



# Escape game

## Scenario & roadmap

### Context

The DigiCity game follows the character of a young woman just turning 20, navigating the challenges of hyperconnectivity in 2056. After she and her friends install a cutting-edge cybernetic implant that enhances their online connections, they experience both the allure of instant access to so many features and the overwhelming consequences of hyperconnectivity, such as information overload, cyberbullying and loss of privacy.

One of the friends, Quinn, has posted photos and captions on her social media account that show her supporting and befriending an extremist group that the other characters have previously condemned. Most people jump to attack her for it, while a few friends, including the main character, decide to look deeper into the situation to find out the truth: she has been hacked and is the target of a defamation campaign, which could cost her an internship in a prestigious company and deeply affect her personal life.



Co-funded by  
the European Union

# Integration

This escape game follows the video game and occurs after its end: after the group of friends have proven that the photos and posts on Quinn's account are fake, the players are now tasked with identifying who hacked her accounts and edited those photos, figuring out their reasons, and deciding what to do with the information they revealed, while protecting their own data from being used against them. It takes the form of an investigation that explores data protection, digital footprint and ethical dilemmas.

The puzzles and data are consistent with the video game content, but the escape game can be played without having played the video game.

## Game Master role and stakes

The Game Master (GM) could play **their own role as a youth worker or educator**, and express that they have **a friend who's a passionate and old-fashioned professor** at DigiCity University (DigiU) who wishes to help Quinn, one of their students, receive justice after her reputation was severely damaged by a defamation campaign. The professor has a history of investigative research but, unfortunately, isn't very tech-savvy or aware of social media behaviours, but has a history of investigative research and wishes to help identify the culprit and how to report them.

To do so, the professor asked the GM/facilitator to recruit a group of students (participants) to help them solve this mystery, expose a hacker and save an innocent student's reputation. Players need to **figure out who edited and posted the photos, how they did it and why**, by analysing digital data.

However, they will have a **time limit**, as the hacker, who now knows that people don't believe their posts about Quinn anymore, may be able to erase their tracks, remove data from accessible servers and thus avoid being caught if the participants aren't fast enough to identify them. Additionally, if

they fail to expose the culprit in that timeframe, someone else may end up becoming a target as well.

The Game Master will prepare and uphold the **hint system**, detailed in the Game Master guide, and be ready to guide and assist the players who can ask for clues or receive them if the GM sees them struggling for too long.

## Escape game settings

**Set-up:** The escape game can take place in a single room with a table and a computer. Hiding places such as folders, bins or drawers can be used to scatter the hints and documents around the room.

**Duration:** 45 minutes

**Participants:** Groups of 3 to 6 players

### Material:

- A digital device (computer or tablet)
- A timer
- Annex 1 - Lockscreen wallpaper
- Annex 2 - Computer password
- Annex 3 - Defamatory post
- Annex 4 - Screenshot of a chat with a friend
- Annex 5 - Correspondence IP addresses
- Annex 6 - DigiCityNet Letter page number 56
- Annex 7 - DigiCityNet Security account
- Annex 8 – Tips & tricks about key concepts

## Phase 1: Introduction and backstory

**Objective:** Setting the scene and explaining the players' roles and goals

### Step 1: The context

---

The GM introduces the context and setting of the escape game in the futuristic town of DigiCity (just like in the video game), where most citizens, especially students, have recently received implant upgrades by DigiCityNet, which enhances their connectivity and access to information.

A breach in that upgrade has caused privacy violations, misinformation and cyberbullying, targeting several users, including one of the main character's friends, Quinn, a bioengineering student, with a defamation campaign which has strained her relationship with her friends and could cost her a prestigious internship. The GM is friends with a professor who's interested in investigation and isn't too tech savvy but believes that Quinn is innocent and needs help finding the identity of the culprit to bring justice to their student. They've prepared some evidence and documents based on their research of Quinn's situation and potentially relevant topics, and asked for assistance to solve it.

### Step 2: The stakes

---

The professor, who isn't too well-versed in social media trends or digital safety, has asked the GM to task a group of students (the players) with solving this mystery and saving the character from losing her internship and reputation, restore the truth and expose the criminal to bring justice to their victims.

Additionally, if they fail to identify the culprit and solve the last enigma within a certain time limit (45 minutes), the hacker will be able to delete the evidence and get away with it, and may continue accessing other people's data and causing harm to their reputation as well.

The players' main goal is to work together to solve a series of puzzles and challenges related to digital citizenship and online safety: identify the risks in

Quinn's digital footprint, protect her privacy and data, and restore trust in her by finding proof that someone hacked her account and created fake photos to defame her, highlighting digital ethics and privacy issues.

## Phase 2: Tracking the source

**Objective:** Understand digital footprints, digital privacy and security settings and the ways to track the origin of online content.

### Step 1: The digital footprint

Players are provided with a series of numbers on a post-it or sticky note: **5298**. They're given access to a series of documents and tools to interact with physically and on a digital device (computer or tablet). Their goal is to trace the origin of the defamation campaign.

#### ◆ Puzzle content:

- ✦ **Annex 1 - Lockscreen wallpaper:** The background of the device shows 4 coloured squares in a specific order: **red, green, blue, purple**.
- ✦ **Annex 2 - Computer password:** A table contains groups of letters and numbers associated with a number from 0 to 9.

#### ✦ Clues:

- On the sticky note, the numbers are in certain colours which match the squares in the wallpaper but in a different order.
- Based on the colours, the series of numbers provided at the beginning of the phase can be rearranged to form the proper passcode: either the simple version (**2859**) or the complex one, using the table to associate each number to a group of letters and numbers are form a more complex passcode (**BB9-H3R-C3P-Z3R**).
- That passcode unlocks the computer and leads to Phase 3 Step 1.

## Step 2: Finding the culprit

---

Players find the screenshot of a chat along with a list of IP addresses and corresponding locations that'll help them identify the hacker.

### ◆ Puzzle content:

- ✦ **Annex 3 - Defamatory post:** It shows a screenshot of the first hateful post made on Quinn's account, which shows a fake picture of her along with a caption supporting an extremist group; it doesn't provide enigma solutions, only relevant context for the story.
- ✦ **Annex 4 - Screenshot of a chat with a friend:** A chat discussion between Quinn and her friend about her receiving help to identify a series of accounts and IP addresses which logged onto her account.
- ✦ **Annex 5 - Correspondence IP addresses:** A series of IP addresses with the corresponding names and postal addresses. The account names are very similar but the names and locations are completely different.

### ✦ Clues:

- Players must analyse the screenshots and identify the correct username, then match it to the IP address to trace it back to the right name and location: **Tur6o\_Per5eku7or ; 477.222.656 ; Paul Steward, 96 Bloody Street, 77-12 CitySky**
- Once players identify the solution, the GM mentions that the address sounds familiar, as it is known to be the technical headquarters of the DigiCityNet company. The culprit could likely be an employee who took advantage of their access to the implant software and sneaked through the update to access users' private data and accounts.

## Phase 3: Protecting privacy

**Objective:** Understand the importance of privacy settings and how to secure locations, personal data and digital identities.

### Step 1: Securing data

---

Players must adjust the victim's profile information and privacy settings and make her account more secure to protect her from further attacks.

#### ◆ Puzzle content:

- ✦ **Annex 6 - DigiCityNet Letter page number 56:** A sheet with multiple series of codes, including letters and numbers, along with the security parameters highlighted by DigiCityNet guidelines based on several criteria: authentication requirements, location visibility, actions against unapproved accounts and actions against suspicious accounts. Each code corresponds to a setting and guideline related to data protection.
- ✦ **Annex 7 - DigiCityNet Security account:** An Excel sheet with a mock-up of the DigiCityNet account interface, displaying the same criteria as the letter page, with empty cells where players can type in the right codes, along with a password to fill in based on provided instructions.

#### ✦ Clues:

- The letter and the Excel sheet both include the same criteria, although in a different order. Players must identify which code, or combination of letters and numbers, they should type in based on which option in the letter provides the most protection for each criterion:
- **Actions against suspicious accounts:** CT5555
- **Actions against unapproved accounts:** CT8675
- **Location visibility:** CT5540
- **Authentication requirements:** CT6723

- Players must then invent a password that matches the indicated instructions. It can be any and all words or sequences of letters or numbers, but it must involve at least 1 number, 1 uppercase letter, 1 lowercase letter and a minimum of 12 characters. A confirmation message will appear once players type in an adequate password of their choice and press Enter.

## Phase 4: Legal and ethical dilemma

**Objective:** Understand the ethical responsibilities involved in handling online defamation and how to respond to a harmful situation (ethical decision-making and legal aspects of online privacy and defamation).

### Step 1: Debate

---

Now that the players have gathered all the evidence about the culprit's identity and secured the victim's account, the GM thanks them and explains the situation: they must now decide what to do with the information they have. Players must deliberate and make a decision, considering the pros and cons of each option and discussing the ethical implications.

#### ◆ Puzzle content:

- ✦ The GM presents them with the two possible courses of action:
  - **Public exposure:** Share the evidence online and publicly accuse the culprit to prove that the victim was innocent and restore her reputation, but with risks of backlash and legal issues with the corporation involved (due to potential doxxing and defamation).
  - **Private reporting:** Report the evidence to DigiCityNet's management, which could involve an internal investigation but may not result in immediate action and could cause the victim to continue facing backlash from people who believe the defamatory accusations.



## Step 2: Decision

The correct solution will depend on the group's decision-making process after an open discussion between the players. The GM could guide them and provide hints in the form of information about similar cases or relevant laws.

- ◆ Both options could lead to positive outcomes, depending on how players approach the consequences: public exposure would help clear the victim's name directly and ensure her relationships and internship are restored but risks further damage in the legal sense since sharing private information, even that of a hacker, can be used against the players and even the victim, and get them in legal trouble. However, private reporting might lead to internal action by DigiCityNet that could hold the culprit legally accountable, through criminal charges and an arrest by the authorities, but would take more time before the public becomes aware of the truth about the victim, meaning that her internship could be revoked and her reputation would still be tarnished in the meantime.
- ◆ Once the decision is made, the GM expresses their support or doubts and asks the players to properly justify their choice. The GM can then confirm whether they believe the participants have adequately solved the issue, whether they're safe from the hacker based on how they learned to protect private data and whether they can access the lecture to complete their degree as promised. The GM promises to share the results of their investigation and their decision with Quinn and her friends, and hopes for justice to come their way thanks to the players' help.

## Phase 5: Debriefing

**Objective:** Ensuring that all participants have gathered and developed the targeted knowledge base and skills.

The GM concludes with a debriefing session, going back to the different concepts and digital citizenship issues that have been tackled and learned

throughout the escape game. Players reflect on the strategic and ethical decisions they made during the game, the importance of digital privacy and how to prevent misinformation and privacy breaches. They can discuss the impact of their actions and explore how to apply the lessons that they've learned in real life.

The GM can then close the game with a reflective discussion on ethical technology use, community engagement and the importance of responsible digital citizenship, then paint a vision for a balanced, ethical digital future that the players can participate in and improve.



Co-funded by  
the European Union

**Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the National agency Tempus Foundation. Neither the European Union nor the National agency Tempus Foundation can be held responsible for them.**

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>

**Project code: 2023-2-RS01-KA220-YOU-000170562**