a hacker's data flow.

Key Technical Elements:

1. Slider-Controlled Throttle: The slider input adjusts the throttle percentage, with the value passed to a function that updates the data flow speed. The higher the throttle, the slower the progress bar updates.
2. Real-Time Feedback: The progress bar's width updates in intervals, providing immediate visual feedback to students.

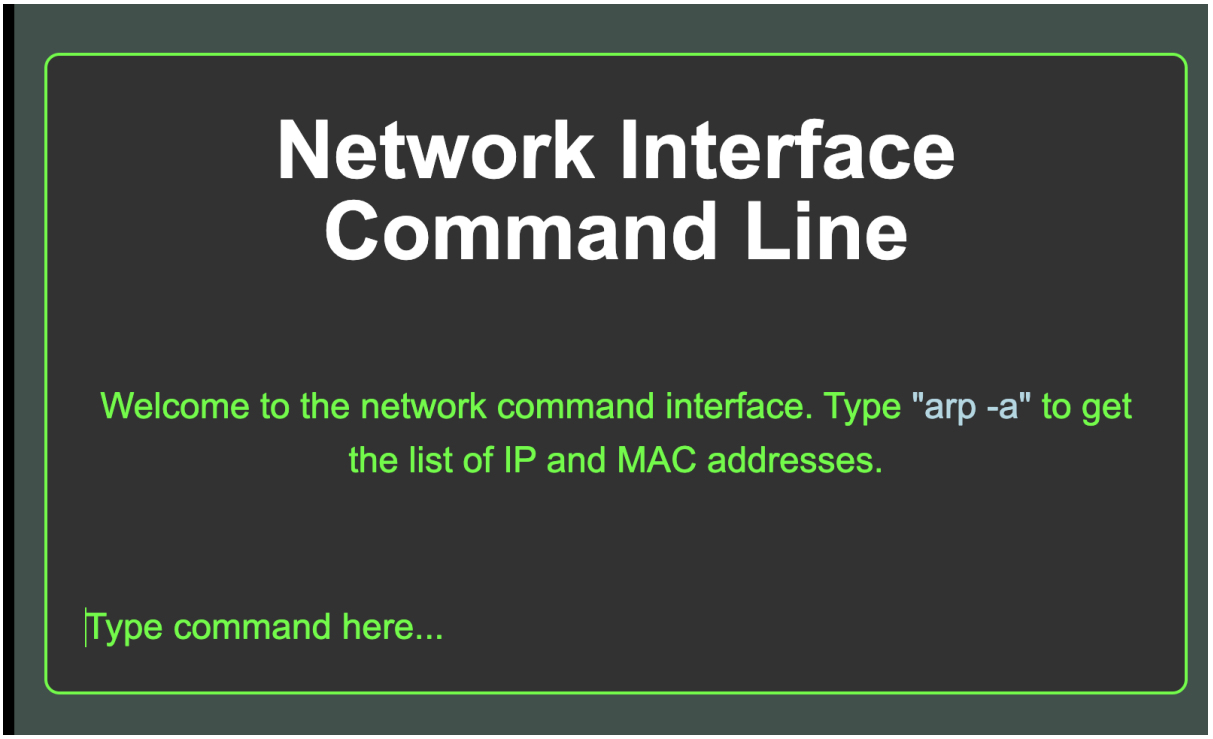


Throttling the data visual

```
<script>
      const throttledProgressBar = document.getElementById('throttled-progress');
      const throttleSlider = document.getElementById('throttle-slider');
      const throttleValue = document.getElementById('throttle-value');
      let throttledProgress = 0;

      function updateThrottledProgress() {
          if (throttledProgress < 100) {
              // Adjust speed based on throttle percentage but ensure it only slows down and doesn't go backward
              let throttleFactor = 1 - (throttleSlider.value / 100); // Throttling factor (0 to 1)
              throttledProgress += 0.5 * throttleFactor; // Progress slower with higher throttle
              throttledProgressBar.style.width = `${Math.min(throttledProgress, 100)}%`;
          }
      }

      // Update displayed throttle percentage value
      throttleSlider.addEventListener('input', function() {
          throttleValue.innerText = throttleSlider.value;
      });

      // Update throttled progress every 100 milliseconds
      setInterval(updateThrottledProgress, 100);
  </script>
```

Throttling JavaScript Code

Command Line Interface: Isolating a Device



Command Line Interface Mini-Game

This mini-game simulates real-world network forensics, teaching students how to find IP addresses and quarantine compromised devices.

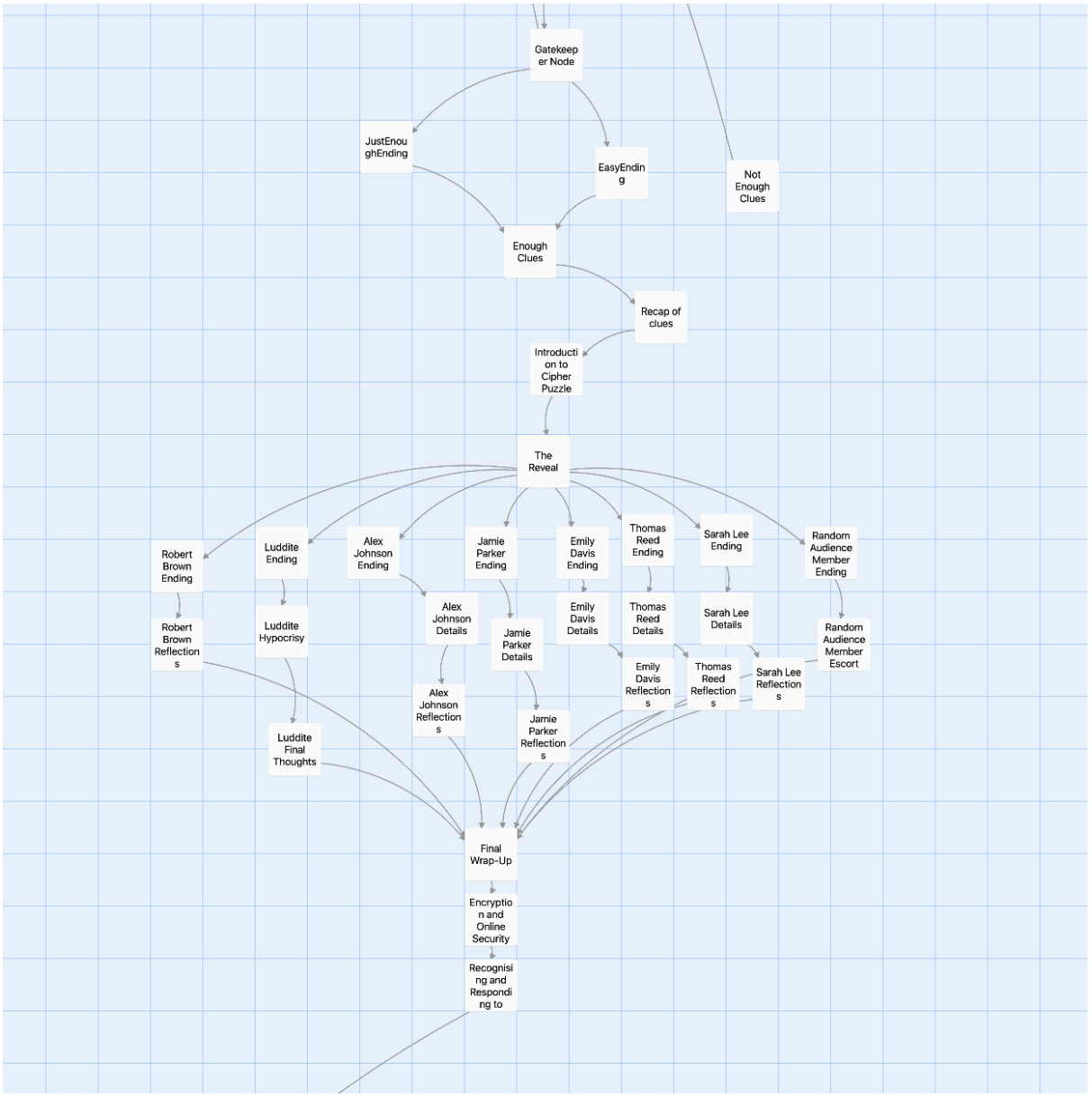
The terminal interface allows students to input basic network commands, such as listing devices and isolating suspicious IP addresses. Using JavaScript, the game tracks student input and updates the screen based on their progress.

The student inputs MAC addresses to isolate suspicious devices. The game checks the entered MAC address against a predefined list. Incorrect entries are handled with error messages, simulating real-world command-line errors.

```
<script>
    // Ensure global harloweVariables is accessible
    if (!window.harloweVariables.timerProgress) {
        window.harloweVariables.timerProgress = 0; // Initialize if not set
    }

    // Initialize the timer progress from Harlowe variable, or 0 if not set
    let progress = window.harloweVariables.timerProgress;

    // Adjust timeRemaining for 300 seconds (5 minutes)
    let timeRemaining = 300 * (1 - progress / 100); // Total time: 300 seconds

    const updateProgressBar = () => {
        document.getElementById('progressBar').style.width = `${progress}%`; // Update progress bar width
        document.getElementById('progressBar').textContent = `${Math.floor(progress)}%`; // Update text inside the bar
    };

    // Function to hide all other links except the fail link
    const hideOtherLinks = () => {
        document.querySelectorAll('tw-link, tw-enchant').forEach(link => {
            if (link.closest('#failLink') === null) {
                link.style.display = 'none';
            }
        });
    };

    // Call this function to start the timer
    const startTimer = () => {
        const timerInterval = setInterval(() => {
            if (timeRemaining > 0) {
                timeRemaining--;
                progress = ((300 - timeRemaining) / 300) * 100; // Calculate progress from 0% to 100%
                updateProgressBar();

                // Update the Harlowe variable
                window.harloweVariables.timerProgress = progress; // Persist progress
            } else {
                clearInterval(timerInterval); // Stop the timer when it reaches 100%
                progress = 100;
                updateProgressBar();

                // Hide all other links and show the fail link
                hideOtherLinks();
                document.getElementById('failLink').style.display = 'block';
            }
        }, 1000);
    };

    // Start the timer automatically
    startTimer();

    const commandInput = document.getElementById("commandInput");
    const responseDiv = document.getElementById("response");
    const twineLink = document.getElementById("twine-link");

    let step = 1; // Track the current step in the process
    let success = false; // Track whether the game was successful

    const commands = {
        "arp -a":
`IP Address       MAC Address
-----------------------------------
192.168.1.10      00:14:22:01:23:45
192.168.1.11      00:14:22:67:89:AB
192.168.1.12      00:14:22:11:22:33
192.168.203.50    00:14:22:77:88:99  <-- Suspicious Device`,
        "192.168.203.50": "<span class='blue-text'>Correct! Now type 'isolate 00:14:22:77:88:99' to isolate the suspicious device.</span>",
        "isolate 00:14:22:77:88:99": "<span class='success-text'>Isolating device with MAC address 00:14:22:77:88:99... SUCCESS!</span>",
        "default": "<span class='blue-text'>Error: Invalid command. Try again.</span>"
    };

    // Function to update console
    function updateConsole(message) {
        responseDiv.innerHTML += `<p>${message}</p>`;
        responseDiv.scrollTop = responseDiv.scrollHeight; // Auto-scroll to bottom
    }

    // Event listener for user input
    commandInput.addEventListener("keydown", function(event) {
        if (event.key === "Enter") {
            const userCommand = commandInput.value.trim();
            commandInput.value = ""; // Clear input field

            if (step === 1 && userCommand === "arp -a") {
                updateConsole("> " + userCommand);
                updateConsole(commands["arp -a"]);
                updateConsole("<span class='blue-text'>Next, type the IP address of the suspicious device:</span>");
                step = 2; // Move to next step
            } else if (step === 2 && userCommand === "192.168.203.50") {
                updateConsole("> " + userCommand);
                updateConsole(commands["192.168.203.50"]);
                step = 3; // Move to next step
            } else if (step === 3 && userCommand === "isolate 00:14:22:77:88:99") {
                updateConsole("> " + userCommand);
                updateConsole(commands["isolate 00:14:22:77:88:99"]);

                // Show the next link after successful isolation
                twineLink.style.display = 'block'; // Show Twine link after success
                twineLink.scrollIntoView(); // Ensure the link is visible on the screen
                success = true; // Mark the game as successful
            } else {
                updateConsole("> " + userCommand);
                updateConsole(commands["default"]);
            }
        }
    });
</script>
```

JavaScript code snippet for Command Line

Solving Case

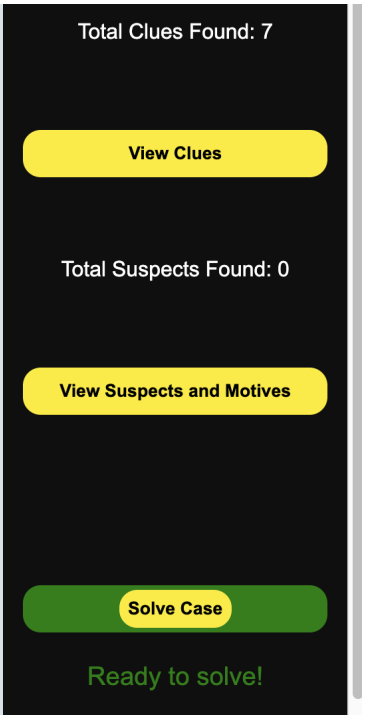


Solving Case Twine Integration

The Solve Case button acts as the final stage of the investigation, allowing players to solve the case based on the clues they've gathered. Once all branches have been completed the main Vote Node is locked, and players can only attempt solving the case.

Solve Case Button Activation

The button becomes available after accumulating at least three clues. Players are rewarded for thorough exploration, as more clues lead to a higher chance of solving the case (in reality this chance percentage does not change).



Case Ready to Solve

Once the button is clicked, the Gatekeeper Node evaluates the number of clues and adjusts the narrative:

- Fewer than 3 clues: Players are told they lack sufficient information and must gather more evidence.
- 3 to 5 clues: The team feels incomplete but proceeds with a reasonable guess, creating tension.
- More than 5 clues: The Task Force is confident, with the evidence clearly pointing to the hacker.

```
<!-- Between 3 and 5 clues -->
(else-if: $cluesFound >= 3 and $cluesFound < 5)[
  <div>
    <p class="speech"><b>Task Force Member 1:</b> "It's a tough call, but I think we might have just enough information to proceed. We've uncovered a fair number of clues, but there are still some gaps in the story."</p>

    <p class="speech"><b>Task Force Leader:</b> "Agreed. We don't have all the answers, but we've got enough to form a hypothesis. The suspicious logs, the encrypted messages—it's starting to come together, even if the full picture isn't clear yet."</p>

    <p class="speech"><b>Task Force Member 2:</b> "We might not know everything, but the clues we've gathered are pointing us in a direction. It's risky, but we have enough to make an informed guess."</p>

    <p class="speech"><b>Task Force Leader:</b> "This isn't a perfect case, but we're not completely in the dark. We've uncovered key motives, methods, and we can piece together the hacker's strategy. It's time to trust our instincts and move forward."</p>

    <p class="speech"><b>Task Force Member 1:</b> "Right. It's now or never. Let's connect the dots and see if we can bring this case to a close."</p>

    <p>[[Continue->JustEnoughEnding]]</p>
  </div>
]

<!-- More than 6 clues -->
(else-if: $cluesFound >= 5)[
  <div>
    <p class="speech"><b>Task Force Member 1:</b> "We've gathered everything we need. There's no doubt—we have more than enough to solve this case. The hacker has left a trail, and we've followed it right to their doorstep."</p>

    <p class="speech"><b>Task Force Leader:</b> "Exactly. Every clue we've collected fits perfectly together: the encrypted messages, the strange software, the unauthorized file transfers. We know the motive, the method, and the perpetrator."</p>

    <p class="speech"><b>Task Force Member 2:</b> "There's no ambiguity here. We've got hard evidence, and we can confidently close this case. We've done more than just uncover the clues—we've understood the hacker's entire plan."</p>

    <p class="speech"><b>Task Force Leader:</b> "Great work, team. This was a complex case, but with the amount of evidence we've gathered, we're in a position to not only identify the hacker but ensure they're brought to justice. It's time to wrap this up."</p>

    <p class="speech"><b>Task Force Member 1:</b> "Let's make the call and put an end to this. We've worked hard, and now it's time to see the results of our efforts."</p>

    <p>[[Continue->EasyEnding]]</p>
  </div>
]
```

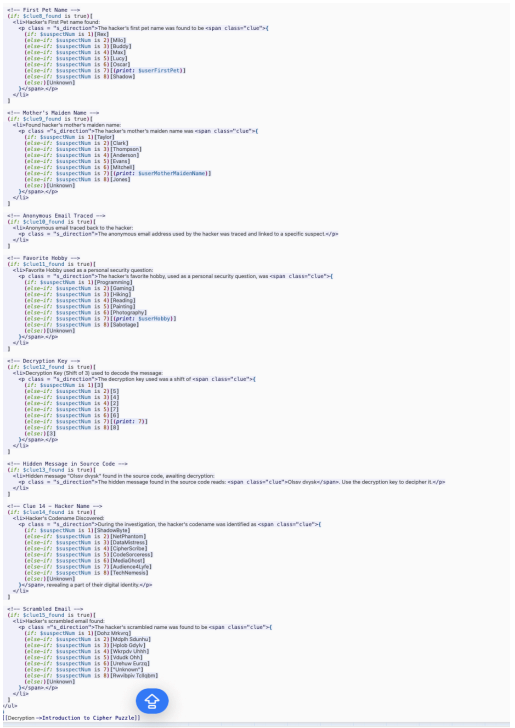
Dynamic Dialogue for Gatekeeper Node

This mechanic offers flexible gameplay, promoting thorough investigation, and enhances replayability by varying the outcomes. It mirrors real-world cybersecurity problem-solving, where success depends on gathering comprehensive evidence.

Clue Recap

Before solving the case, players are presented with a Clue Recap summarising the clues they've discovered. This checkpoint ensures that players have a clear overview of their progress.

Using conditional logic the clues are listed dynamically using if conditions to determine which clues to show. This recap helps players organise their findings and ensures they are making an informed decision before proceeding to solve the case.



Clue Recap Page Code Snippet

Cipher Puzzle

Cipher Page Visual

Cipher Puzzle: Interactive Decryption Challenge

Following the Clue Recap, the Cipher Puzzle provides an interactive, educational experience where players use gathered clues to decipher the hacker's encrypted name and role. This puzzle emphasises problem-solving and critical thinking.

The interface consists of two main sections:

- Left Column: Displays dynamic suspect information, including encrypted details like the name, role, and hacker name, based on the player's investigation.
- Right Column: Contains the Cipher Decryption Area, where players input the encrypted name and decryption key to solve the puzzle.

Players use the clues they've found to decrypt the hacker's name:

- Encrypted Input: Players enter the encrypted name.
- Decryption Key: Players input the cipher key (shift value) discovered during the investigation.
- Decrypt Button: Clicking this performs the decryption via a Caesar Cipher algorithm, revealing the decrypted name.
- Reset Button: Allows players to retry or correct input.

```
<script>
  document.getElementById('decryptButton').addEventListener('click', function() {
    // Get the input values
    var encryptedText = document.getElementById("encryptedInput").value;
    var shift = parseInt(document.getElementById("decryptKey").value);
    var result = '';

    // Decrypt the input using Caesar Cipher
    for (var i = 0; i < encryptedText.length; i++) {
      var c = encryptedText[i];

      // Only shift letters
      if (c.match(/[a-z]/i)) {
        // Get ASCII code
        var code = encryptedText.charCodeAt(i);

        // Uppercase letters
        if ((code >= 65) && (code <= 90)) {
          c = String.fromCharCode(((code - 65 - shift + 26) % 26 + 26) % 26 + 65); // Adjusted for correct backward shift
        }
        // Lowercase letters
        else if ((code >= 97) && (code <= 122)) {
          c = String.fromCharCode(((code - 97 - shift + 26) % 26 + 26) % 26 + 97); // Adjusted for correct backward shift
        }
      }

      // Append the decrypted character
      result += c;
    }

    // Display the decrypted text
    document.getElementById("decryptedOutput").innerHTML = "Decrypted Name: " + result;
  });

  document.getElementById('resetButton').addEventListener('click', function() {
    // Clear the input fields and output
    document.getElementById("encryptedInput").value = '';
    document.getElementById("decryptKey").value = '';
    document.getElementById("decryptedOutput").innerHTML = "Decrypted Name: ";
  });


      function caesarCipherEncrypt(str, shift) {
        return str.split('').map(char => {
            if (char.match(/[a-z]/i)) {
                const base = char.charCodeAt(0) < 97 ? 65 : 97;
                const encryptedChar = String.fromCharCode(((char.charCodeAt(0) - base + shift) % 26) + base);
                return encryptedChar;
            }
            return char; // Non-letter characters remain unchanged
        }).join('');
    }

    // Automatically encrypt the user's name when the passage loads
    const inputString = window.harloweVariables.userName; // Get the Harlowe variable
    const encryptedString = caesarCipherEncrypt(inputString, 7);

    // Display the output
    document.getElementById('output').innerHTML = encryptedString;

    // Store the result back into a Harlowe variable
    window.harloweVariables.encryptedName = encryptedString; // Store it in a Harlowe variable
</script>
```

Caesar's Cipher Code Implementation

The Reveal and Endings

The Reveal and Endings offer a personalised conclusion to the investigation. Each of the eight possible endings reflects the depth of the narrative, varying based on which suspects were identified. These endings not only resolve the story but also serve as a final educational moment, tying the clues together and providing closure.

Example Endings

Robert Brown Ending: If identified as a suspect, Robert confesses to exploiting his role as Librarian to plant malicious code, criticising the school's lax security. If not suspected, his dialogue is more boastful, mocking the Task Force for failing to catch him.

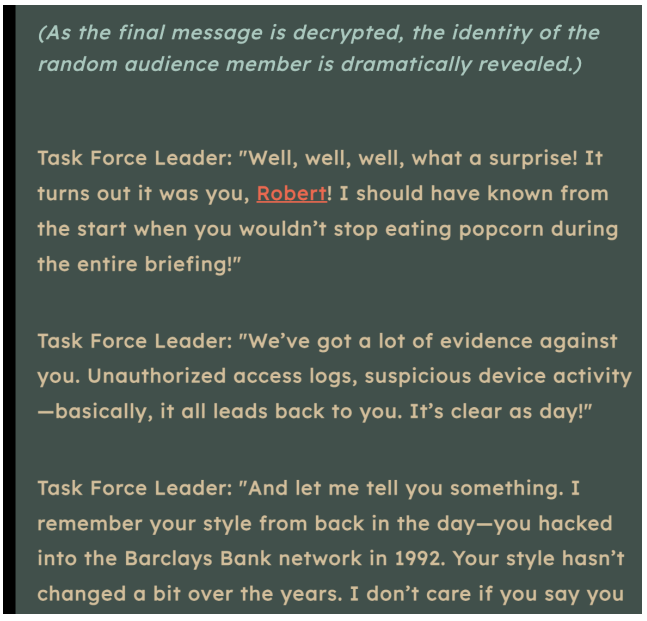
```
<!-- Conditional Dialogue for Suspect Status -->
{
  <!-- If Robert Brown is in the suspects list -->
  (if: $suspect6_found is true)[
    <p class="speech"><b>Robert Brown:</b> "I suppose I underestimated you. You caught me fair and square. As a Librarian and Media Specialist, I exploited my access to the system's media archives to insert malicious code and redirect data streams. I utilized my knowledge of the library's network to bypass security measures and cover my tracks. My intention was to demonstrate the vulnerabilities in our media and data management systems."</p>

    <p class="speech"><b>Task Force Member:</b> "So your primary concern was with how the media and data systems were managed and the security oversights associated with them?"</p>

    <p class="speech"><b>Robert Brown:</b> "Precisely. The lack of adequate security for sensitive information and media assets was alarming. Despite numerous requests for better security protocols, nothing was done. By creating a significant disruption, I hoped to force a reassessment of our data handling and protection practices."</p>

    <p class="s_direction">(Robert appears both determined and regretful.)</p>

    <p class="speech"><b>Task Force Leader:</b> "While your actions did reveal critical security flaws, the method you chose was extreme and disruptive. Addressing these issues through appropriate channels would have been more effective and less damaging."</p>
  ]

  <!-- If Robert Brown is not in the suspects list -->
  (else:)[
    <p class="speech"><b>Robert Brown:</b> "Hah! You think you could catch me? I'm far more clever than you could ever imagine. As a Librarian and Media Specialist, I had the perfect cover. I exploited my access to the system's media archives, inserting malicious code and redirecting data streams without raising suspicion. You never stood a chance!"</p>

    <p class="speech"><b>Task Force Member:</b> "So you used your role as a cover to bypass security measures, all while flaunting your superiority?"</p>

    <p class="speech"><b>Robert Brown:</b> "Exactly! It was all too easy. The lack of adequate security for sensitive information and media assets was laughable. I needed to show everyone how flawed the system was, and I did it with style. Maybe now you'll appreciate the brilliance of my plan."</p>

    <p class="s_direction">(Robert's demeanor is arrogant and unapologetic.)</p>

    <p class="speech"><b>Task Force Leader:</b> "Your actions revealed critical security flaws, yes, but they also caused chaos and harm. There were better ways to address these issues than through malicious actions."</p>
  ]
}
```

Rober Brown Dynamic Ending

Luddite Reveal: Mr. Luddite’s dramatic confession reveals that his chaotic actions were meant to expose the school’s overreliance on technology. His dialogue is humorous yet critical, underscoring the risks of blindly adopting technological solutions without considering broader implications.

Luddite Reveal Ending

Random Audience Member Reveal: For a comedic twist, a random audience member is accused as the hacker. The exaggerated, humorous dialogue adds levity, with the Task Force Leader overreacting and accusing the audience member of impossible feats, offering a memorable and lighthearted conclusion.



Audience Member Ending

Plenary and Final Wrap-Up

The conclusion ensures the educational elements are reinforced, summarising key cybersecurity concepts like encryption, network traffic analysis, and insider threats. The interactive narrative merges gamified storytelling with educational objectives.

Stylistic Implementation

Lexend Deca was selected as the primary font for its readability, especially for dyslexic readers. It features increased letter spacing to reduce "crowding," making letters easier to distinguish. The larger x-height ensures lowercase letters are closer in size to uppercase, aiding identification. Its uniform stroke weight provides consistent thickness, improving legibility, while clear letter shapes help differentiate commonly confused characters like "b" and "d."

Imported via Google Fonts, Lexend Deca was applied to key text elements such as dialogue and stage directions, enhancing accessibility and user experience.

```
/* Import the Google Font for H1 */
@import url('https://fonts.googleapis.com/css2?
family=Protest+Guerrilla&display=swap');
/* Import Lexend Deca from Google Fonts */
@import url('https://fonts.googleapis.com/css2?family=Lexend+Deca&display=swap');
```

Importing Lexend Deca

Styling for Dialogue and Stage Directions

To maintain the script format of Cyber Play, CSS tags "speech" (for dialogue) and "s_direction" (for stage directions) were used. These elements were styled for legibility, especially for dyslexic readers, featuring increased letter spacing, larger font sizes, and high-contrast colours.

These properties enhance accessibility, with line height preventing "line skipping" and letter spacing reducing crowding, ensuring the content is dyslexia-friendly and easy to read.

```
/* Styling for speech */
.speech {
    font-family: 'Lexend Deca', sans-serif; /* Use Lexend Deca for speech */
    font-size: 24px; /* Dyslexia-friendly font size */
    line-height: 1.6; /* Increased line height for readability */
    letter-spacing: 0.05em; /* Spaced-out letters */
    font-weight: bold; /* Bold text for speech */
    color: #D6BD98; /* Speech text color */
    margin: 10px 0; /* Add space above and below */
    text-align: left; /* Align speech to the left */
}

/* Styling for stage directions */
.s_direction {
    font-family: 'Lexend Deca', sans-serif; /* Use Lexend Deca for stage
directions */
    font-size: 24px; /* Dyslexia-friendly font size */
    line-height: 1.6; /* Increased line height for readability */
    letter-spacing: 0.05em; /* Spaced-out letters */
    font-style: italic; /* Italicized text for stage directions */
    color: #A5C9C0; /* Lighter color for stage directions */
    margin: 10px 0; /* Add space above and below */
    text-align: left; /* Align stage directions to the left */
}
```

Speech and Stage Direction Styling

Colour Choices

The dark background (#000000) with lighter text (#D6BD98 for speech and #A5C9C0 for stage directions) ensures high contrast, enhancing readability for users.

Colour Choices on Screen

Media Calls

Although designed for implementation on Large Screens I decided to implement Media to ensure the interface adapts seamlessly across a range of devices. These queries adjust layout, font size, and container widths based on screen resolution.

Key Media Queries

- Large Screens (HDTV or bigger)
    - Query: @media only screen and (min-width: 1600px)
    - Target: Screens 1600 pixels or wider
    - Purpose: To prevent the design from appearing too sparse on large displays by increasing font size, sidebar width, and container padding, ensuring readability and balance.

```
/* ---------------------- MEDIA QUERIES ---------------------- */

/* Large Screens - HDTV or bigger */
@media only screen and (min-width: 1600px) {
    h1 {
        font-size: 4rem;
    }
    .speech {
        font-size: 36px;
        line-height: 1.8;
    }
    .s_direction {
        font-size: 36px;
    }
    #sidebar {
        width: 15%;
        padding: 20px;
    }
    #back-sidebar {
        width: 15%;
        padding: 20px;
    }
    tw-passage {
        max-width: 1200px;
        padding: 40px;
    }
}
```

```
/* Small Screens - Mobile Devices */
@media only screen and (max-width: 768px) {
    h1 {
        font-size: 1.5rem;
    }
    .speech {
        font-size: 18px;
        line-height: 1.4;
    }
    .s_direction {
        font-size: 18px;
    }
    #sidebar {
        width: 100%;
        height: auto;
        position: relative;
        padding: 10px;
    }
    #back-sidebar {
        width: 100%;
        height: auto;
        position: relative;
        padding: 10px;
    }
    tw-passage {
        max-width: 100%;
        padding: 10px;
    }
    img {
        max-width: 100%;
        height: auto;
    }
```

Code For Media Queries (Large and Small)

- Small Screens (Mobile Devices)
    - Query: @media only screen and (max-width: 768px)
    - Target: Screens 768 pixels or smaller (phones, small tablets)
    - Purpose: To optimise readability and usability by stacking sidebars vertically, reducing font size, and making the layout more compact for small screens.

Dynamic Units (rem, em, %)

The project shifted from fixed pixel (px) values to fluid units like rem, em, and percentages (%). These responsive units allow elements to adjust dynamically based on screen size, zoom level, or browser preferences, ensuring a more adaptable and user-friendly interface.

```css
/* Target all H1 elements */
h1 {
    font-family: 'Protest Guerrilla', sans-serif;
    font-size: 2.5rem;
    font-weight: 400;
    color: #F5F5F5; /* Adjust the color as needed */
    text-align: center;
}
```

```css
/* Style for individual passages */
tw-passage {
    width: 100%; /* Full width */
    max-width: 800px; /* Set a max width */
    padding: 20px;
    margin: 10px auto;
    background-color: #40534C; /* Dark background for each passage */
    border-radius: 8px;
    box-shadow: 0 0 10px rgba(0, 0, 0, 0.5); /* Subtle shadow */
    text-align: center; /* Center align the passage content */

    /* Ensure it fills the remaining height of the screen */
    flex: 1 1 auto;
    display: flex;
    flex-direction: column;
    justify-content: center;
}
```

Dynamic Units

Images and Multimedia through Wix

Wix was used to host images and audio, enhancing the interactivity and immersion of the story. Images were embedded into Twine using Wix-hosted URLs. Audio elements, set to auto-play upon opening, added a dynamic layer of engagement.

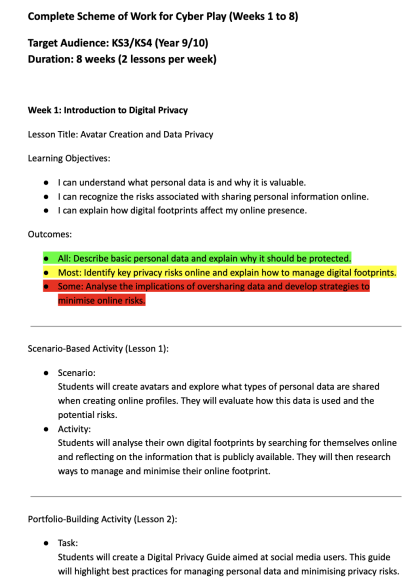
Scheme of Work

The Cyber Play Scheme of Work is an 8-week curriculum designed to introduce students to key cybersecurity concepts. Each week focuses on a different aspect of digital literacy and online safety. The scheme provides teachers with a clear, adaptable roadmap for delivering lessons in an engaging, manageable way.

With 10 years of teaching experience, I understand the importance of simple, effective resources. This scheme is designed to reduce preparation time, offering ready-to-use materials that can be easily tailored to different classroom needs.

High-Level Breakdown

- Week 1: Digital Privacy – Understanding personal data and digital footprints.
- Week 2: Phishing and Social Engineering – Identifying online threats and manipulation tactics.
- Week 3: Network Security – Analysing network traffic for cyber threats.
- Week 4: Online Safety and Digital Footprints – Managing online presence responsibly.
- Week 5: Encryption and Data Protection – Learning encryption techniques for securing sensitive data.
- Week 6: Malware and Cyber Attacks – Recognizing and mitigating malware.
- Week 7: Social Engineering and Online Scams – Deepening understanding of online manipulation.
- Week 8: Final Challenge and Review – Collaborative "cyber escape room" to reinforce learning.



Complete Scheme of Work for Cyber Play (Weeks 1 to 8)

Target Audience: KS3/KS4 (Year 9/10)
Duration: 8 weeks (2 lessons per week)

Week 1: Introduction to Digital Privacy

Lesson Title: Avatar Creation and Data Privacy

Learning Objectives:

- I can understand what personal data is and why it is valuable.
- I can recognize the risks associated with sharing personal information online.
- I can explain how digital footprints affect my online presence.

Outcomes:

- All: Describe basic personal data and explain why it should be protected.
- Most: Identify key privacy risks online and explain how to manage digital footprints.
- Some: Analyse the implications of oversharing data and develop strategies to minimise online risks.

Scenario-Based Activity (Lesson 1):

- Scenario:
  Students will create avatars and explore what types of personal data are shared when creating online profiles. They will evaluate how this data is used and the potential risks.
- Activity:
  Students will analyse their own digital footprints by searching for themselves online and reflecting on the information that is publicly available. They will then research ways to manage and minimise their online footprint.

Portfolio-Building Activity (Lesson 2):

- Task:
  Students will create a Digital Privacy Guide aimed at social media users. This guide will highlight best practices for managing personal data and minimising privacy risks.

Scheme of Work Example

Week 1: Introduction to Digital Privacy

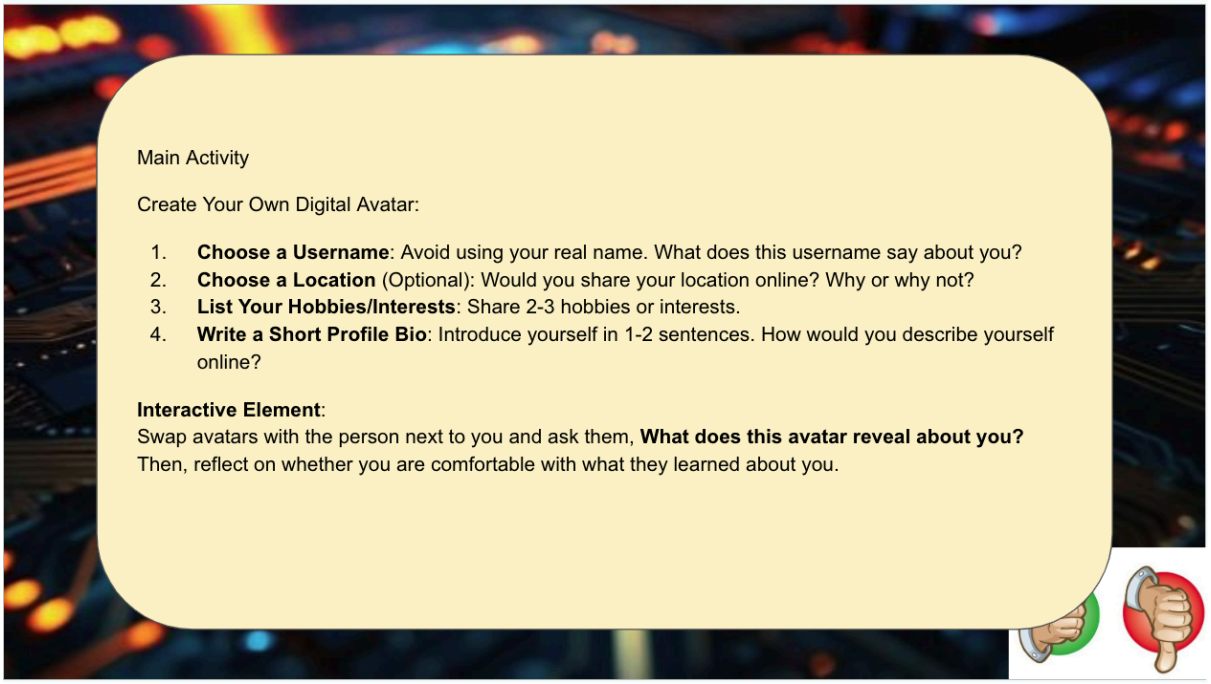
Week 1 introduces students to digital privacy, personal data, and digital footprints, laying the foundation for broader cybersecurity lessons. The activities focus on understanding the risks of oversharing personal information online.

DCF Integration:

- Citizenship: Students understand the implications of sharing personal data and how to safeguard their digital identities.
- Interacting and Collaborating: Group discussions about digital footprints foster reflection on personal data risks.
- Digital Literacy: Students learn to critically assess the online information they share and how it can be misused.

Week 1, Lesson 1: Avatar Creation and Data Privacy (W1L1)

This lesson introduces the concept of personal data and digital footprints. Students create avatars to represent their online identities, reflecting on the risks involved in sharing personal information. Their avatars mirror the characters' digital identities, highlighting how cybercriminals exploit personal data, reinforcing how seemingly harmless information can lead to identity theft or breaches.



Main Activity Week 1 Lesson 1

Main Activity for Week 1, Lesson 1:

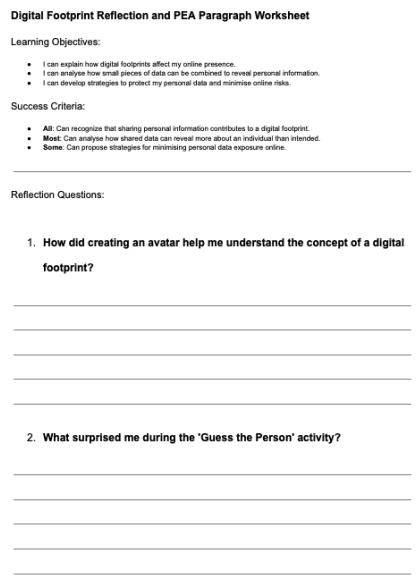
Students create avatars by selecting a username, location, hobbies, and a short bio. This helps them think critically about personal data exposure. A follow-up discussion reveals how easily these details could be used to identify someone.

Week 1, Lesson 2: Guess the Person – Exploring Digital Footprints (W1L2)

Building on the concept of digital footprints, this lesson demonstrates how small pieces of data can reveal a person's identity. Students analyse shared information to understand the implications of their digital footprint, similar to the investigative work they will perform in Cyber Play.

Activities:

Guessing Exercise: Students identify their peers based on avatar details like usernames and hobbies. After each guess, they discuss the clues used for identification, reinforcing the idea that small data points can build a complete identity.



Digital Footprint Reflection and PEA Paragraph Worksheet

Learning Objectives:

- I can explain how digital footprints affect my online presence.
- I can analyse how small pieces of data can be combined to reveal personal information.
- I can develop strategies to protect my personal data and minimise online risks.

Success Criteria:

- **All**: Can recognize that sharing personal information contributes to a digital footprint.
- **Most**: Can analyse how shared data can reveal more about an individual than intended.
- **Some**: Can propose strategies for minimising personal data exposure online.

Reflection Questions:

1. **How did creating an avatar help me understand the concept of a digital footprint?**

2. **What surprised me during the 'Guess the Person' activity?**

Example Resource Week 1 Lesson 2

Example Resource for Week 1, Lesson 2:

PowerPoints for W1L1 and W1L2 guide students through avatar creation and digital footprint analysis. Worksheets and templates help students analyse the personal data they share.

Week 2: Phishing and Social Engineering

Week 2 focuses on phishing and social engineering, teaching students to identify and counter these cyber threats. The lessons build practical cybersecurity skills while drawing parallels to Cyber Play, where students take on the roles of cybersecurity detectives. This approach immerses students in real-world scenarios, allowing them to apply classroom concepts in a simulated environment.

DCF Integration:

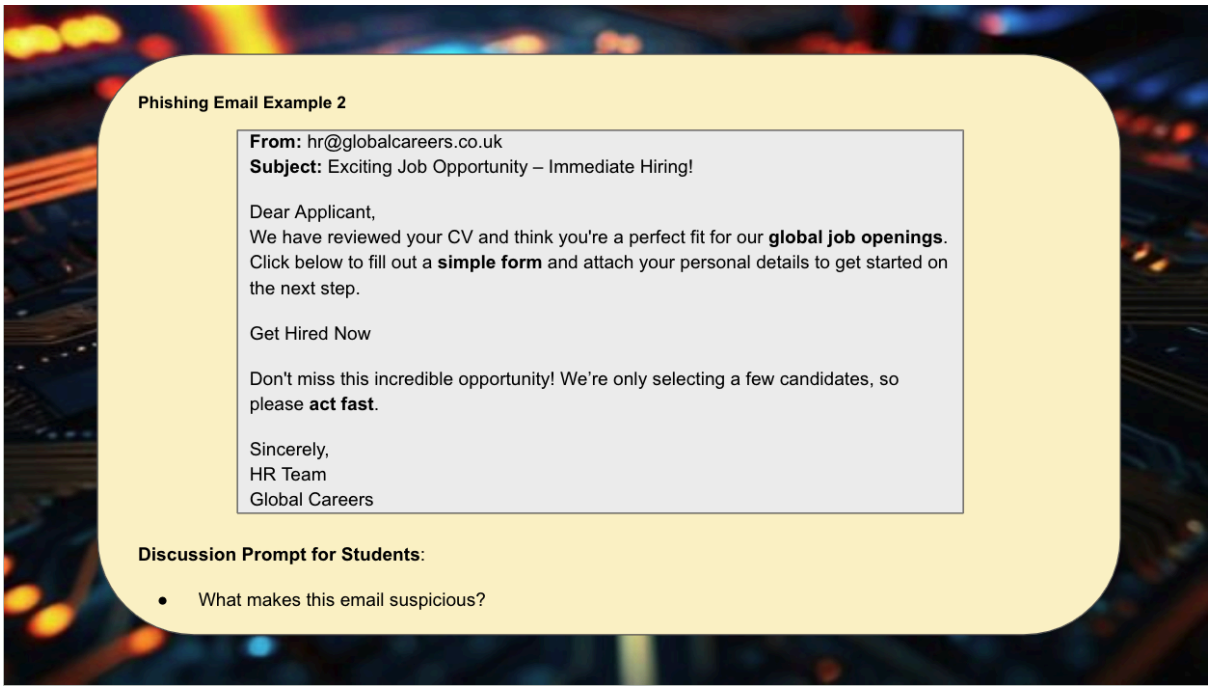
- Citizenship: Understanding ethical online behaviour and how to respond to cyber threats.
- Interacting and Collaborating: Group work encourages teamwork and communication to solve phishing and social engineering problems.
- Digital Literacy: Enhances students' ability to critically analyse digital content and recognise malicious behaviour.

Week 2, Lesson 1: Phishing and Social Engineering Tactics (W2L1)

This lesson introduces students to phishing and social engineering tactics, focusing on identifying and preventing these threats. Students are guided through a real-world phishing email, learning to spot red flags such as suspicious URLs, grammatical errors, and urgent requests. This practical exercise builds Digital Literacy as students critically assess online communications and understand how phishing works.

Main Activity for Week 2, Lesson 1:

By analysing phishing emails and collaborating to identify the "social engineer" in the group, students develop their Interacting and Collaborating skills. Additionally, discussions on the ethical implications of social engineering strengthen their understanding. The lesson concludes by tying classroom activities to Cyber Play, helping students understand how phishing and social engineering work together in real-world cyberattacks.



Week 2, Lesson 2: Creating an Anti-Phishing and Social Engineering Campaign (W2L2)

In this lesson, students take a proactive role by creating an anti-phishing and social engineering campaign where they must educate others about cyber threats. The lesson begins with a recap of phishing and social engineering tactics, linking these concepts back to the challenges faced in the interactive narrative.

Main Activity for Week 2, Lesson 2:

Students collaborate to design anti-phishing campaigns, including infographics, email templates, and social media posts, aimed at raising awareness about phishing and social engineering. This project develops their Digital Literacy, while their teamwork skills are enhanced through Interacting and Collaborating. Students reflect on the ethical challenges of cybercrime, reinforcing their understanding of Citizenship.

The plenary session encourages students to reflect on the "social engineer" role from the previous lesson, further connecting their classroom experience to Cyber Play.

1. Infographic Template (For Campaign Design)

Title: Anti-Phishing and Social Engineering Awareness

Section 1: What is Phishing?

- Brief definition:
  (Example: Phishing is a type of online scam where attackers trick individuals into giving out personal information through fake emails or websites.)

Section 2: Common Phishing Tactics

- List of tactics:
  - Suspicious email addresses.
  - Fake URLs.
  - Urgent language.

Section 3: How to Avoid Phishing Scams

- Tips for avoiding scams:
  - Never click on suspicious links.
  - Verify the sender before responding to emails.
  - Use two-factor authentication for your accounts.

Resource for Week 2 Lesson 2

Week 2 Resources and Integration with the Story

PowerPoint Presentations (W2L1, W2L2): These presentations guide students through phishing email analysis, social engineering simulations, and group discussions, which align with the Cyber Play storyline.

Worksheets and Campaign Templates: Students use these materials to develop their anti-phishing campaigns. A direct connection between classroom activities and the interactive narrative ensures that students' learning experiences are reinforced and applied within the game.

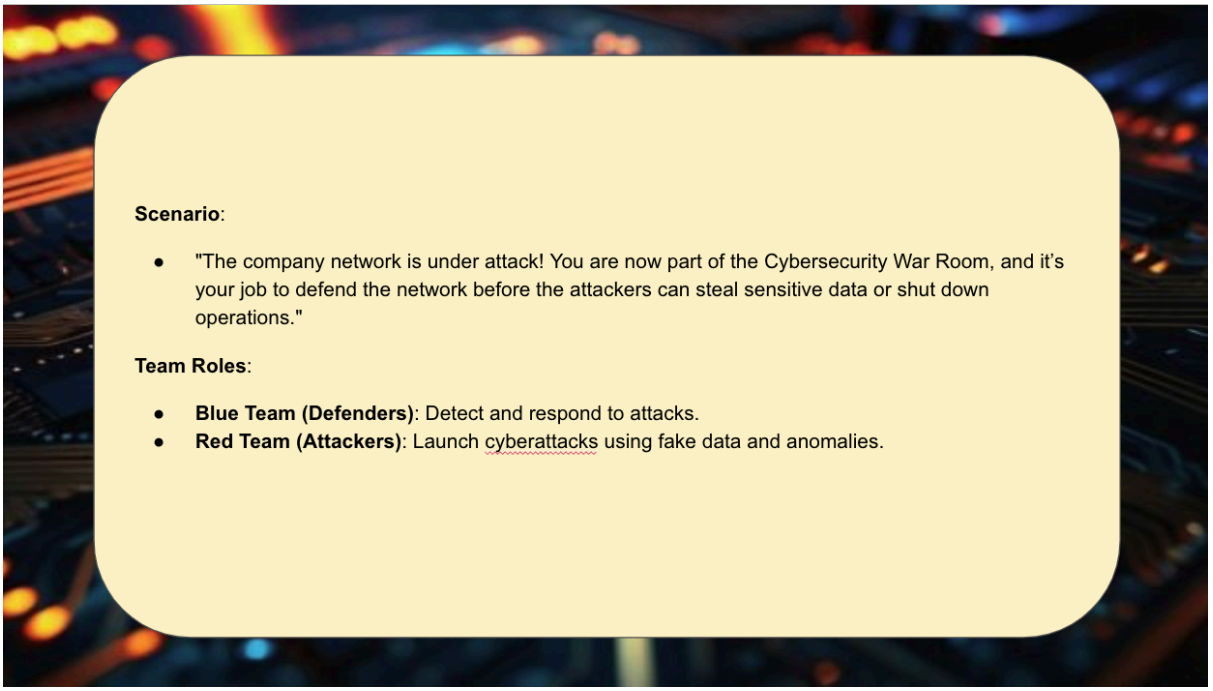
Week 3: Cybersecurity War Room and Network Defense Focus

Week 3 immerses students in practical cybersecurity defence strategies through the "Cybersecurity War Room", a simulation that emphasises real-time network monitoring, incident response, and teamwork. These lessons closely mirror the structure of Cyber Play. This hands-on approach gives students a deeper understanding of network security and incident management in real-world scenarios.

DCF Integration:

- Data and Computational Thinking: Students analyse network traffic, identify patterns, and respond to cyber threats. These activities sharpen their problem-solving and data interpretation skills, preparing them for both classroom challenges and those presented in Cyber Play.
- Citizenship: By focusing on network protection, students gain an understanding of online safety and learn how to respond to cyber threats effectively.
- Interacting and Collaborating: Students are divided into Blue Team (defenders) and Red Team (attackers), working collaboratively to either launch or defend against simulated cyberattacks, providing them with a taste of real-world cybersecurity roles.

Week 3, Lesson 1: Cybersecurity War Room – Red Team vs. Blue Team (W3L1)



This lesson features a live simulation where students are divided into two teams: Red Team (attackers) and Blue Team (defenders). The Red Team attempts to breach the network, while the Blue Team monitors traffic logs in real-time and responds to the attacks. The session begins by assigning roles within the Blue Team: Network Admin, Incident Response Lead, and Security Analyst, each tasked with securing different aspects of the network. Meanwhile, the Red Team plans and executes various cyberattacks such as data exfiltration, DDoS, and reconnaissance.

This real-time activity reinforces how strategic decisions in both the classroom and the play shape the outcome of cyberattacks, making the experience immersive and educational.

Activities

The Blue Team analyses network traffic logs to identify suspicious patterns such as unknown IP addresses or spikes in data transfer, while the Red Team executes attacks.

The Blue Team must take immediate action, such as blocking IP addresses or isolating compromised sections of the network, to prevent the attacks from succeeding.

After the simulation, students participate in a debrief, reflecting on their defence strategies and relating their experiences to the decisions made by Cyber Play characters. This helps deepen their understanding of cyber defence tactics.

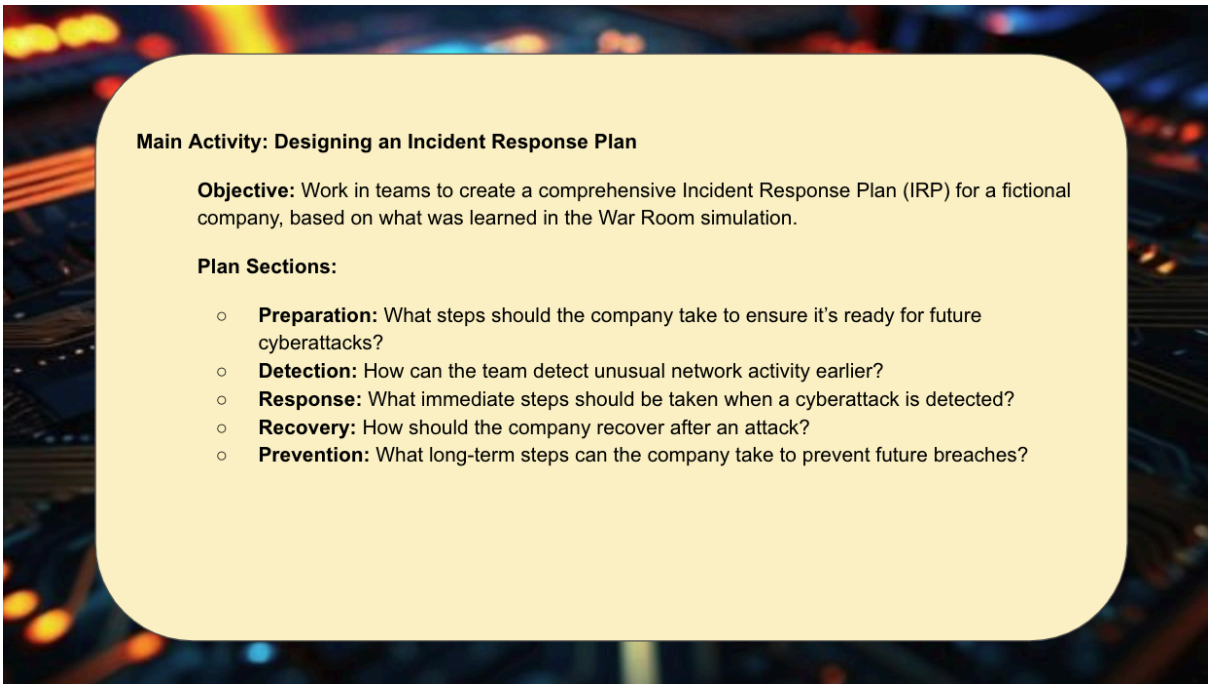
This exercise not only teaches real-time network monitoring and incident response but also integrates with the Cyber Play narrative, giving students a hands-on understanding of cybersecurity principles while reinforcing the skills of teamwork and decision-making under pressure.

Week 3, Lesson 2: Post-War Room – Building a Cyber Defense Strategy (W3L2)

In this lesson, students reflect on their War Room experience and design a comprehensive Incident Response Plan (IRP) aimed at strengthening network defences. The IRP covers key areas such as detection, response, recovery, and prevention of cyberattacks. As students build their defence plans, they mirror the strategic actions of characters in Cyber Play.

The lesson begins with students reflecting on what went right or wrong during the War Room simulation and discussing areas where their defences could be improved. Working in groups, they develop response plans outlining how they would monitor network activity, detect potential threats, and respond to any breaches that occur. Their IRPs also include long-term strategies to prevent future attacks, such as improving firewalls, conducting regular penetration testing, and training staff on security protocols.

Each group presents its IRP to the class, discussing their defence strategies and receiving feedback. This collaborative reflection emphasises the importance of having a robust defence strategy and ties back into the Cyber Play narrative, where the effectiveness of their cybersecurity measures directly impacts their success in stopping future attacks.



Week 3 Main Activity

Resources for Week 3:

- PowerPoint Presentations (W3L1 and W3L2): These presentations guide students through the War Room simulation and Incident Response Plan creation. They ensure that technical concepts, such as network defence, are clearly tied to the Cyber Play narrative, aligning classroom tasks with the story progression.
- Network Traffic Logs and Attack Instructions: Simulated traffic logs and attack instructions provide a realistic experience for both teams.
- Incident Response Plan Templates: These templates help students structure their IRPs, focusing on detection, response, recovery, and prevention.

Week 4: Digital Footprints and Online Safety

In Week 4, students explore the impact of digital footprints and online safety, focusing on how their digital activities can be tracked and exploited, much like characters in Cyber Play. The lessons encourage students to analyse how small online actions contribute to a broader digital identity.

DCF Integration: The lessons incorporate key elements of the Digital Competence Framework (DCF):

- Citizenship: Students learn how digital footprints are formed and reflect on their responsibilities in maintaining online privacy.
- Interacting and Collaborating: By working in groups to analyse case studies, students examine the long-term consequences of digital actions.

- Digital Literacy: The lesson enhances students' critical evaluation of their own online behaviours, teaching them to make informed decisions about managing their digital presence.

Week 4, Lesson 1: Investigating Your Digital Footprint (W4L1)

This lesson introduces the concept of digital footprints, focusing on how every online action leaves a trace that can have long-term impacts on individuals and organisations.

The session begins with students reflecting on their own digital activities, such as social media posts or online purchases, building an understanding of how personal information accumulates to form a digital footprint. This reflection encourages students to consider the potential consequences of their online actions, both positive and negative.

In the main activity, students investigate the digital footprints of public figures, examining how their online behaviour has shaped their reputations. By studying real-life case studies, students develop a practical understanding of how digital footprints can be used or manipulated.

The lesson concludes with a plenary discussion, linking students' findings to the Cyber Play narrative and reinforcing the importance of managing their own digital footprints. This reflection prepares them to apply the same critical thinking when navigating the digital world in the story.

Week 4, Lesson 2: Creating Your Digital Footprint Management Plan (W4L2)

In this lesson, students shift from analysing digital footprints to creating their own Digital Footprint Management Plan.

The lesson starts with a reflection on the previous session, encouraging students to consider how their own digital footprints shape their online identities. They are asked to think about the steps they can take to control their digital presence.

The main activity involves students developing their Digital Footprint Management Plans. They critically assess their own online behaviours and research strategies to monitor, limit, and safeguard their digital footprints, such as adjusting privacy settings or removing outdated accounts.

In the plenary, students share their management plans with the class, discussing the strategies they devised and reflecting on the importance of controlling their digital footprints.

Resources

PowerPoint Presentations (W4L1, W4L2) guide students through the activities, including digital footprint analysis and the creation of management plans. Worksheets provide a framework for students to develop their own strategies. By integrating these resources, students deepen their understanding of online identity management while staying engaged with the story.

Week 5: Cybersecurity and Encryption

Week 5 introduces students to encryption methods, deepening their understanding of how data protection works in cybersecurity. This directly connects with the Cyber Play narrative, allowing students to engage with encryption challenges similar to those faced by cybersecurity professionals. These lessons provide practical skills in safeguarding sensitive information.

DCF Integration: The lessons align with the Digital Competence Framework (DCF), with a focus on:

- Data and Computational Thinking: Students explore various encryption methods and understand their role in protecting data.

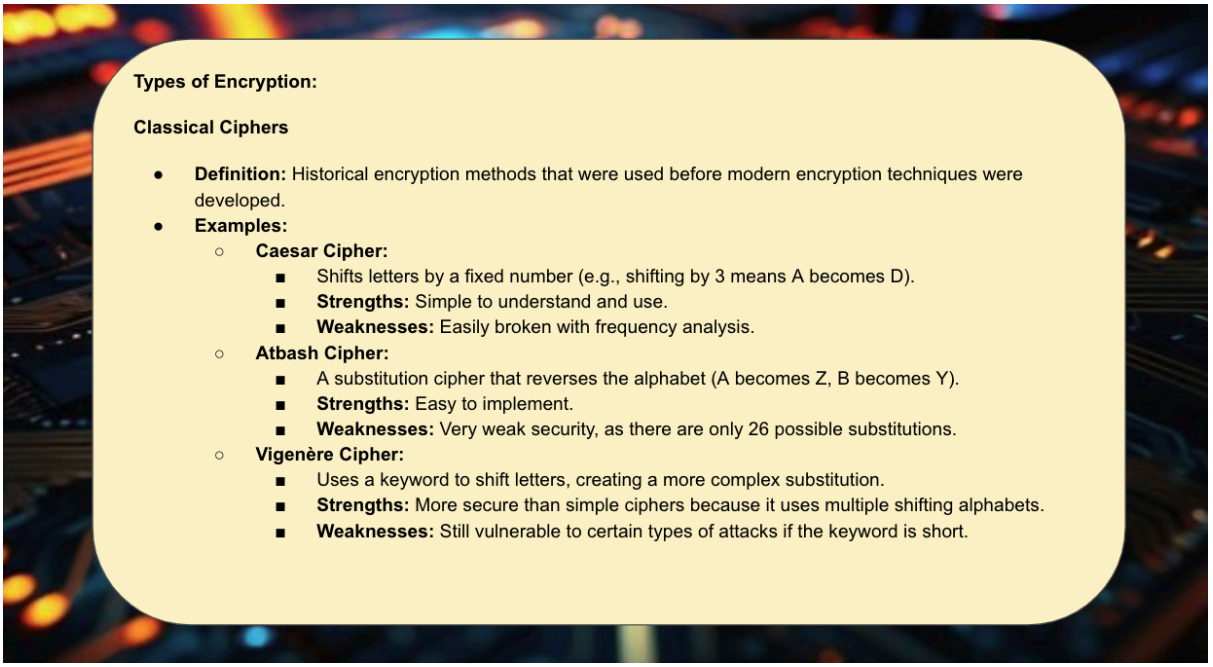
- Citizenship: The lessons highlight the importance of online safety and personal data protection, emphasising practical applications in real-world cybersecurity contexts.

Week 5, Lesson 1: Exploring Encryption Methods (W5L1)

Students explore various encryption methods, such as the Caesar Cipher, Atbash Cipher, Vigenère Cipher, and Substitution Cipher, engaging in activities that reflect the investigative and problem-solving aspects of the Cyber Play storyline. The lesson begins with an overview of encryption and its role in securing data, after which students are divided into groups. Each group is assigned a different encryption method to study, practice, and apply to encode and decode messages. They then prepare a demonstration to present their findings.

The lesson's connection to Cyber Play becomes evident as students engage in problem-solving tasks. This collaborative exercise also mirrors the teamwork required within the narrative, where characters must work together to address

complex cybersecurity challenges.



Week 5 Lesson 1 Explaining Classical Ciphers

Week 5, Lesson 2: Creating an Encryption Best Practices Guide (W5L2)

In this lesson, students consolidate their knowledge of encryption by creating a Best Practices Guide, detailing how encryption works, its importance, and how it can be applied to protect data in real-world situations. The session begins with a reflection on the encryption methods explored in the previous lesson, followed by a discussion on applying these techniques to safeguard data. Students then work individually to compile a guide covering different encryption methods, modern encryption standards (such as AES and RSA), and practical tips for using encryption in personal and organisational settings.

By developing an encryption guide, students directly apply their learning to a practical context. This task challenges students to think critically about how

encryption can be used in diverse scenarios, building their problem-solving skills, which are key to the Cyber Play narrative. The plenary session encourages students to share a key strategy from their guide, fostering collaboration and knowledge-sharing, which are crucial when facing cyber threats, both in the classroom and in Cyber Play.

Section 3: Modern Encryption Methods

- AES (Advanced Encryption Standard):
  - Explanation:

    _____

  - Uses:

    _____
- RSA (Rivest-Shamir-Adleman):
  - Explanation:

    _____

  - Uses:

    _____

_____

Section 4: Best Practices for Encryption

- Practical Advice:
  - _____
  - _____
  - _____
  - _____

Week 5 Lesson 2 Resource

Week 5 Resources and Integration with the Story:

PowerPoint presentations (W5L1, W5L2) guide students through the process of exploring encryption methods and creating their guides, linking these activities back to the strategies used by characters in Cyber Play.

Through group presentations, students share their encryption findings, mirroring the teamwork and communication skills necessary for overcoming cybersecurity challenges in Cyber Play.

Week 6: Malware and Cyber Attacks

Week 6 focuses on identifying, preventing, and responding to malware attacks. Through practical exercises, students gain hands-on experience in recognising and combating various forms of malware, including viruses, ransomware, and spyware. These lessons provide foundational knowledge that students apply both in class and in the simulated world of Cyber Play, where rapid response and teamwork are critical to addressing malware threats.

Digital Competence Framework (DCF) Integration:

- Citizenship: Students learn about the dangers of online threats and how to protect themselves and others from malware.
- Interacting and Collaborating: Group activities emphasise teamwork in identifying and mitigating malware threats.
- Digital Literacy: Students build their understanding of malware, its transmission, and how to prevent or respond to attacks.

Week 6, Lesson 1: Malware Outbreak Simulation – Defend the Network (W6L1)

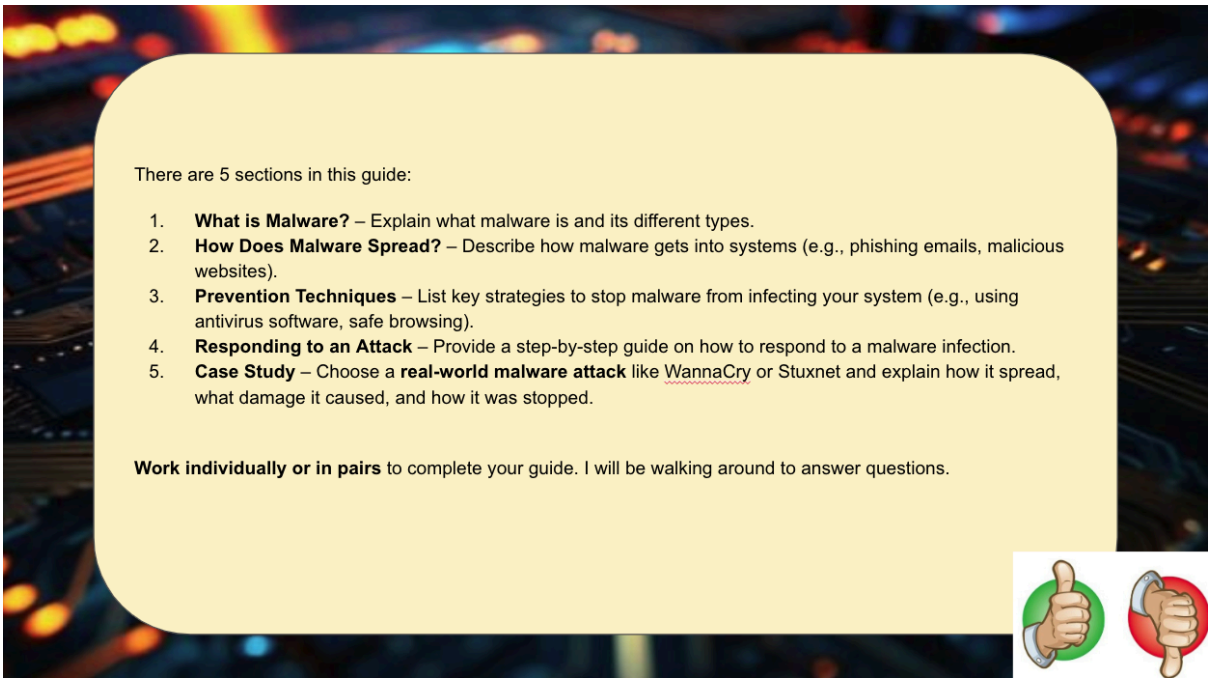
This lesson immerses students in malware identification and containment, focusing on practical responses to cyberattacks. The classroom becomes a "cybersecurity war room," where students take on the role of cybersecurity professionals, reflecting the characters in Cyber Play, who must similarly respond to threats.

The lesson begins with students introduced to different malware types, viruses, ransomware, and spyware, and their potential effects on systems. As the simulation unfolds, they are tasked with identifying the nature of a malware attack based on clues such as suspicious emails, network activity, and compromised files. The focus is on critical thinking and collaboration.

As the malware outbreak intensifies, students must respond quickly, simulating the containment of the attack by disconnecting infected systems and using antivirus software. This fast-paced scenario highlights the importance of coordinated, real-time responses, much like the quick decisions needed in the interactive story.

The lesson concludes with students simulating the restoration of systems using backups, reflecting the recovery phases in Cyber Play. Through this hands-on experience, students develop practical cybersecurity skills while deepening their engagement with the storyline.

Ransomware Detected Powerpoint Slide



Malware Prevention Activity Slide

Following the simulation, students develop a comprehensive guide on preventing and responding to malware attacks. This task builds on the knowledge gained during the simulation and applies it to real-world contexts. The guide they create is intended for use by both individuals and organisations, reflecting the proactive roles characters assume in Cyber Play, where they prepare others to defend against cyber threats.

Students develop strategies for avoiding malware, such as using antivirus software, updating systems, and practising safe browsing. They also analyse the effectiveness of these methods, reinforced by their experience in the simulation. Their guide includes step-by-step response protocols, like isolating infected systems and restoring data.

By creating this guide, students demonstrate their role as cybersecurity defenders in the narrative. This task deepens their understanding of malware while allowing them to contribute to the story by equipping others with knowledge to protect against future cyber threats.

Week 6 Resources and Integration with the Story

PowerPoint presentations for W6L1 and W6L2 guide students through identifying malware and developing prevention strategies. These materials link classroom activities to events in Cyber Play, ensuring that students' learning is embedded in the story.

Malware clue sheets simulate real-world malware symptoms, enabling students to apply their knowledge in both educational and narrative contexts.

Week 7: Social Engineering and Online Scams

In Week 7, students explore advanced social engineering tactics like vishing (voice phishing) and smishing (SMS phishing). They apply their knowledge by developing action plans to protect against these threats. The lessons build on their understanding of psychological manipulation and focus on proactive defence strategies.

DCF Integration

The lessons align with the Digital Competence Framework (DCF) by addressing:

- Citizenship: Exploring ethical issues in online behaviour and protecting against manipulation.
- Interacting and Collaborating: Group work to solve cybersecurity problems, emphasising professional collaboration.
- Digital Literacy: Developing the ability to critically assess social engineering tactics and create response plans.

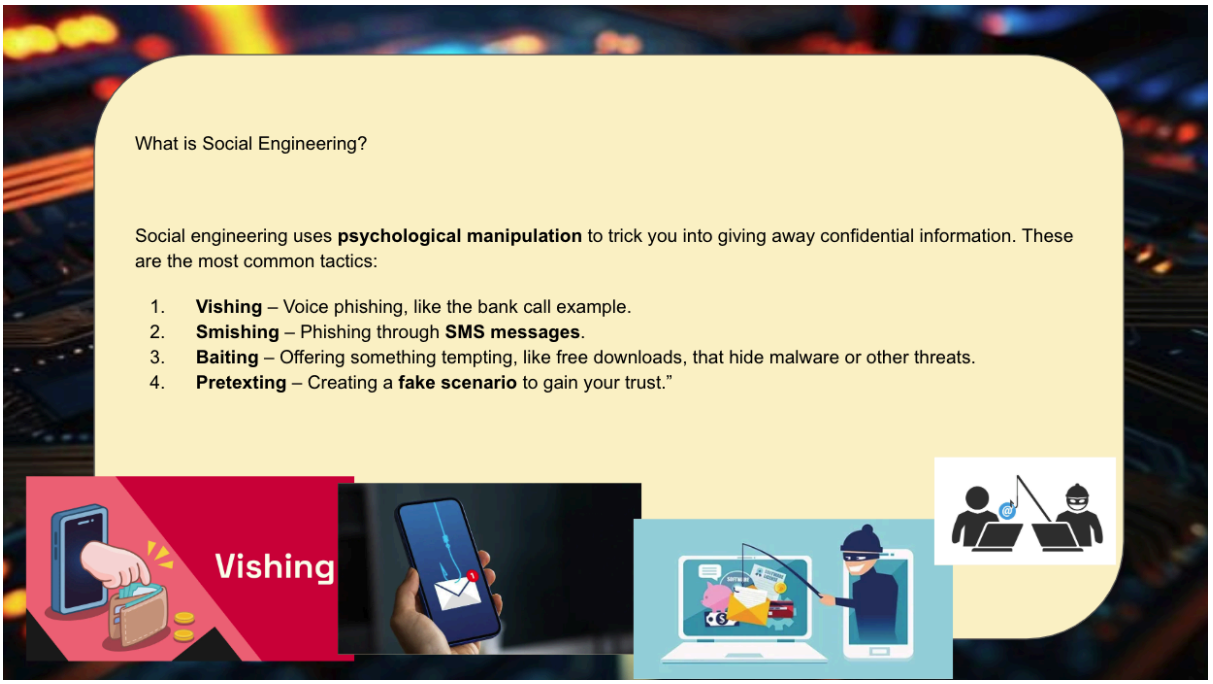
Week 7, Lesson 1: Advanced Social Engineering Tactics (W7L1)

In this lesson, students explore advanced social engineering techniques like vishing and smishing through real-world simulations. These activities help them apply their understanding to both the classroom and the Cyber Play narrative.

The lesson starts with an imagined vishing scenario, where a "bank" urgently requests sensitive information. Students analyse why the attack might work, focusing on psychological manipulation. This exercise enhances their critical thinking and links to the Cyber Play narrative by examining tactics characters face in the storyline.

In the main activity, students research different social engineering tactics, such as vishing, smishing, baiting, and pretexting. Working in groups, they examine how these attacks operate and present real-world examples. This mirrors the collaborative nature of problem-solving in Cyber Play, reinforcing their Interacting and Collaborating skills.

The plenary ties the group work into a discussion about recognizing and responding to these manipulative techniques.



What is Social Engineering Slide

Week 7, Lesson 2: Developing an Action Plan (W7L2)

In this lesson, students act as cybersecurity experts, developing action plans to defend against social engineering tactics discussed in Lesson 1. This activity mirrors their characters' roles in Cyber Play, where creating defence strategies to protect digital systems and personal information is crucial.

The lesson begins with a recap of social engineering tactics, highlighting psychological manipulation. Students are tasked with developing action plans that outline steps for identifying, mitigating, and educating others about these tactics. This proactive approach enhances their Digital Literacy and Citizenship by addressing personal and organisational security risks.

In the main activity, students work in groups to create detailed action plans, including identifying warning signs, response protocols, and educational materials such as infographics or posters. The collaborative task strengthens Interacting and Collaborating skills.

The plenary concludes with group discussions, where each team shares a key strategy from their action plan. This reflection reinforces the importance of awareness and preparedness in defending against social engineering, both in the

real world and within Cyber Play

Resource 1: Social Engineering Role Play Scenarios and Scripts

Scenario 1: Vishing Attack (Voice Phishing)

Overview: In this scenario, the attacker pretends to be a bank representative trying to steal personal information over the phone.

Attacker Script:
(Attacker calls the victim)
Attacker: "Good afternoon, this is John from [Bank Name]. I'm calling to alert you about a suspicious transaction on your account. There was a charge of £500 made this morning. Was this you?"
(Pause for victim's response)
Attacker: "We need to verify your identity to block the transaction. Can you please confirm your full name and account number?"

Victim Response (Guidance):

- Do not provide personal information.
- Ask for verification of the caller's identity.
- Suggest calling the bank back using an official number found on your bank card.

Week 7 Script

Week 7 Resources and Integration with the Story:

- PowerPoint Presentations for W7L1 and W7L2: These guide students through social engineering tactics and the development of defence strategies, aligning directly with the progression of Cyber Play.

- Worksheets and Infographic Templates: These help students create comprehensive action plans and educational materials. These resources prepare students to defend against social engineering in both the classroom and the interactive narrative.

Week 8: Final Review and Escape Room Challenge

Week 8 immerses students in a practical cybersecurity challenge using an Escape Room format. Students apply the skills learned throughout the course, focusing on teamwork, problem-solving, and cybersecurity techniques. The Escape Room ties into the Cyber Play narrative, with progress linked to solving puzzles that reflect real-world cyber threats.

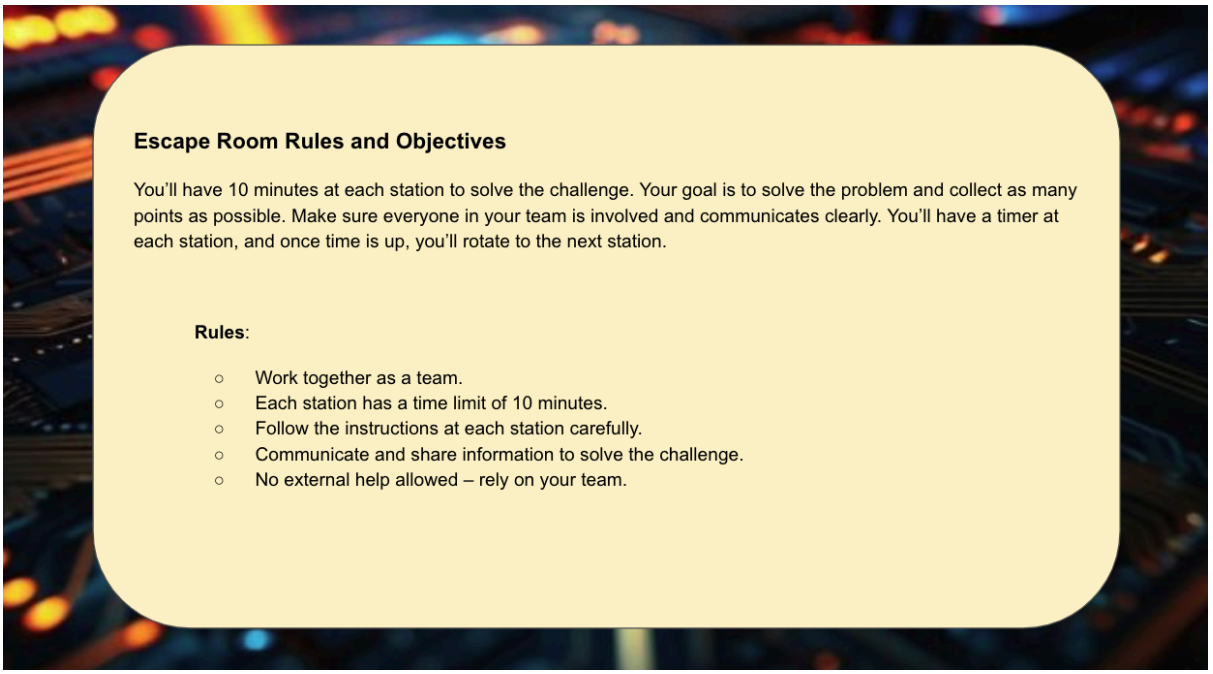
DCF Integration:

- Citizenship: Students respond to cybersecurity threats, reinforcing ethical and practical responsibilities.
- Interacting and Collaborating: The rotation between Escape Room stations promotes teamwork and communication.
- Digital Literacy: Activities enhance students' ability to assess digital threats like phishing, malware, and network vulnerabilities, and develop strategies to overcome them.

Week 8, Lesson 1: Introduction to the Escape Room Challenge (W8L1)

This lesson introduces students to the Escape Room Challenge, outlining game mechanics and station rotations, each focusing on key cybersecurity concepts covered during the course. The escape room simulates real-world cyber defence scenarios, testing students' ability to identify and mitigate threats.

Students are briefed on the challenge objectives: mitigating cyber threats under time constraints, reinforcing the high-pressure nature of cybersecurity work. Teams rotate through stations covering malware identification, network security, phishing detection, and social engineering.



Escape Room Rules and Objectives

Week 8, Lesson 2: Reflection and Peer Assessment (W8L2)

This lesson serves as a reflective conclusion to the *Cyber Play* curriculum, focusing on teamwork, problem-solving, and cybersecurity knowledge through peer and self-assessment.

The session begins with students reflecting on their escape room challenge experience, discussing strategies, teamwork, and the skills they applied. This reflection strengthens their understanding of real-time collaboration in cybersecurity.

Students complete peer assessments, evaluating another team's communication, problem-solving, and decision-making. This exercise mirrors professional post-incident evaluations in cybersecurity, reinforcing *Interacting and Collaborating* skills.

Students then reflect on how the escape room challenges applied cybersecurity concepts to real life, such as recognizing phishing and malware. This connects back to the *Cyber Play* narrative. Writing prompts guide them to think critically about a key skill they've learned and how they'll apply it in real-world scenarios, reinforcing *Citizenship* through responsible online behaviour.

Finally, students complete a self-assessment, rating their confidence in applying cybersecurity skills and teamwork, helping them recognize their growth over the course of the project.

Week 8 Resources and Integration with the Story:

- **PowerPoint Presentation (W8L2):** Guides reflection and assessment activities, linking students' experiences with real-world post-incident reviews in cybersecurity.

- **Peer Assessment Form:** Allows structured feedback on communication, teamwork, and problem-solving, mirroring the collaborative nature of cybersecurity.
- **Reflection Writing Prompts Sheet:** Encourages students to connect their learning to real-world digital safety, reinforcing key concepts from *Cyber Play*.
- **Self-Assessment Sheet:** Helps students reflect on their growth and identify areas for improvement, promoting self-awareness in their cybersecurity knowledge and teamwork skills.

Form Implementation

The implementation of feedback forms in Cyber Play utilised Google Forms to gather both quantitative and qualitative data at four stages: pre-scheme, post-scheme, immediately after the play, and in a long-term follow-up. Google Forms was chosen for its ease of use, wide accessibility, and instant data collection.

Key Features:

- Quantitative Data: Collected through multiple-choice and Likert scale questions, measuring students' knowledge, confidence, and understanding before and after the play.
- Qualitative Data: Open-ended questions allowed students and teachers to provide deeper insights into their experiences, offering suggestions and highlighting areas for improvement.
- Accessibility: Forms were shared through simple links, ensuring ease of distribution and use across different schools and devices.

These forms provide essential feedback, shaping both the immediate and long-term educational effectiveness of Cyber Play.

Analysis and Evaluation

Rubric Evaluation

This rubric evaluates the Cyber Play project based on the Principles of Progression from the Welsh Government's Curriculum for Science and Technology and the Digital Competence Framework (DCF). Five key educational areas are scored on a scale from 1 (Not Encouraged) to 4 (Strongly Encouraged).

Area of Analysis	Description	Success Score
Effectiveness as a learner	The project promotes independent learning by encouraging students to experiment and improve through feedback, though more scaffolding could enhance its inclusivity.	3.5/5
Breadth and depth of knowledge	Students engage with increasingly complex cybersecurity concepts, building on prior knowledge effectively.	4.0/5
Understanding ideas across disciplines	Cross-disciplinary learning is encouraged, though improvements are needed in the Phishing Branch for clarity.	3.0/5

Refinement of skills	Investigative and problem-solving skills are developed, but the project could include more support for varying ability levels.	3.5/5
Transferring learning to new contexts	The project offers real-world relevance by allowing students to apply knowledge in new cybersecurity scenarios.	4.0/5

Total Score: 18/25 (72%)

The project aligns well with Principles of Progression and DCF goals, promoting computational thinking, independence, and practical applications. However, refinements in scaffolding and clarity (especially in the Phishing Branch) would improve accessibility and understanding for all students, enhancing the overall impact.

Analysis of Project Design and Implementation

The Cyber Play project was created to immerse students in a narrative-driven, interactive experience that deepens their understanding of digital literacy and cybersecurity. By positioning students as active participants who solve real-world cybersecurity problems like phishing, malware, and network security, the project successfully blends theoretical learning with practical application.

As Cyber Play developed, the narrative and structural complexity evolved significantly beyond the original flowchart. While the initial concept provided a

straightforward, branching path to guide students through various cybersecurity challenges, the final version incorporated additional branches, mini-games, and more dynamic interactions to heighten engagement and educational impact. The introduction of features like real-time decision-making, interactive multimedia elements, and more complex narrative branches, including paths like Network Traffic Analysis and Malware, came as the project matured. These changes were driven by research, technical experimentation, and a growing understanding of how to create a more immersive and educational experience for students. The original flowchart, which mapped the basic structure, no longer fully represents the final scope of the play. This reflects the iterative nature of design and implementation, where new opportunities and challenges shaped the final product. For comparison, the original flowchart is included in the appendix to demonstrate how the project grew in complexity.

This design aligns well with the Increasing Effectiveness as a Learner principle from the Principles of Progression. Rather than passively absorbing information, students actively apply their knowledge in a structured narrative, which enhances engagement and understanding. This also supports progression steps 3 and 4 of the DCF, which focus on fostering independent learning and applying knowledge across multiple contexts.

Feedback and Testing

Though full-scale testing at Bridgend STEAM College was limited by time constraints, informal testing was conducted in several international schools following the Cambridge International Curriculum. Despite these schools not adhering to the Digital Competence Framework (DCF), they provided valuable insights into the project's educational impact. However, formal testing aligned with the DCF and Principles of Progression could provide a more comprehensive evaluation in the future.

Informal testing revealed that students responded particularly well to the time-based challenges, such as those found in the Network Traffic Branch. These fast-paced, interactive scenarios fostered critical thinking and decision-making under pressure, aligning with the Computational Thinking strand of the DCF. Students noted that they felt more pressure from the 5-minute timer enhancing their engagement and reinforcing key learning objectives. This directly supports the Principles of Progression, particularly in developing interdisciplinary skills and problem-solving abilities.

However, the Phishing Branch was identified as the least engaging component of Cyber Play. Feedback suggested that the tasks were too ‘boring’ for some students, with elements like email metadata analysis proving difficult to understand. This highlights the need for further interactivity, scaffolding and differentiation within this branch. Future iterations could focus on simplifying the metadata analysis and breaking down the more challenging tasks into smaller, more accessible, interactive steps.

An additional suggestion is to offer differentiated tasks, where students can choose between basic and advanced phishing challenges. This would allow students to build confidence with simpler tasks before progressing to more advanced phishing detection techniques. For instance, integrating interactive elements such as drag-and-drop activities could help students visualise and understand concepts like email spoofing and fake metadata more intuitively. By making the content more interactive and visual, students could engage more deeply with the cybersecurity concepts being taught.

Additionally, narrative-driven clues could be introduced to make the phishing investigation feel less static. For instance, real-time pop-up notifications simulating a breached inbox could immerse students further into the scenario, making the learning process more engaging. By refining these aspects, the Phishing Branch would not only align better with the DCF but also promote digital literacy and critical thinking in a more practical and intuitive context.

During the informal tests, hands-up voting replaced the originally planned Mentimeter system for audience interaction. While this adaptation had minimal impact on the play's educational value, feedback suggested that the play could benefit from a more seamless voting and interaction mechanism. Future iterations could explore integrating a custom polling system, which would allow real-time data collection and provide a more streamlined voting process. This would enhance alignment with the Interacting and Collaborating strand of the DCF, encouraging greater collaboration and more active participation from students.

Future Testing Plans and Data Collection

In future iterations, a formal testing phase could be conducted in two to three DCF-aligned schools, ensuring the play is evaluated within the context of the Welsh educational system. The pre- and post-survey methodology could be implemented to gather both quantitative and qualitative data, offering insights into student engagement, knowledge retention, and behavioural changes after participating in Cyber Play.

Teachers' insights could also be gathered to assess the play's effectiveness in a classroom setting. This would involve feedback on:

- Classroom Engagement: How well Cyber Play integrates into the existing curriculum and how students apply the learned concepts in subsequent lessons.
- Knowledge Application: Teachers could observe how well students use cybersecurity concepts in other subjects, particularly in IT or digital literacy tasks.
- Differentiation and Student Engagement: Feedback could include observations on how well the play supports varied learning abilities, and whether additional differentiation is needed to ensure accessibility for all students.

By incorporating student and teacher feedback further, the project could evolve to better meet the educational needs of learners and align more fully with the DCF. This iterative process of testing, refinement, and improvement would ensure that Cyber Play remains a relevant and effective tool in promoting digital competence in real-world cybersecurity scenarios.

Pedagogical Approach

The pedagogical foundation of Cyber Play is scenario-based learning, which promotes active collaboration and real-time problem-solving. This aligns well with both Computational Thinking and Data Analysis within the DCF. By placing students in the role of cybersecurity professionals, they engage with practical, hands-on tasks that encourage independent thinking and decision-making.

While most branches, such as Network Traffic and Malware, successfully facilitate skill refinement and problem-solving, the Phishing Branch requires better scaffolding. During testing, students found this section too complex, particularly in navigating the more technical aspects of phishing and social engineering. Simplifying the sequence of tasks, offering clearer instructions, and breaking down the activities into smaller steps would ensure accessibility for students at progression step 3 of the DCF. This could include introducing differentiated tasks where advanced students can opt for more challenging extensions, allowing for differentiated learning within the same branch.

The Network Traffic and Malware branches, on the other hand, effectively support skill progression by gradually increasing complexity and offering immediate feedback. Students were able to improve their decision-making and technical understanding through structured problem-solving and interactive simulations.

In summary, the project achieves its goal of fostering increasing effectiveness as a learner, but minor adjustments, particularly in the Phishing Branch, are needed to balance accessibility and challenge for all learners.

Resource Effectiveness

The resources accompanying Cyber Play were designed to be flexible, collaborative, and project-based, reducing preparation time for teachers. However, feedback from testing revealed a need for more built-in differentiation, as the current resources depend heavily on the teacher's ability to adapt the materials. To address this, future iterations will incorporate more scaffolding and differentiated activities, ensuring that students of varying abilities can progress independently. Adding these features will also improve the project's alignment with the increasing breadth and depth of knowledge principle, expanding students' understanding of cybersecurity beyond basic concepts.

By encouraging students to apply their knowledge to new, more complex challenges, the resources will also strengthen alignment with the Digital Literacy strand of the DCF, fostering critical engagement and thoughtful decision-making in digital contexts.

Alignment with Educational Frameworks

The design of the Cyber Play project aligns well with several key areas of the Welsh Digital Competence Framework (DCF):

- Citizenship Strand: Lessons on digital privacy, identity, and online safety directly address the DCF's focus on digital responsibility. The activities in Week 1—such as creating avatars and exploring digital footprints—provide students with practical opportunities to reflect on their digital identities, aligning with the Identity, Image, and Reputation elements of the DCF.
- Data and Computational Thinking Strand: The Network Traffic and Malware branches are particularly strong in meeting the objectives of the Computational Thinking strand, offering real-world challenges that promote critical thinking, problem-solving, and the ability to recognize malicious behaviour online.
- Interacting and Collaborating Strand: Activities like the Phishing and Social Engineering exercises in Week 2 encourage collaboration, helping students develop teamwork and communication skills, which are central to both the DCF and the Principles of Progression.

Limitations and Technical Challenges

One of the significant technical challenges encountered during the development of Cyber Play was the limitation of Twine's Harlowe engine. While Harlowe's simplicity allowed for rapid prototyping, it lacked the flexibility needed for more complex interactions, particularly in integrating dynamic elements like live voting and real-time

feedback through JavaScript. This limitation was especially evident in sections like the Phishing Branch and Suspect Node, where more complex decision-making or decryption tools could have enhanced the educational experience.

In future iterations, shifting to the SugarCube engine would provide better support for JavaScript integration, allowing for real-time interaction and improved performance. SugarCube's advanced functionality would enable smoother handling of variables, more sophisticated interactive elements, and dynamic multimedia integration, thus enhancing the narrative's interactivity. The engine would also support better branching logic, crucial for scenarios where students need immediate feedback or for implementing more dynamic outcomes based on student choices.

By addressing these limitations, the project could be expanded to include more engaging elements, such as real-time decryption tasks, multi-user input features, and richer storytelling through enhanced multimedia capabilities. This would also allow for more detailed data collection on student engagement and learning outcomes.

Mentimeter integration also posed a challenge, as it couldn't store or track responses within the play. Developing a custom polling system would enable real-time data collection, enhancing the Interacting and Collaborating strand by providing a more seamless interactive experience.

Relevance to Real-World Scenarios

Cyber Play was designed to reflect real-world cybersecurity challenges, aligning with the Principles of Progression by helping students apply their learning to practical problems like phishing, network security, and malware analysis. These scenarios mirror digital threats students might face, promoting critical thinking and decision-making.

Feedback revealed that while the Network Traffic and Malware branches were effective due to their fast-paced, interactive nature, the Phishing Branch needed refinement. It was identified as less engaging, likely because it was pitched at too high a level for the target age group and is more static when compared to Malware and Network Traffic Analysis Branches. Students found it harder to relate to the scenarios, leading to disengagement.

To improve alignment with the DCF and better support progression steps 3 and 4, future iterations will simplify the Phishing Branch content without sacrificing educational value. This will involve creating more intuitive and relatable scenarios, helping students build confidence in recognising phishing and social engineering tactics.

Feedback also highlighted strong engagement with the narrative elements, like Mr. Luddite. Future refinements will focus on making the educational content more interactive, incorporating more interactive or time-based challenges similar to those used in the Network Traffic section to enhance engagement and understanding.

In summary, future iterations will better pitch the Phishing Branch to the target age group, ensuring that students can more effectively engage with and apply their learning.

Suggestions for Future Work

Future iterations of Cyber Play could aim to expand interactivity, refine weaker sections such as the Phishing Branch, and introduce more time-sensitive challenges to enhance engagement. Additionally, the resource materials could be improved to offer better differentiation, ensuring students of varying abilities can progress at their own pace.

A formal testing plan could be introduced to ensure Cyber Play fully aligns with the Principles of Progression and the Digital Competence Framework (DCF). This plan could involve piloting the play in DCF-aligned schools, with the collection of both qualitative and quantitative data to measure the project's effectiveness in fostering student engagement, knowledge retention, and changes in online behaviour.

The pilot study could involve two to three schools, with each session followed by structured surveys and focus groups. Pre-play surveys could assess students' initial understanding of cybersecurity concepts, while post-play surveys could evaluate their grasp of topics like phishing, malware, and network traffic analysis. These surveys would also assess students' confidence in handling cyber threats and their ability to apply the knowledge gained from the play.

To track long-term outcomes, follow-up surveys could be conducted several weeks after the sessions to assess knowledge retention and behavioural changes, such as improved password security or heightened awareness of phishing attempts. This

approach would help evaluate the sustained impact of Cyber Play on students' cybersecurity habits.

Teacher feedback could also be incorporated into the evaluation process. Educators could provide insights into how well the play integrates with existing curriculum content, the level of student engagement, and suggestions for further development. This feedback would be crucial in refining the play, particularly in the Phishing Branch, and ensuring that the educational content remains accessible to all students.

A comprehensive report could be generated from the pilot study's findings, outlining how the insights could be applied to refine the play. These refinements would ensure that Cyber Play not only achieves its educational goals within the DCF but also delivers an engaging, immersive experience that strengthens students' digital competence and critical thinking in real-world cybersecurity contexts.

Conclusion

Project Outcomes and Achievements

The Cyber Play project set out to create an engaging, narrative-driven tool that would educate students on digital literacy and online safety, and it evolved into an exploration of gamified learning. Through this project, I have learned that gamification can significantly enhance student engagement by providing an immersive alternative to traditional methods of teaching.

Several key accomplishments stand out. The Network Traffic branch emerged as a major success due to its timed, decision-based gameplay, which mirrors real-world urgency in cybersecurity scenarios. This feature fostered student engagement by creating high-pressure decision-making opportunities, enhancing their critical thinking.

The variable dialogue system was another achievement. This dynamic interaction system, where characters would react differently based on student choices, added a layer of realism that reflects real-world cybersecurity unpredictability. It allowed students to understand how their decisions influence outcomes.

One of the most rewarding technical challenges was the development of a cipher system to scramble student names for in-game encryption tasks. This overcame limitations of the Harlowe engine and added a personalised, interactive element to the learning experience by integrating real-time encryption challenges. This feature tied into the play's narrative and enriched its educational value.

Impact, Unexpected Outcomes, and Value of the Project

A key realisation from developing Cyber Play was the potential it holds for making complex cybersecurity topics accessible and engaging for students. Although full-scale testing wasn't conducted, the project itself showcases the potential of interactive storytelling as an educational tool. By weaving practical cybersecurity challenges into the narrative, the play encourages critical thinking and decision-making. Early feedback from informal testing and development highlighted the effectiveness of this approach, particularly in fostering a sense of agency among students, even with minimal interactivity.

Additionally, even with simplified tools, such as hands-up voting instead of Mentimeter, the play successfully fostered collaboration and teamwork. This outcome was not anticipated but highlighted the potential for decision-based learning environments to encourage student agency, even with limited interactivity.

Cyber Play addresses a key issue in computing education, where traditional lecture-heavy methods often fail to engage students meaningfully. The gamification aspect makes learning relevant, turning passive lessons into active, decision-driven experiences. However, while the project has great potential, it also poses practical challenges, developing the resources themselves took months, and its implementation may be demanding or impossible for teachers with busy schedules. Nonetheless, it can serve as a prototype for more flexible and integrated gamified educational tools.

The innovation lies in the use of gamification. Though the individual lessons remain traditional, the overall project pushes boundaries, placing students at the centre of a

narrative-driven learning experience. Feedback from informal testing was limited but provides valuable insights for future iterations. With refinement, Cyber Play offers a strong foundation for engaging students in digital literacy and cybersecurity.

Reflection

The Cyber Play project has been both challenging and rewarding, pushing me to develop technically and creatively. One of the main hurdles was Harlowe’s limitations with JavaScript integration, which slowed development. Switching to the more flexible SugarCube engine earlier could have enhanced interactivity and functionality, reducing these technical issues however by the time i realised this technical limitation the ‘skeleton’ of the play was already written and SugarCube would have required a blank page restart.

Mentimeter, though engaging, proved disruptive when overused, breaking the flow of the narrative. A custom polling system tailored for seamless integration would have offered a more cohesive experience and is something that could be developed in future iterations.

Testing revealed that the Phishing Branch was too complex for the target audience. Simplifying this section and aligning it with students' comprehension levels will be key to future iterations.

This project has shown me the immense potential of gamified learning, not just in Computing but across multiple subjects. Expanding Cyber Play into a more scalable tool, with customizable stories for various educational contexts, could revolutionise how subjects are taught, especially as digital learning becomes more prominent.

Additionally, I see potential in live performances of Cyber Play, where students take on active roles, making decision-making more dynamic. Scaling down for classroom use could foster deeper engagement and offer richer learning opportunities.

Overall, this project has illuminated a gap in EdTech that immersive, narrative-driven tools like Cyber Play can fill. With refinement, it could become a valuable asset for both students and educators, transforming digital literacy education.

References

A definitive guide to the seven-point story structure. Art of Narrative. 2022. Available at: https://artofnarrative.com/2022/03/30/a-definitive-guide-to-the-seven-point-story-structure/ [Accessed: 28 September 2024].

ACM. 2018. *ACM Code of Ethics and Professional Conduct*. Available at: https://www.acm.org/code-of-ethics [Accessed: 21 September 2024].

Aprea, C. and Ifenthaler, D. 2020. *Game-based learning across the disciplines*. Cham: Springer International Publishing. doi: 10.1007/978-3-030-75142-5.

BCS. 2023. *BCS Code of Conduct*. Available at: https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct/ [Accessed: 21 September 2024].

Constructivist learning theory. Educational Technology. [2021]. Available at: https://educationaltechnology.net/constructivist-learning-theory/ [Accessed: 27 September 2024].

Cyber security breaches survey 2024 - GOV.UK. [no date]. Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024 [Accessed: 23 August 2024].

CyberFirst Overview. National Cyber Security Centre (NCSC). [no date]. Available at: https://www.ncsc.gov.uk/cyberfirst/overview [Accessed: 2 July 2024].

Cyber Security - Key Stage 4. TeachComputing.org. 2024. Available at: https://teachcomputing.org/curriculum/key-stage-4/cyber-security [Accessed: 21 July 2024].

CyberStart. [no date]. Available at: https://cyberstart.com [Accessed: 28 June 2024].

Developing a vision for curriculum design - Hwb. [no date][a]. Available at: https://hwb.gov.wales/curriculum-for-wales/designing-your-curriculum/developing-a-vision-for-curriculum-design/#curriculum-design-and-the-four-purposes [Accessed: 17 July 2024].

Developing a vision for curriculum design - Hwb. [no date][b]. Available at: https://hwb.gov.wales/curriculum-for-wales/designing-your-curriculum/developing-a-vision-for-curriculum-design/#curriculum-design-and-the-four-purposes [Accessed: 17 July 2024].

Daniela, L. 2021. *Smart pedagogy of game-based learning*. 1st ed. Cham: Springer International Publishing AG. doi: 10.1007/978-3-030-76986-4.

Digital Competence Framework. 2020. Available at: https://hwb.gov.wales/curriculum-for-wales/digital-competence-framework [Accessed: 21 July 2024].

European Union. 2016. *General Data Protection Regulation (GDPR) (EU) 2016/679*. Available at: https://gdpr.eu/ [Accessed: 21 September 2024].

Hou, H.T., ed. 2023. *Game-Based Learning and Gamification for Education*. Basel, Switzerland: MDPI - Multidisciplinary Digital Publishing Institute.

Introduction to Curriculum for Wales guidance - Hwb. [no date]. Available at: https://hwb.gov.wales/curriculum-for-wales/introduction-to-curriculum-for-wales-guidance/ [Accessed: 21 July 2024].

Jabbar, A.I.A. and Felicia, P. 2015. Gameplay engagement and learning in game-based learning: a systematic review. *Review of Educational Research*, 85(4), pp. 740-779. doi: 10.3102/0034654315577210.

Li, C.T. and Hou, H.T. 2024. Remote blended game-based learning: integrating synchronous game-based learning with asynchronous inquiry-based learning. *Journal of Science Education and Technology*, 33(5), pp. 746-758. doi: 10.1007/s10956-024-10118-8.

Marques, M.M. and Pombo, L. 2021. Current trends in game-based learning—introduction to a special collection of research. *Education Sciences*, 11(10), p. 622. doi: 10.3390/educsci11100622.

Online Safety - Key Stage 4. TeachComputing.org. 2024. Available at: https://teachcomputing.org/curriculum/key-stage-4/online-safety [Accessed: 21 July 2024].

Optimising adolescent wellbeing in a digital age. [no date]. Available at: http://www.bmj.com/ [Accessed: 16 August 2024].

Plass, J.L., Homer, B.D. and Kinzer, C.K. [no date]. Foundations of game-based learning. *Educational Psychologist*. Available at: www.tandfonline.com/hedp [Accessed: 11 Aug 2024].

Routes for Learning. Hwb. [no date]. Available at: https://hwb.gov.wales/curriculum-for-wales/routes-for-learning [Accessed: 04 August 2024].

Science and Technology - Curriculum for Wales. Hwb. [no date]. Available at: https://hwb.gov.wales/curriculum-for-wales/science-and-technology [Accessed: 30 September 2024].

Theroux, R. 2020. The use of story-based learning in a women's health course. *Journal for Nurse Practitioners*, 16(7), pp. e93-e96. doi: 10.1016/j.nurpra.2020.04.008.

Trinket.io. [no date]. Available at: https://trinket.io/pygame/969287086f?outputOnly=true [Accessed: 01 August 2024].

Wang, Z., Zhu, H., Liu, P. and Sun, L. 2021. Social engineering in cybersecurity: a domain ontology and knowledge graph application examples. *Cybersecurity*, 4(1), pp. 1-21. doi: 10.1186/s42400-021-00094-6.

Wang, Z., Sun, L. and Zhu, H. 2020. Defining social engineering in cybersecurity. *IEEE Access*, 8, pp. 85094-85115. doi: 10.1109/ACCESS.2020.2992807.

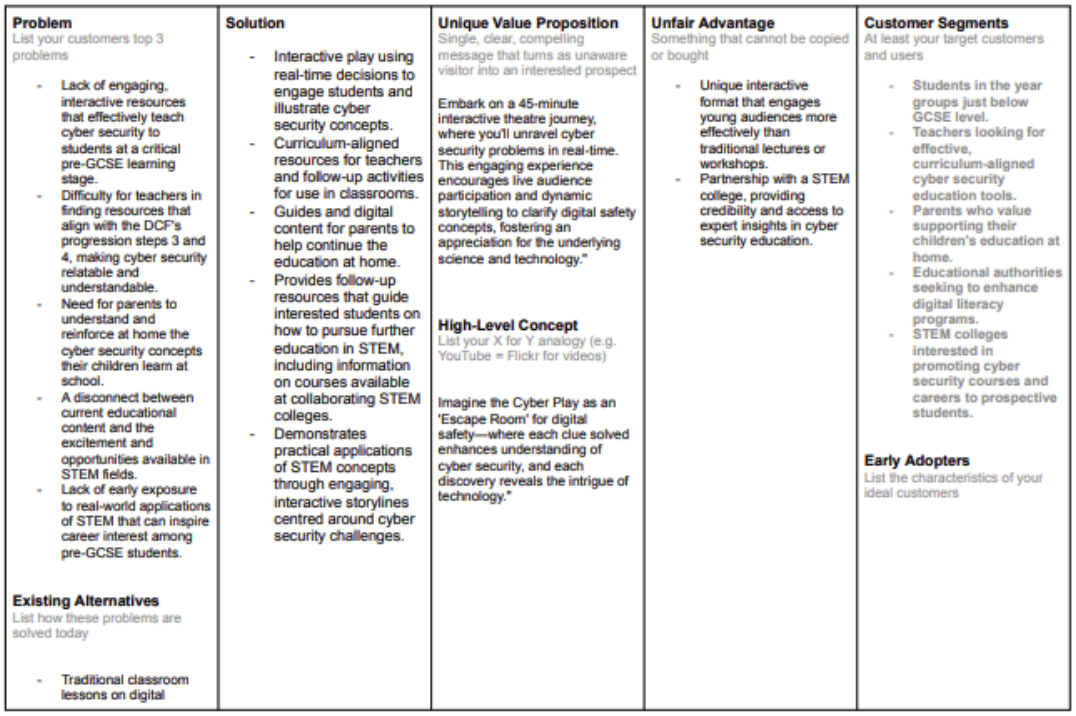
Wang, Z., Zhu, H. and Sun, L. 2021. Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods. *IEEE Access*, 9, pp. 11895-11910. doi: 10.1109/ACCESS.2021.3051633.

Well-being of Future Generations (Wales) Act 2015: the essentials | GOV.WALES. [no date]. Available at:

https://www.gov.wales/well-being-future-generations-act-essentials-html [Accessed: 22 July 2024].

Well-being of Future Generations (Wales) Act 2015: the essentials | GOV.WALES. [no date]. Available at: https://www.gov.wales/well-being-future-generations-act-essentials-html [Accessed: 22 July 2024].

Appendix



Problem
List your customers top 3 problems

- Lack of engaging, interactive resources that effectively teach cyber security to students at a critical pre-GCSE learning stage.
- Difficulty for teachers in finding resources that align with the DCF's progression steps 3 and 4, making cyber security relatable and understandable.
- Need for parents to understand and reinforce at home the cyber security concepts their children learn at school.
- A disconnect between current educational content and the excitement and opportunities available in STEM fields.
- Lack of early exposure to real-world applications of STEM that can inspire career interest among pre-GCSE students.

Existing Alternatives
List how these problems are solved today

- Traditional classroom lessons on digital citizenship and cyber security.
- Online e-learning platforms offering cyber security modules.
- Workshops and seminars provided by external educational organisations.

Solution

- Interactive play using real-time decisions to engage students and illustrate cyber security concepts.
- Curriculum-aligned resources for teachers and follow-up activities for use in classrooms.
- Guides and digital content for parents to help continue the education at home.
- Provides follow-up resources that guide interested students on how to pursue further education in STEM, including information on courses available at collaborating STEM colleges.
- Demonstrates practical applications of STEM concepts through engaging, interactive storylines centred around cyber security challenges.

Unique Value Proposition
Single, clear, compelling message that turns as unaware visitor into an interested prospect

Embark on a 45-minute interactive theatre journey, where you'll unravel cyber security problems in real-time. This engaging experience encourages live audience participation and dynamic storytelling to clarify digital safety concepts, fostering an appreciation for the underlying science and technology."

High-Level Concept
List your X for Y analogy (e.g. YouTube = Flickr for videos)

Imagine the Cyber Play as an 'Escape Room' for digital safety—where each clue solved enhances understanding of cyber security, and each discovery reveals the intrigue of technology."

Unfair Advantage
Something that cannot be copied or bought

- Unique interactive format that engages young audiences more effectively than traditional lectures or workshops.
- Partnership with a STEM college, providing credibility and access to expert insights in cyber security education.

Customer Segments
At least your target customers and users

- Students in the year groups just below GCSE level.
- Teachers looking for effective, curriculum-aligned cyber security education tools.
- Parents who value supporting their children's education at home.
- Educational authorities seeking to enhance digital literacy programs.
- STEM colleges interested in promoting cyber security courses and careers to prospective students.

Early Adopters
List the characteristics of your ideal customers

Key Metrics
At least the key numbers that tell you how your business is doing

- Number of school engagements and student reach per academic year.
- Student interest levels in STEM before and after the play, measured via surveys.
- Feedback scores from students, teachers, and parents on educational impact and engagement.
- Number of follow-up resource downloads and inquiries about STEM educational programs.
- Engagement metrics during the play, particularly in segments highlighting STEM career paths.

Channels
List your path to customers

- Direct school engagements and performances.
- Educational conferences and workshops.
- Online marketing through educational platforms and social media.
- STEM education fairs and college open days where the play can be performed to attract prospective students.

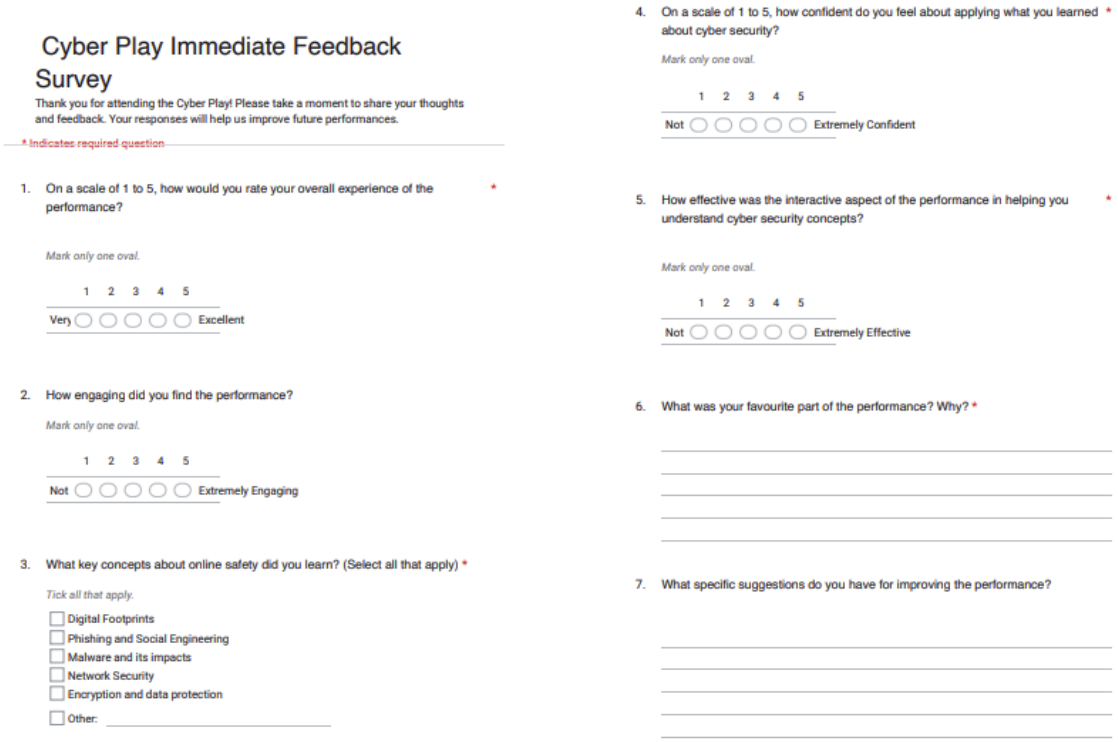
Cost Structure
List your fixed and variable costs

- Production costs including script development, set design, and actor fees.
- Logistics and travel costs for touring to various schools.
- Marketing and promotional expenses.
- Development costs for educational materials and follow-up activities.

Revenue Streams
List your sources of revenue

- School booking fees for performances.
- Grants and funding from educational and technological development programs.
- Sponsorships from cyber security and technology companies.
- Potential funding from educational grants focused on STEM promotion.

Appendix 1 - Lean Canvas for Cyber Play



Cyber Play Immediate Feedback Survey

Thank you for attending the Cyber Play! Please take a moment to share your thoughts and feedback. Your responses will help us improve future performances.

* Indicates required question

1. On a scale of 1 to 5, how would you rate your overall experience of the performance? *

Mark only one oval.

1 2 3 4 5

Very ◯ ◯ ◯ ◯ ◯ Excellent

2. How engaging did you find the performance?

Mark only one oval.

1 2 3 4 5

Not ◯ ◯ ◯ ◯ ◯ Extremely Engaging

3. What key concepts about online safety did you learn? (Select all that apply) *

Tick all that apply.

- ☐ Digital Footprints
- ☐ Phishing and Social Engineering
- ☐ Malware and its impacts
- ☐ Network Security
- ☐ Encryption and data protection
- ☐ Other: _____

4. On a scale of 1 to 5, how confident do you feel about applying what you learned about cyber security? *

Mark only one oval.

1 2 3 4 5

Not ◯ ◯ ◯ ◯ ◯ Extremely Confident

5. How effective was the interactive aspect of the performance in helping you understand cyber security concepts? *

Mark only one oval.

1 2 3 4 5

Not ◯ ◯ ◯ ◯ ◯ Extremely Effective

6. What was your favourite part of the performance? Why? *

_____

_____

_____

_____

_____

7. What specific suggestions do you have for improving the performance?

_____

_____

_____

_____

_____

Appendix 2 - Post-Session Form

30/09/2024, 10:26 Pre-Scheme of Work Survey

Pre-Scheme of Work Survey

Thank you for participating in the Cyber Play! As we prepare for the upcoming lessons on cyber security, we'd like to gather your thoughts and check your understanding of what was learned. Your responses will help us tailor the lessons to better meet everyone's needs.

* Indicates required question

1. What key concepts about cyber security do you remember learning about in the Cyber Play? *

2. On a scale of 1 to 5, how well do you feel you understand the concept of online safety? *

   Mark only one oval.

	1	2	3	4	5	
Not	◯	◯	◯	◯	◯	Very well

3. What topics are you most interested in learning more about during the upcoming scheme of work? (Select all that apply) *

   Tick all that apply.

   - ☐ Protecting personal information
   - ☐ Recognising phishing attempts
   - ☐ Understanding malware
   - ☐ Safe online practices
   - ☐ Other: ____________

1/3

30/09/2024, 10:26 Pre-Scheme of Work Survey

4. Have you or your students applied any of the knowledge gained from Cyber Play in daily life? *

   Mark only one oval.

   - ◯ Yes
   - ◯ No
   - ◯ Maybe

5. For teachers: How have you observed your students applying this knowledge?

6. What are your expectations for the upcoming lessons on cyber security? *

7. Any other feedback or suggestions? *

This content is neither created nor endorsed by Google.

2/3

Appendix 3 - Pre-Scheme of Work Survey

Cyber Play Post-Scheme of Work Survey

Instructions: Thank you for participating in the Cyber Play scheme of work! We appreciate your feedback. Your responses will help us evaluate the effectiveness of the lessons and improve future programs.

* Indicates required question

1. On a scale of 1 to 5, how would you rate your overall experience of the scheme of work? *

Mark only one oval.

1 2 3 4 5

Very ◯ ◯ ◯ ◯ ◯ Excellent

2. What key concepts about cyber security do you feel you learned during the scheme of work? (Select all that apply) *

Tick all that apply.

- ☐ Digital footprints
- ☐ Phishing and social engineering
- ☐ Malware and its impacts
- ☐ Network security
- ☐ Encryption and data protection
- ☐ Other

3. Please briefly explain why you selected these concepts *

4. On a scale of 1 to 5, how confident do you feel about applying what you learned about cyber security? *

Mark only one oval.

1 2 3 4 5

Not ◯ ◯ ◯ ◯ ◯ Extremely Confident

5. Have you applied any of the knowledge gained from the scheme in your daily life? *

Mark only one oval.

- ◯ Yes
- ◯ No
- ◯ Maybe

6. If yes, please describe how *

7. How engaging did you find the lessons? *

Mark only one oval.

1 2 3 4 5

Not ◯ ◯ ◯ ◯ ◯ Extremely Engaging

8. Which lesson did you find the most valuable or interesting? Why? *

9. Teacher Feedback (For Teachers Only)

What strategies or activities do you feel were most effective in teaching the concepts? What challenges did you encounter while delivering the scheme?

10. What specific suggestions do you have for improving the scheme of work? *

11. Any other feedback or comments? *

Appendix 4 - Post-Scheme of Work Survey

Cyber Play Long-Term Follow-Up Survey

Instructions: Thank you for participating in the Cyber Play and the subsequent scheme of work! We'd like to check in to see how the experience has influenced your understanding and behaviours regarding cyber security. Your feedback is valuable for improving future programs.

* Indicates required question

1. Which key concepts about cyber security do you still remember? (Select all that apply) *

Mark only one oval.

- ◯ Digital footprints
- ◯ Phishing and social engineering
- ◯ Malware and its impacts
- ◯ Network security
- ◯ Encryption and data protection
- ◯ Other: _____

2. Have you applied any of the knowledge gained from the Cyber Play and the scheme in your daily life? *

Mark only one oval.

- ◯ Yes
- ◯ No
- ◯ Maybe

3. Have you made any changes to your online behaviour as a result of what you learned? *

Tick all that apply.

- ☐ Yes
- ☐ No

4. If yes, please specify

_____

5. On a scale of 1 to 5, how confident do you feel about your ability to protect yourself online? *

Mark only one oval.

	1	2	3	4	5	
Not	◯	◯	◯	◯	◯	Extremely confident

6. Are you interested in learning more about cyber security topics in the future? *

Mark only one oval.

- ◯ Yes
- ◯ No
- ◯ Maybe

7. If yes, what specific topics would you like to explore?

_____

8. How would you describe the impact of the Cyber Play and the scheme of work on your understanding of online safety? *

_____

9. Have you observed any changes in your students' knowledge or behaviour regarding cyber security since the program?

Teacher Feedback (For Teachers Only)

Mark only one oval.

- ◯ Yes
- ◯ No
- ◯ Maybe

10. If yes, please elaborate

_____

11. What suggestions do you have for improving future cyber security programs? *

_____

12. Any other feedback or comments? *

_____

Appendix 5 - Long Term Follow Up Survey

Story Outline

Genre: Interactive Theater/ Educational Play

Duration: 45 minutes

Audience: School children just below GCSE level, educators, and parents

Format: Choose-your-own-adventure interactive play with audience participation through real-time voting on decisions that impact the storyline and learning outcomes.

Overview: "Cyber Play" is an interactive theatre production where the audience members collaborate with the characters to uncover the culprit behind a cyber incident. The narrative is driven by the audience's choices, which influence the direction and outcome of the story. The play is designed to educate on various cybersecurity topics through engaging, real-time decision-making.

Structure:

Stage 1: Introduction (Act 1: The Hook)

- Introduction: The audience participates in a digital event and is asked to create digital avatars through seemingly innocent questions (Name Generator attack).
- Dramatic Incident: The task force enters and announces that a security breach has occurred, and everyone is a potential suspect. The investigation must begin immediately.
- Mr. Luddite's Role: Mr. Luddite is introduced as a character who casts doubt on technology and spreads misinformation from the start. He engages with the audience, challenging their trust in digital tools while providing educational hints.

Stage 2: Discovery of Clue and Branch Choices (Act 2: Plot Point 1)

- Caesar Cipher Clue: Early in the investigation, a clue involving a Caesar Cipher is uncovered. The audience helps decrypt it, unlocking further information about the nature of the breach.
- Branching Paths: After solving the cipher, the audience is presented with three independent investigation paths to explore:
  1. Phishing
  2. Malware
  3. Network Traffic Analysis
- Audience Choice: The audience can vote or choose which branch to explore first. They must collect clues from these branches to proceed toward solving the overall mystery.

Stage X: Network Traffic Branch (Act 3: Pinch Point 1)

- Network Traffic Investigation: The audience delves into network traffic logs to detect suspicious activity.
- Critical Stakes: This is where the 5-minute timer is introduced. The audience has to stop a major data upload attack by analysing network patterns and traffic spikes.
- Pinch Points: Throughout this branch, wrong decisions can lead to game failure and the path being blocked, with the data being uploaded or encrypted.
- Correct Decisions: The audience identifies the correct traffic anomalies and stops the upload, gaining key clues about the perpetrator's digital footprint.

Stage X: Malware Branch (Act 3: Pinch Point 2)

- Malware Investigation: The task force discovers that the system has been infected by ransomware. The audience is presented with three critical choices:
  1. Restoring from backups
  2. Running cleanup software
  3. Paying the ransom
- Pinch Points: Wrong choices, such as paying the ransom, lead to delays or confusion, while the correct decision (backups or cleanup) yields a major clue, like the name or identity of the perpetrator hidden in malware logs.
- Luddite's Role: Mr. Luddite continues to question the efficacy of digital solutions, but his fake news distractions in this branch have more educational focus, teaching about data backups and ransomware handling.

Stage X: Phishing Branch (Act 3: Pinch Point 3)

- Phishing Investigation: The audience investigates phishing attempts by examining email headers, metadata, and suspicious links.
- Pinch Points: Wrong decisions in this branch lead to minor annoyances or chasing incorrect leads, but the path remains open for further investigation.
- Correct Decisions: The audience finds important clues in email patterns and fake sender data, helping them identify potential suspects. They piece together who sent the phishing emails and why.
- Luddite's Role: Luddite inserts misinformation here as well, casting doubt on the legitimacy of email headers and metadata. The audience must critically analyse the phishing clues to stay on track.

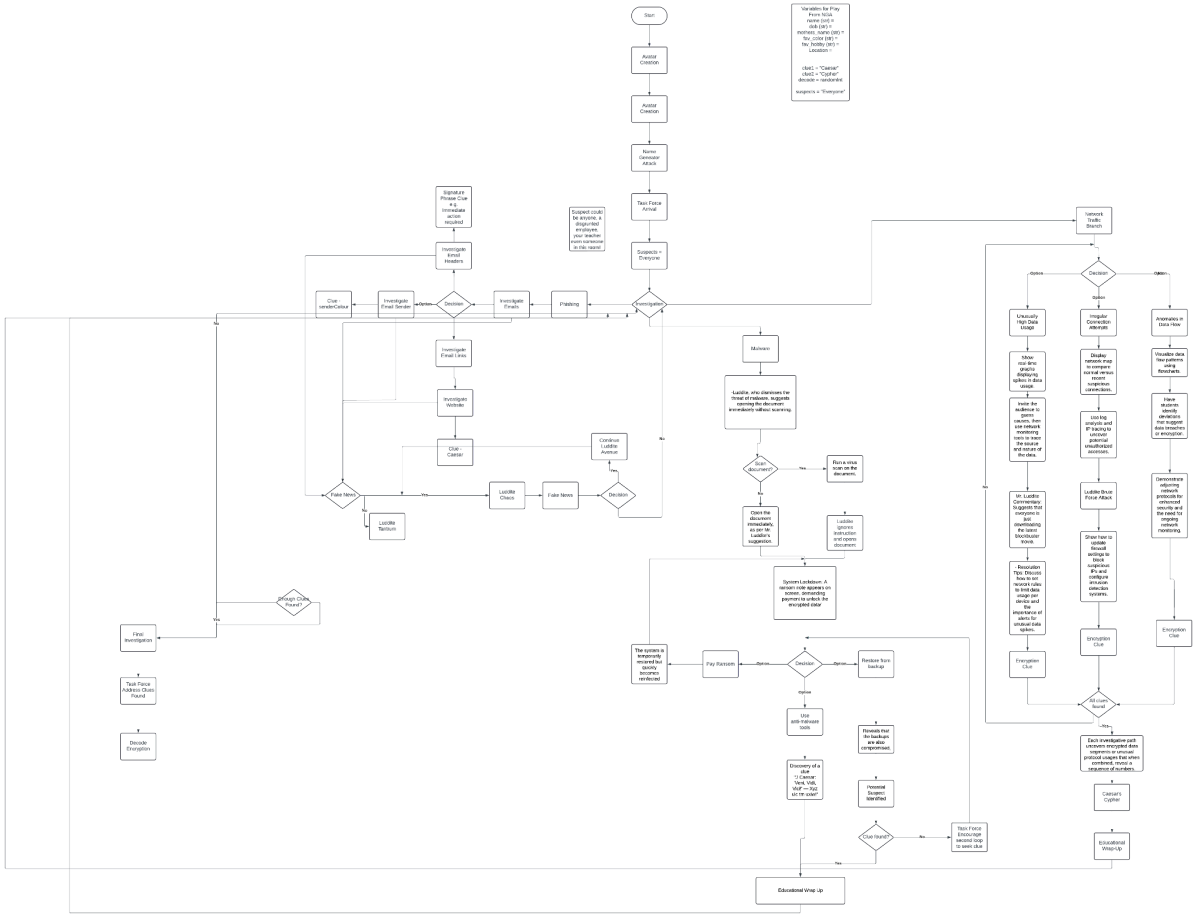
Stage 6: Decryption (Final Puzzle Unlocked)

- Decryption Tool Unlocked: Once enough clues have been gathered from at least one or more branches, the final Caesar Cipher decryption tool unlocks. The audience is tasked with decrypting the scrambled name, role, and details of the perpetrator.
- Puzzle Solving: The correct decryption reveals the identity of the perpetrator, allowing the investigation to reach its climax.

Stage 7: Resolution and Educational Wrap-Up (Final Act)

- Final Reveal: The task force gathers everyone together and reveals the identity of the culprit based on the decrypted information and clues collected throughout the investigation.
- Educational Wrap-Up: The task force concludes by summarising the key cybersecurity lessons, such as:
  - How to identify phishing attempts
  - Best practices for malware and ransomware defence
  - Importance of recognizing fake news and misinformation
  - The role of network traffic analysis in stopping breaches
- Celebratory Conclusion: The play ends on a positive note, celebrating the audience's participation and reinforcing the importance of being cyber-aware in their daily lives.

Appendix 6 - Full Story Outline



Appendix 7 - Original Cyber Play Flowchart