Game Summaries

1. Monopoly Adaptation: Password Quest

- **Objective:** Compete to create the longest and strongest password.
- **Gameplay Mechanics:**
  - Instead of money, players collect characters to build their passwords.
  - Landing on spaces not owned may require players to give away characters.
- **Chance Cards:**
  - Adapted to represent threat scenarios:
    - "Getting hacked" sends you to jail.
    - "Account logged in by someone else" forces a password reset, losing all characters.
- **Railroads:** Represent major tech companies.
- **Free Parking:** Take a break, scroll on social media.
- **Passing "Go":** Collect 2 characters (instead of $200).
- **Winning Condition:** The player with the longest password (most characters) wins.

2. Escape Room Educational Game

- **Objective:** Students must complete their unique card to successfully escape.
- **Game Mechanics:**
  - Each student receives a card with:
    - Questions they need answers to from other students.
    - Questions they can answer for other students.
  - Questions are based on content learned throughout the year and vary between cards.
- **Completion:** Once a student's card is fully answered, they successfully escape.

3. Kahoot Cybersecurity Challenge

- **Game Format:** Utilize Kahoot to assess students' cybersecurity knowledge.
- **Gameplay:**
  - Questions feature pairs of similar images.
  - Students must identify which image represents a potential threat or phishing attempt.
    - Example: Distinguishing between an email from a friend versus a suspicious link.
- **Modes:** Play individually or collaboratively as a group.

4. Red Team / Blue Team Cybersecurity Simulation

- **Scenario-Based Activities:**
  - **War-Time Defense Game:**
    - Players defend a country (real or fictional) in a wartime scenario.
    - Defenders strategize to protect against digital threats.
    - Attackers plan to exploit vulnerabilities left by defenders.
  - **Password Escape Room:**
    - Players locate parts of a password scattered as clues.
    - Clues are user authentication questions; correct answers reveal password locations.
  - **Password Guessing Game (Wordle-style):**
    - Instead of guessing a word, players guess a user's password.

        - Guesses reveal how close they are to the correct password.
    - **Speed-Dating Password Match:**
        - Players use clues gathered about others to guess their potential passwords.
        - Closest matches win the game.

5. Real-Life Scenario Simulator

- Experience training videos and simulation activities where you face situations and make critical decisions that impact the outcome.
- Each scenario focuses on personal and data security measures to help you learn effective protection strategies.

6. Bruteforce a Password

- Code a Python script to simulate breaking into a fake social media account using password lists, teaching students about security vulnerabilities.
- Students or groups tackle multiple accounts with different passwords, marking completion by changing the hacked account’s name to theirs.

7. Authentication App

- Students create an authentication app to verify passwords and manage security questions, gaining insights into implementation and system weaknesses.

8. Strong Password Competition

- Students input a fake password into an app or website to assess its strength, aiming to create the most secure password or compete for strength ratings.

9. Biometric Authentication

- Engage in a scavenger hunt involving tasks related to understanding and interacting with biometrics, such as using fingerprint scanners or facial recognition for authentication.

10. Phishing Activity

- Recreate a popular social media platform to demonstrate how phishing schemes trick users into divulging personal information, highlighting vulnerability to identity theft.

11. Hacker Simulation:

- Conduct an unplanned activity where students interact with a simulated cyberhacker on a fake social media account to learn about protecting personal information and recognizing malicious intent.