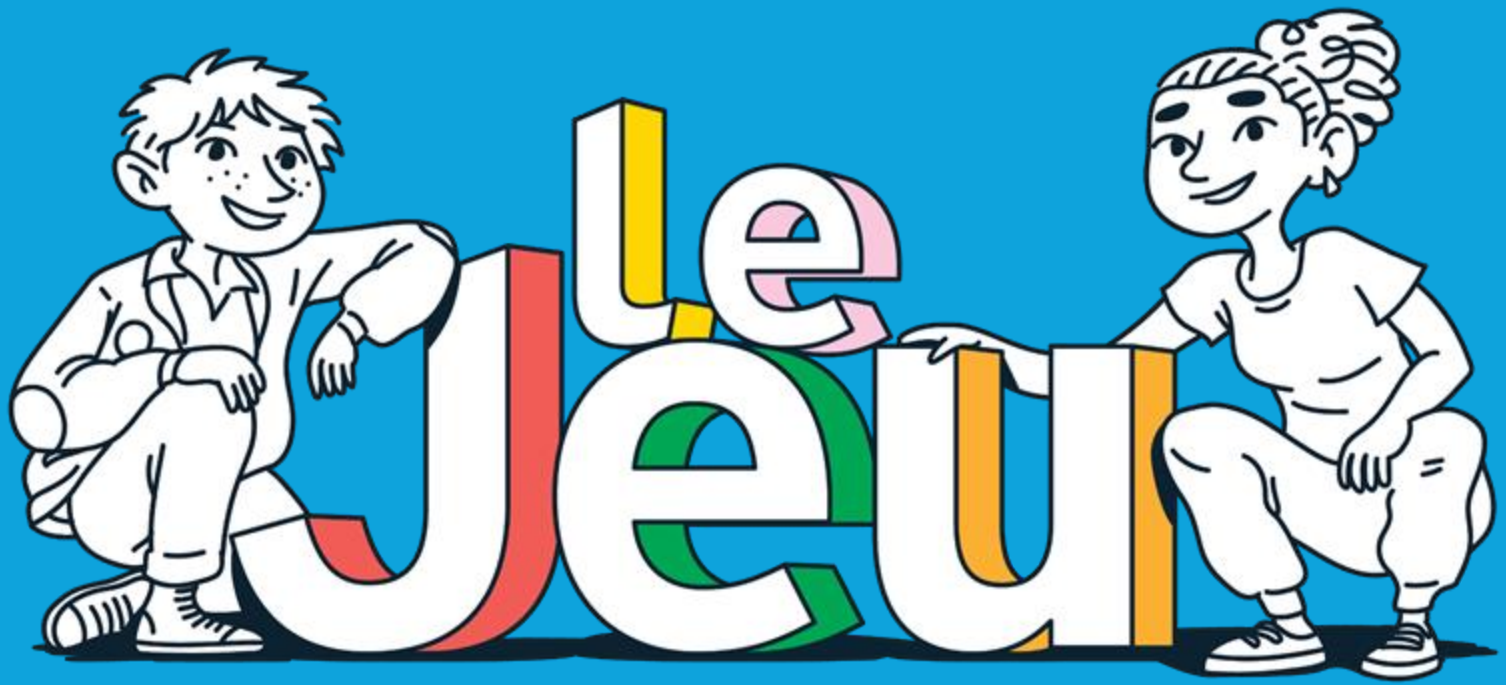


Guide des règles

2024 | Par FRESQUE DES CYBERCITOYENS

Comment utiliser ce guide ?

Ce guide a été construit pour vous aider à préparer une session de sensibilisation avec le jeu « Fresque des cybercitoyen·ne·s ».

Il contient toutes les informations nécessaires à l'animation. Nous vous conseillons cependant de suivre une séance de formation en e-learning au préalable.

Pour naviguer dans ce guide :

1. Utiliser le sommaire pages 3 et 4 : vous pouvez cliquer sur les titres pour vous rendre directement dans une section du guide ;
2. Depuis toutes les pages du guide, vous pourrez retourner au sommaire en cliquant sur l'icône  située en bas à gauche des pages.

Ce guide n'est pas fait pour être imprimé. Le jour de votre animation, munissez-vous du « Tuto Express » qui reprend toutes les informations essentielles.

SOMMAIRE

SOMMAIRE

1. INTRODUCTION

1.a Présentation générale du jeu

Le jeu "Fresque des cybercitoyen·ne·s" est une initiative éducative visant à sensibiliser les adolescents aux bonnes pratiques de sécurité numérique et à promouvoir des comportements responsables en ligne.

Conçu par Advens for People and Planet en partenariat avec l'académie de Paris et avec l'expertise en cybersécurité d'Advens, ce jeu offre une expérience ludique, collaborative et instructive pour les élèves de collège.

1.a Présentation générale du jeu

La Fresque des cybercitoyens et citoyennes se présente sous la forme d'un jeu de cartes élaboré pour encourager l'intelligence collective au sein d'équipes de joueurs qui rivalisent pour remporter la partie. En impliquant les élèves dans des discussions, des défis et des prises de décisions, le jeu offre une approche interactive et participative de l'apprentissage des pratiques de cybersécurité et de l'utilisation responsable d'internet.

Une session est divisée en deux parties :

- La première vise l'acquisition de connaissances sur la sécurité numérique ;
- La seconde permet la mise en pratique de celles-ci face à des scénarios d'attaque.

Les thématiques abordées sont :

- Le cyberharcèlement
- La désinformation
- La cyberdéfense
- Les techniques de cyberattaque
- La gestion des mots de passe
- La protection de la vie privée

Zoom sur les notions du jeu

À travers un quiz et des scénarios illustrés, les élèves pourront donc développer des connaissances sur les enjeux suivants :

1. Protection des données personnelles et outils de cybersécurité : Le jeu permet aux participants d'identifier et de protéger leurs données personnelles et de découvrir les équipements de cybersécurité pour renforcer leur sécurité en ligne.
2. Techniques de piratage et sécurité des comptes : Les cartes abordent les techniques de piratage courantes, tout en mettant l'accent sur la création de mots de passe solides et la protection des comptes en ligne.
3. Désinformation et vérification des informations : Les joueurs sont encouragés à développer leur esprit critique en comprenant le phénomène de la désinformation et en apprenant à mieux s'informer en ligne.
4. Cyberharcèlement et respect en ligne : Le jeu aborde le cyberharcèlement, favorise des discussions sur le respect en ligne et guide les participants vers des comportements constructifs et positifs. Il indique également les moyens de réagir face à ce type de situation.

1.b Objectifs pédagogiques

Les objectifs pédagogiques du jeu Fresque des cybercitoyens et citoyennes peuvent être classés en trois catégories principales : la connaissance, la réflexion et la collaboration. Ces objectifs pédagogiques sont traités à la fois à travers le contenu du jeu, c'est-à-dire les thématiques abordées, mais aussi à travers le fonctionnement du jeu.

1.b Objectifs pédagogiques

1. Connaissance

Compréhension du monde numérique

Les joueurs seront sensibilisés aux concepts clés du cyberespace, tels que la vie privée en ligne, la sécurité des données, la désinformation, etc.

Prise de conscience

Les joueurs prendront conscience de l'impact de leurs actions en ligne sur eux-mêmes, leur entourage et la société en général. Ils seront en mesure d'identifier les comportements non sécurisés et les manifestations de cyberharcèlement.

Connaissance des menaces

Les joueurs seront informés des risques du cyberespace et des attaques les plus courantes, tels que la cyberintimidation, le vol d'identité, vols de données personnelles, mais aussi des types d'attaquants et de leurs techniques : hackeur, cyberprédateur ou harceleur.

Connaissance des stratégies de prévention et d'action

Les joueurs développeront une bonne compréhension des mécanismes et des outils de prévention, ainsi que des mesures de sécurité à mettre en place. Ils sauront comment réagir de manière efficace en cas de menaces, d'attaques ou d'incidents en ligne.

2. Réflexion

Pensée éthique

Les joueurs seront encouragés à réfléchir à la dimension éthique de leurs actions en ligne et à leurs conséquences.

Prise de décisions éclairées

Les joueurs apprendront à prendre des décisions éclairées et réfléchies lorsqu'ils interagissent dans le cyberespace.

Analyse critique

Les joueurs développeront leurs compétences d'analyse en évaluant les meilleures actions à réaliser pour bloquer des attaques et relever des défis liés à la citoyenneté numérique.

3. Collaboration

Travail d'équipe

Les joueurs apprendront à collaborer au sein de leurs équipes pour échanger des idées, discuter des meilleures réponses à apporter et trouver des solutions ensemble.

Communication

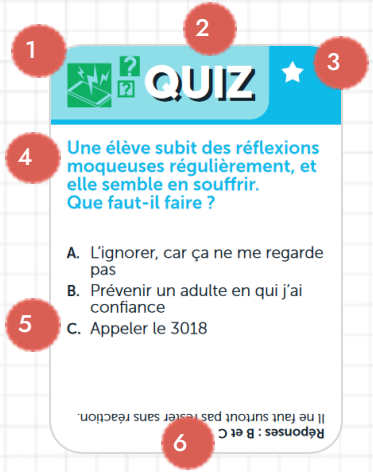
Les joueurs amélioreront leurs compétences en communication en partageant leurs opinions, en argumentant leurs points de vue et en expliquant leurs choix.

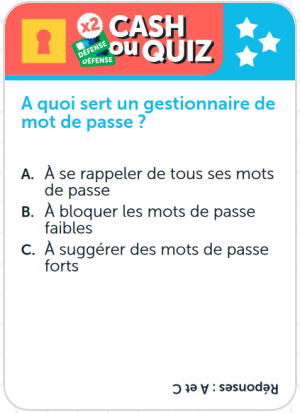
Apprentissage collectif

Les joueurs tireront parti des connaissances et des perspectives diverses de leurs coéquipiers pour enrichir leur compréhension globale de la citoyenneté numérique.

2. CONTENU DU JEU

2.a 90 cartes “Quiz”





1. Thématique de la carte (Cf Slide suivant)
2. Type de carte : Cash ou Quiz / Quiz / Vrai ou Faux
3. Niveau de difficulté : 1, 2, 3 étoiles
4. Question
5. Propositions de réponses
6. Réponse et texte explicatif
7. Dos de la carte : identique pour toutes les cartes « Quiz »

2.a Les thématiques des cartes “Quiz”

Thématique Cyberharcèlement

Thématique Cyberattaque

Thématique Désinformation

Thématique Mot de passe

Thématique Cyberdéfense

Thématique Vie Privée

Retrouvez l’explication des cartes, des sources et des liens pour aller plus loin sur chacune des thématiques dans le guide des cartes disponible sur le site fresquedescybercitoyens.fr/ressources

2.b Particularités des cartes « Défense » et « Cyberattaque »

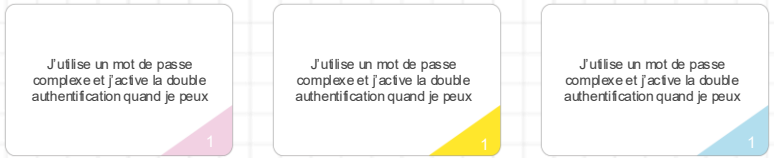
Les cartes « Défense » et les cartes « Cyberattaque » sont composées de trois lots de cartes identiques :

- 15 cartes « Défense » et 15 cartes « Cyberattaque » pour l'équipe bleue
- 15 cartes « Défense » et 15 cartes « Cyberattaque » pour l'équipe rose
- 15 cartes « Défense » et 15 cartes « Cyberattaque » pour l'équipe jaune

Tous les lots sont identiques, modulo la couleur de l'équipe. Cela permet à l'animateur de trier et ranger les cartes facilement.

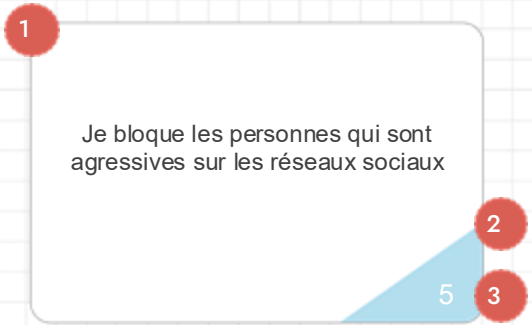
Par ailleurs, ces cartes présentent un numéro inscrit en bas à droit de la carte.

Le numéro permet à l'animateur de sélectionner ses scénarios d'attaque et d'appliquer la correction de façon simple, notamment en s'appuyant sur les propositions détaillées au Chapitre 6. Scénarios d'attaque de ce guide.
Les numéros sont identiques sur tous les lots de cartes.



Exemple pour une carte « Défense »

2.c 15 cartes “Défense” par équipe (45 cartes en tout)



1. Intitulé de la carte « Défense »
2. Couleur de l’équipe : rose, jaune ou bleu
3. Numéro de la carte
4. Dos de la carte : identique pour toutes les cartes « Défense », modulo la couleur de l’équipe

2.d 15 cartes “Cyberattaque” par équipe (45 cartes en tout)

1. Type de carte : Attaquant / Attaque / Impact
2. Intitulé de la carte « Cyberattaque »
3. Image de la carte
4. Couleur de l’équipe : rose, jaune ou bleu
5. Numéro de la carte
6. Dos de la carte : identique pour toutes les cartes « Cyberattaque » , modulo la couleur de l’équipe

3.
RÈGLES DU JEU

3.a Les règles du jeu

Dans ce jeu de cartes, chaque équipe cherche à gagner plus de points que les autres. Les équipes sont composées de 2 à 4 participants, avec un maximum de 3 équipes pour une boite de jeu.

Le but du jeu – Phase Quiz :

Les équipes se posent des questions à tour de rôle et gagnent des points en donnant la ou les bonnes réponses.

Le but du jeu – Phase Cyberattaque :

Chaque équipe détermine quelles sont les 5 meilleurs cartes « Défense » pour se protéger ou réagir face à une cyberattaque.

>> Il est possible de jouer les deux phases dans la même session d'une heure ou de les répartir sur deux heures non consécutives.

1. Première partie du jeu : Phase de « Quiz »

- Répartissez des ados en équipes de 2 à 4 personnes.

>> Maximum 3 équipes : une équipe jaune, une équipe bleue, une équipe rose.

- Proposez-leur de choisir un nom d'équipe.
- Disposez des cartes « Quiz » sélectionnées en amont au centre de la table, face cachée.

>> Pour 30 minutes de jeu, sélectionnez environ 30 cartes de niveaux équivalents.

- Chacune son tour, les équipes vont piocher une carte « Quiz » et poser la question à l'équipe à sa gauche, en tournant dans le sens des aiguilles d'une montre. Un chrono peut être ajouté pour dynamiser le jeu.

>> L'équipe qui pose la question doit lire le type de carte, la question et les propositions de réponse (sauf pour les cartes « Cash ou Quiz »). Après concertation, l'équipe adverse répond à la question posée en choisissant aucune, une, deux ou trois bonnes réponses. L'équipe qui a posé la question doit lire la ou les bonnes réponses et le texte explicatif.

- Lorsqu'une équipe répond juste, elle gagne 1 carte « défense » piochée dans le paquet de son équipe (rose, bleu ou jaune).

>> Spécificité des cartes « Cash ou Quiz » : L'équipe qui pose la question ne lit pas les propositions de réponses et propose à l'équipe adverse de répondre « Cash ». Si l'équipe choisit le mode « Cash » et a au moins une réponse juste, elle gagne 2 cartes « défense ». Si elle n'est pas sûre de connaitre la réponse, elle peut choisir le « Quiz ».

- A la fin de cette première phase, comptez les « points » - Chaque carte « Défense » gagnée rapporte 1 point.

2. Deuxième partie du jeu : Phase « Scénario d'attaque »

- Demandez aux équipes de disposer toutes les cartes « Défense » devant elles (15 cartes en tout), même celles qu'elles n'ont pas gagnées lors de la précédente phase.
- Disposez une séquence d'attaque identique devant chacune des équipes (vous pouvez vous aider du guide animateur, Chapitre 6. Scénarios d'attaque).
- Les équipes doivent réfléchir aux cinq meilleures cartes « Défense » à utiliser pour bloquer l'attaque et les disposer sous la séquence d'attaque.

>> Seules les cartes « Défense » ayant un rapport direct avec l'attaque rapportent des points.

- Lorsqu'elles ont terminé (il peut être nécessaire d'utiliser un chrono d'environ 10 min), corrigez avec chacune des équipes ou faites une correction collective selon le temps dont vous disposez.
- Comptez les points - Chaque carte « Défense » correctement utilisée rapporte 1 point. Vous pouvez également vous aider de notre correction dans le Chapitre 6. Scénarios d'attaque.

- Additionnez les points des deux phases de jeu :

L'équipe qui a le plus de points a gagné !

3.b Le déroulement d'une session

Vous trouverez sur les slides d'après deux exemples de déroulé d'ateliers pouvant être menés dans un contexte scolaire.

Il est cependant possible de les adapter, par exemple :

- En passant moins de temps sur le Quiz et en traitant deux scénarios d'attaque ;
- En complétant une session Quiz par une séance de sensibilisation en classe sur la ou les thématiques abordées ;
- En proposant une activité type Ice-Breaker durant l'introduction.

Pour une première animation, nous vous suggérons de ne pas mener les deux parties du jeu dans la même session d'une heure (Exemple 1).

Par ailleurs, nous vous recommandons de ne pas faire durer le jeu plus d'une heure pour maintenir la concentration des élèves.

Le déroulement d'une séance est détaillé dans le chapitre 5. Animer une Fresque

3.b Le déroulement d'une session – Exemple 1

Durée : 60 minutes

Nombre de participants : 24 élèves (répartir 2 groupes de 12 avec 2 jeux « Fresque des cybercitoyens »)

Nombre d'encadrants : 1 animateur confirmé ou 2 animateurs débutants

Déroulé :

1. Introduction [0 -> 10 min]

Mise en équipe et choix du nom de leur équipe

Présentation de l'atelier (objectifs, règles de l'atelier, etc...)

2. Explication des règles du quiz [10 -> 15 min]

3. Phase de quiz [15 -> 45 min]

5. Fin de l'activité [45 -> 55 min]

Annonce des vainqueurs

Tour de table pour avoir des retours sur l'atelier

6. Après l'atelier [55 -> 60 min]

Tri des cartes et rangement du jeu

Rangement de l'espace de jeu

3.b Le déroulement d'une session – Exemple 2

Durée : 60 minutes

Nombre de participants : 27 élèves (répartir 3 groupes de 9 avec 3 jeux « Fresque des cybercitoyens »)

Nombre d'encadrants : 2 animateurs confirmés ou 3 animateurs débutants

Déroulé :

1. Introduction [0 -> 5 min]

Mise en équipe et choix du nom de leur équipe

Présentation de l'atelier (objectifs, règles de l'atelier, etc...)

2. Explication des règles du quiz [5 -> 10 min]

3. Phase de quiz [10 -> 35 min]

4. Explication des règles de la phase scénario d'attaque et mise en place [35 -> 40 min]

5. Phase du scénario d'attaque [40 -> 50 min]

6. Fin de l'activité [50 -> 55 min]

Annonce des vainqueurs

Tour de table pour avoir des retours sur l'atelier

7. Après l'atelier [55 -> 60 min]

Tri des cartes et rangement du jeu

Rangement de l'espace de jeu

3.b Le déroulement d'une session

1. Première partie du jeu : Phase de « Quiz »

- Il y a plusieurs types de question :
  - Vrai ou faux :
    - Un point gagné par bonne réponse.
  - Quiz :
    - Zéro, une, deux ou trois bonnes réponses possibles ;
    - Toutes les bonnes réponses doivent être données pour gagner le point ;
    - Un point gagné par bonne réponse.
  - Cash ou quiz (1 ou 2 points gagnés) :
    - Une, deux ou trois bonnes réponses possibles ;
    - Un point gagné si réponse type quiz, c'est-à-dire avec les propositions de réponses ;
    - Deux points gagnés si l'équipe répond cash, c'est-à-dire sans les propositions de réponses ;
    - Une seule bonne réponse peut être donnée pour gagner les deux points si réponse cash.
- Les points gagnés peuvent être matérialisés par des cartes « Défense » que les équipes piochent au fil de la partie.

3.c Compter les points

1. Première partie du jeu : Phase de « Quiz »

- Il y a plusieurs types de question :
  - Vrai ou faux :
    - Un point gagné par bonne réponse.
  - Quiz :
    - Zéro, une, deux ou trois bonnes réponses possibles ;
    - Toutes les bonnes réponses doivent être données pour gagner le point ;
    - Un point gagné par bonne réponse.
  - Cash ou quiz (1 ou 2 points gagnés) :
    - Une, deux ou trois bonnes réponses possibles ;
    - Un point gagné si réponse type quiz, c'est-à-dire avec les propositions de réponses ;
    - Deux points gagnés si l'équipe répond cash, c'est-à-dire sans les propositions de réponses ;
    - Une seule bonne réponse peut être donnée pour gagner les deux points si réponse cash.
- Les points gagnés peuvent être matérialisés par des cartes « Défense » que les équipes piochent au fil de la partie.

2. Deuxième partie du jeu : Phase « Cyberattaque »

- L'animateur positionne une séquence d'attaque (cf Chapitre 6. Scénarios d'attaque)
- Les équipes ont 10 minutes pour échanger et positionner les cinq meilleures cartes « Défense » correspondant au scénario d'attaque :
  - Mauvaise carte : 0 point
  - Bonne carte : 1 point
- Si vous disposez du temps nécessaire, vous pouvez demander aux équipes de justifier le choix des cartes « Défense » et accorder des points supplémentaires si la justification est cohérente avec le scénario.

4. SÉQUENCE PÉDAGOGIQUE

4. Construire une séquence pédagogique

Pour que le jeu se joue dans les meilleures conditions et pour maximiser l'atteinte de objectifs pédagogiques de la Fresque, il est fortement conseillé de sélectionner en amont les cartes Quiz et le scénario d'attaque associé en fonction du niveau des élèves et des thématiques que l'on souhaite aborder.

En effet, si vous disposez l'intégralité des 90 cartes Quiz devant les élèves, la difficulté des questions posées (indiquée par 1, 2 ou 3 étoiles) variera d'une équipe à l'autre et cela risque de créer un sentiment d'injustice, de frustration voire d'échec pour certains élèves ou équipes.

4. Construire une séquence pédagogique

1. Sélectionner les thématiques

En fonction des thématiques que vous souhaitez aborder, vous pouvez trier les questions et sélectionner les cartes que vous placerez devant les élèves lors de la première partie du jeu. Dans un second temps, vous pourrez définir un scénario d'attaque associé aux thématiques apprises lors de la première phase. Pour rappel, les thématiques sont indiquées en haut à gauche des cartes « Quiz » et sont répertoriées au slide 2.a Les thématiques des cartes "Quiz". Vous pourrez identifier le bon scénario d'attaque grâce au Chapitre 6. Scénarios d'attaque.

2. Sélectionner le niveau des cartes

Une fois la thématique choisie, vous pourrez sélectionner le niveau des cartes en fonction de la connaissance des élèves sur la thématique abordée. Celui-ci est indiqué en haut à droite des cartes « Quiz » avec une étoile (1 étoile étant le niveau facile).

3. Exemple d'une séquence pédagogique

Session	Classe	Thématiques abordées	Sélection de 30 cartes Quiz	Scénario d'attaque	Cartes « Défense »
1	6e	Cyberharcèlement & mot de passe	Cartes de niveau 1 sur les thématiques abordées	3 -> 6 -> 7 -> 12	7 - 15 - 9 - 1
2	6e	Cyberharcèlement & vie privée	Cyberharcèlement : Sélection de cartes de niveau 1 & 2 Vie privée : Cartes niveau 1	2 -> 6 -> 14	7 - 8 - 9 - 10 - 13
3	5e	Piratage, mot de passe & équipement	Cartes de niveau 1 sur les thématiques abordées	1 -> 5 -> 9 -> 13	4 - 2 - 3 - 12 - 11

3. Exemple d'une séquence pédagogique

Session	Classe	Thématiques abordées	Sélection de 30 cartes Quiz	Scénario d'attaque	Cartes « Défense »
4	5e	Révision des acquis des sessions 1 à 3	Cartes de niveaux 1 & 2, sur les thématiques cyberharcèlement, piratage, mot de passe, équipement & vie privée	2 -> 5 -> 7 -> 12	4 - 11 - 15 - 1 - 7
5	4e	Désinformation, vie privée & équipement	Désinformation : Cartes de niveau 1 & 2 Vie privée et équipement : Cartes de niveau 2 & 3	1 -> 9 -> 4 -> 11	2 - 3 - 7 - 11 - 15

4. Construire une séquence pédagogique

Session	Classe	Thématiques abordées	Sélection de 30 cartes Quiz	Scénario d'attaque	Cartes « Défense »
6	4e	Piratage, équipement & mot de passe	Cartes de niveaux 2 & 3 sur les thématiques abordées	1 -> 10 -> 11 -> 12	14 - 15 - 1 - 7 - 11
7	3e	Toutes les thématiques	Sélection de cartes de niveaux 2 & 3 sur l'ensemble des thématiques	Au choix	X
8	3e	Toutes les thématiques	Sélection de cartes de niveaux 2 & 3 sur l'ensemble des thématiques	Au choix	X

5.
ANIMER UNE FRESQUE

5.a Généralité sur le rôle de l'animateur

Lors de la création de cette fresque, nous avons voulu que tout le monde puisse animer une session : il suffit de lire ce guide et de suivre les cartes : aucune connaissance en cybersécurité n'est préalablement requise. En effet, l'animateur n'a pas le rôle d'enseigner dans ce cadre, mais bien de faire respecter le cadre du jeu.

5.a Généralité sur le rôle de l'animateur

L'animateur de l'atelier a un ensemble de responsabilités clés :

1. Préparer la session (Cf 5b. Avant l'Atelier)
2. Accueillir et gérer le groupe (Cf 5c. Pendant l'Atelier)
3. Guider et faciliter la session de sensibilisation :

- Répondre aux questions et définir les termes si besoin à l'aide du glossaire ;
- Assurer le respect des principes du jeu (respect mutuel, atmosphère positive...) ;
- Encourager les équipes et rester à l'écoute ;
- Assurer le bon respect du temps.

4. Conclure et réaliser le bilan de l'atelier (Cf 5c. Pendant l'atelier et 5d. Après l'Atelier)

- Conclusion à la fin de session avec les participants ;
- Rangement du jeu ;
- Déclaration de la session via le QR Code sur la boite.

5.b Avant l'atelier

Si c'est votre premier atelier, nous vous recommandons de récupérer, voire d'imprimer si vous le juger nécessaire, le Tuto Express : vous y trouverez l'ensemble des documents pour animer une séance « clef en main ». Pour rappel, ce guide n'a pas vocation à être imprimé.

En amont de l'atelier :

1. Trouvez des personnes disponibles et formées pour vous aider à encadrer : nous recommandons un animateur par jeu (soit pour 12 participants maximum).
2. Définissez votre séquence pédagogique selon les connaissances et la maturité des participants et les notions que vous souhaitez aborder. Pour cela, vous pouvez vous aider de la section 4. Séquence Pédagogique de ce guide.
3. Vérifiez que vous disposez du matériel nécessaire :
    - Jeu de la fresque (1 jeu pour 12 élèves au maximum) ;
    - La version « Tuto express » du Guide animateur ;
    - Un papier et un stylo pour faire le compte des points ;
    - En option : Un chrono (montre, sablier, téléphone) pour chronométrer et dynamiser le jeu.

5.c Le jour de l'atelier

Le jour de l'atelier, voici les consignes pour préparer la salle avant le début de la séance de sensibilisation :

1. Une table dispose d'un jeu « Fresque des cybercitoyen·ne·s » et d'un animateur :
   - Si vous avez plusieurs groupes, c'est-à-dire plus de 12 jeunes en même temps, vous devrez créer plusieurs îlots de tables disposant chacune d'un jeu ;
   - Si vous avez un groupe de 12 participants ou moins, une seule table de jeu sera suffisante.

2. Configurez l'espace de jeu en créant idéalement des îlots adaptés au nombre de joueurs. Si vous êtes plusieurs animateurs, répartissez-vous dans les différents espaces de manière que chacun soit responsable d'une zone de jeu. Une session peut être relativement bruyante : essayez tant que possible d'espacer les îlots les uns des autres.

3. Placez les cartes « Quiz » sélectionnées pour la séance au centre de chacun des îlots :
   - Réservez les paquets de cartes « Défense » que vous distribuerez au début de la partie ;
   - Réservez les scénarios d'attaque que vous avez préparés pour la deuxième partie de la séance.

1. Introduction

Cette première phase d'introduction peut être réalisée avec l'ensemble des groupes, par exemple en classe entière, avant de répartir les élèves par groupe de 12 maximum. Transmettez les informations essentielles aux participants :

- Présentez-vous si c'est la première fois que vous rencontrez ce public ;
- Expliquez l'objectif de cette séance de sensibilisation ;
- Décrivez brièvement le déroulé de la séance et donnez les durées des deux parties (les règles seront expliquées après) ;
- Explicitez ce que les joueurs sont autorisés à faire (parler librement, s'entraider, donner des définitions, etc…)

Afin de briser la glace, vous pouvez également poser quelques questions aux jeunes ou faire un sondage à main levée :

- Qu'est ce que c'est que pour vous la cybersécurité ?
- Que font les hackeurs ou une hackeuses ?
- Qui ici a déjà eu un virus informatique ?
- Qui a déjà eu un compte piraté ?
- Qui a déjà reçu une tentative d'escroquerie par message ?

2. Création des groupes et des équipes

Répartissez les élèves en groupe : chaque groupe sera affecté à une table de jeu avec son animateur.
Puis répartissez les élèves en équipes de 4 joueurs maximum. Ici deux possibilités, à vous de déterminer le plus appréciable :

- Vous pouvez laisser les jeunes se mettre en équipes comme ils veulent ;
- Vous pouvez répartir les participants en équipes vous-même.

Dans le second cas, cela peut permettre d'homogénéiser le niveau des équipes et de briser certaines dynamiques afin de rendre le groupe plus facile à encadrer, cependant cela peut également générer de la frustration.

Afin de renforcer l'implication, vous pouvez demander à chaque équipe de se trouver un nom.

3. Explication des règles

Expliquez en premier le déroulement global du jeu :

- Le jeu se déroule en deux phases : la première c'est un Quiz, auquel ils répondront par équipe, et dans la seconde ils devront repousser une cyberattaque ;
- Durant chaque phase, les équipes pourront marquer des points ;
- L'équipe avec le plus de points à l'issue des deux phases aura gagné.

Puis expliquez les règles du Quiz plus en détail (Cf Chapitre 3.a Règles du jeu). Il n'est pas nécessaire d'expliquer dès à présent les règles du scénario car cela pourra créer de la confusion.

Vous pouvez désigner un maître du temps qui aura pour tâche de veiller au respect des différents temps de jeu ou bien le faire vous-même.

4. Mise en place du quiz

Cf Chapitre 3.a Règles du jeu

5. Conseils d'animation (1/2)

Durant la phase de Quiz, le jeu est fait pour être cogéré par les joueurs, voici cependant un ensemble de conseils pour vous permettre d'animer au mieux l'activité :

- N'hésitez pas à circuler entre les différentes équipes afin de veiller au bon déroulement du jeu ;
- Assurez-vous que les échanges se déroulent bien entre les équipes ;
- Assurez-vous que chaque équipe prend le temps de réfléchir et d'argumenter avant de donner sa réponse ;
- Après qu'ils ont répondu à une question, vous pouvez leur demander s'ils connaissaient le sujet ou bien si cela leur était déjà arrivé afin de renforcer l'implication et l'interactivité. Cependant il ne faut pas trop en abuser au risque de diminuer la prise d'autonomie et le rythme du jeu ;
- Si vous voyez qu'une question ou qu'un terme n'est pas compris, vous pouvez le reformuler ou donner la définition. Le mieux reste toutefois de demander à un volontaire d'essayer d'expliciter les notions avec ses propres mots et/ou de donner un exemple pour ses camarades ;

5. Conseils d'animation (2/2)

Durant la phase de Quiz, le jeu est fait pour être cogéré par les joueurs, voici cependant un ensemble de conseils pour vous permettre d'animer au mieux l'activité :

- En règle générale, plus vous vous appuierez sur leurs expériences personnelles plus ils seront impliqués dans l'activité ;
- Observez les équipes qui pourraient potentiellement se démotiver et n'hésitez pas à les encourager ;
- A une minute de la fin du temps alloué à la phase de Quiz, faite une annonce pour dire que cela sera le dernier tour.

5. Fin du quiz & mise en place de l'attaque

Après avoir réclamé l'attention et mis fin à la partie « Quiz », vous pouvez faire une annonce des scores.

Puis expliquez les règles du Scénario d'attaque (Cf Partie 3.a Règles du jeu) et la façon dont les points seront gagnés.

Demandez ensuite à chaque équipe de disposer toutes les cartes « Défense » devant eux (15 cartes par équipe). Pendant ce temps, disposez le scénario d'attaque préalablement choisi en relation avec la thématique abordée lors du « Quiz » devant chacune des équipes, et expliquez ce scénario. Pour une meilleure immersion, nous vous recommandons de présenter le scénario de façon romancée et de ne pas juste lire les cartes. Vous pouvez vous appuyer sur nos scénarios dans la partie Chapitre 6. Scénarios d'attaque.

Par exemple : Une cyberharceleuse réussit à trouver ton mot de passe et elle a donc accès à tous tes comptes (Insta, Snap, ENT…). Elle va en profiter pour se faire passer pour toi, c'est-à-dire « usurper ton identité », pour envoyer des messages à tes amis ou à des profs. Qu'est-ce que vous pouvez utiliser comme carte « Défense » pour empêcher que cela se produise ? Ou pour réagir si c'est trop tard ?

6. Correction de la deuxième partie

Pour corriger le scénario, vous pouvez :

- Faire une correction individuelle par équipe ;
- Vous appuyer sur une équipe pour faire la correction générale.

7. Fin de l'activité

La fin de l'activité doit être un moment de conclusion du jeu et d'un retour au calme mais également permettre d'avoir un retour des participants sur leur expérience. Pour cela nous vous proposons de :

1. Demander le tri et le rangement des cartes par couleur, c'est-à-dire par équipe ;
2. Faire l'annonce de l'équipe vainqueur et la féliciter ;
3. Faire un tour de table pour recueillir les impressions.

5.d Pendant l'atelier

Selon le temps disponible et le nombre de participants, vous pouvez faire un tour de table où chaque participant s'exprime à tour de rôle.

Par exemple : Chaque participant dit une notion qu'il a apprise, un élément du jeu qu'il a aimé et un élément qu'il a moins aimé.

Si le groupe est trop important ou que vous êtes à court de temps, vous pouvez faire par sondage à main levée :

- Qui va changer son mot de passe en rentrant ?
- Qui n'a pas aimé l'activité ? / Qui a bien aimé ? / Qui a beaucoup aimé l'activité ?
- Qui n'a rien appris de nouveau ? Qui a un peu appris ? Qui a beaucoup appris ?

Cette phase est très importante pour l'apprentissage : elle permet de fixer les notions apprises lors de la séance et de se questionner sur ses pratiques.

5.e Après l'atelier

Après l'atelier, chaque animateur est invité à scanner le QR Code qui se trouve sur le dos de la boite de jeu pour déclarer la session en remplissant les informations suivantes :

- Le nombre de participants et d'animateurs ;
- Age moyen (9-10 ans ; 11-12 ans; 13-14 ans ; 15-16 ans) ;
- Le numéro de département ;
- Evaluation de la session selon l'animateur ;
- Des axes d'amélioration identifiés.

Aucune des sections n'est obligatoire. Cependant, pour que ce jeu continue d'exister et de s'améliorer, il est essentiel que vous nous fassiez des retours sur votre expérience et sur celle des participants. En effet, ce jeu ne pourra continuer d'exister et de s'améliorer qu'avec votre aide. De plus, la complétion du questionnaire de retour vous donnera accès à une page web cachée vous permettant de suggérer une nouvelle question de quiz : la meilleure question suggérée sera intégrée dans la prochaine édition de la fresque.

5.f Facteurs clés de succès d'une session

1

Préparation de la session

La phase de préparation de la session de sensibilisation (choix des thématiques et des niveaux) est essentielle pour maximiser son impact sur les collégiens.

RDV sur 4. Préparer sa séquence pédagogique

2

Présence d'un animateur par jeu

La présence d'au moins un animateur par groupe (c'est-à-dire par jeu) permet de mieux cadrer la séance et d'identifier de potentiels situations problématiques rencontrées par les élèves.

3

Répartition préalable des joueurs dans les équipes

La constitution des équipes à l'avance permet de mélanger les niveaux des élèves, optimisant ainsi l'impact de la séance de sensibilisation et leur engagement dans le jeu.

4

Plusieurs parties

Une séance est plus efficace lorsqu'elle est divisée en deux phases : une heure dédiée au Quiz et une autre à la phase « Cyberattaque ». Plusieurs sessions permettent de consolider les connaissances et d'adopter de bons réflexes.

6. SCÉNARIOS D'ATTAQUE

6. Scénarios d'attaque

Exemples de scénario clef en main

Vous trouverez ci-dessous des propositions de scénarios d'attaque classés par type d'attaquants. Vous pouvez également créer vos propres scénarios en sélectionnant des cartes « Attaquant », « Attaque » et « Impact ».

4.a Hackeur.se

Scénario	Cartes « Cyberattaque »	Cartes « Défense »
Une hackeuse propage un virus sur ton téléphone ou ton ordinateur qui lui permet d'avoir accès à tes comptes et elle revend tes données sur le dark web.	1 -> 9 -> 4 -> 11	2 - 3 - 7 - 11 - 15
Un hackeur pirate un réseau wifi public. Comme il voit tout ce qui transite sur le réseau, il capte ton mot de passe et vole l'accès à tes comptes. Alors, il décide de revendre tes données sur le dark web.	1 -> 10 -> 4 -> 11	1 - 7 - 11 - 14 - 15
Même scénario que ci-dessus, mais cette fois-ci le hackeur décide de te faire chanter : par exemple, il te demande de l'argent pour te rendre tes accès à tes comptes sur les réseaux sociaux.	1 -> 10 -> 4 -> 14	1 - 8 - 11 - 14 - 15

4.a Hackeur.se

Scénario	Cartes « Cyberattaque »	Cartes « Défense »
Un hackeur se renseigne sur toi sur internet. Comme il voit tout ce que tu as publié, il devine ton mot de passe. Avec celui-ci, il récupère tes accès à tes comptes et usurpe ton identité (= il se fait passer pour toi).	1 -> 6 -> 4 -> 12	1 - 7 - 9 - 10 - 11 - 13 - 15
Un hackeuse t'envoie un mail de phishing. Tu cliques le lien dans le mail et cela installe un virus sur ton appareil qui supprime tes données.	1 -> 5 -> 9 -> 13	2 - 3 - 4 - 11 - 12
Un hackeuse t'envoie un mail de phishing. Tu cliques le lien dans le mail et cela installe un virus sur ton appareil et revend tes données sur le dark net.	1 -> 5 ->9 -> 4 -> 11	1 - 2 - 3 - 4 - 7 - 11 - 15

4.b Cyberprédateur.trice

Comme vous pourrez le constater, les attaques des cyberharceleurs et cyberprédateurs sont quasiment similaires. Ce qui diffère c'est le type d'attaquant et son objectif final : le prédateur attend généralement quelque chose d'intime en échange de son « attaque ».

Choisissez l'une ou l'autre selon la thématique que vous souhaitez aborder avec votre public.

Scénario	Cartes « Cyberattaque »	Cartes « Défense »
Une cyberprédatrice se renseigne sur toi, par exemple via les réseaux sociaux et elle te fait chanter : par exemple, elle te demande de lui envoyer des photos intimes. En échange, elle te fait croire qu'elle ne va pas envoyer des informations personnelles sur toi à tes amis ou tes parents.	2 -> 6 -> 14	5 - 7 - 8 - 9 - 10 - 13

4.b Cyberprédateur.trice

Scénario	Cartes « Cyberattaque »	Cartes « Défense »
Un cyberprédateur se renseigne sur toi, par exemple sur les réseaux sociaux, et te harcèle par messages ou à l'école.	1 -> 8 -> 15	5 - 6 - 7 - 8 - 13
Un cyberprédateur t'envoie un message de phishing afin de trouver ton mot de passe. Avec tes comptes, il se fait passer pour toi (= usurpe ton identité) pour obtenir des rendez-vous avec tes amis.	2 -> 5 -> 7 -> 12	1 - 4 - 7 - 8 - 11 - 15
Une cyberprédatrice se renseigne sur toi et avec les informations qu'elle a obtenues, elle trouve ton mot de passe et usurpe ton identité. Elle contacte tes amis et tente d'obtenir des photos intimes.	2 -> 6 -> 7 -> 12	1 - 7 - 8 - 9 - 10 - 11 - 13 - 15

4.c Harceleur.se

Scénario	Cartes « Cyberattaque »	Cartes « Défense »
Un cyberharceleur se renseigne sur toi sur internet. Avec les infos qu'il trouve, il décide de faire chanter : par exemple, il te demande de faire ses devoirs. En échange, il te dit qu'il n'enverra pas certaines photos de toi à toute la classe.	3 -> 6 -> 14	5 - 7 - 8 - 9 - 10 - 13
Une cyberharceleuse te trouve sur les réseaux sociaux et t'envoie des messages injurieux	3 -> 8 -> 15	5 - 6 - 7 - 8 - 13
Un cyberharceleur devine ton mot de passe et se fait passer pour toi sur les réseaux sociaux ou sur l'ENT.	3 -> 7 -> 12	1 - 4 - 7 - 8 - 11 - 15
Une cyberharceleuse se renseigne sur toi, trouve ton mot de passe et te fait du chantage ou te menace de diffuser des infos persos sur toi.	3 -> 6 -> 7 -> 14	1 - 5 - 7 - 8 - 9 - 10 - 11 - 13 - 15

7.
FOIRE AUX QUESTIONS

Comment réagir si on me pose une question dont je ne connais pas la réponse ?

Nous avons tenté de mettre le plus d'informations possibles dans ce guide et dans le guide des cartes et des sources pour vous permettre de répondre à la plupart des questions que pourraient avoir les participants.

Cependant il est toujours possible que vous soyez confronté à une question dont vous ne trouvez pas immédiatement la réponse. Dans ce cas, nous vous recommandons d'être transparent : avouez ne pas savoir. Vous pouvez alors lui proposer de vous renseigner et de revenir vers lui ou bien lui proposer de chercher la réponse de son côté et ensuite de la transmettre à l'ensemble du groupe.

Vous pouvez également nous transmettre vos questions à l'adresse fresquedescybercitoyens@advens.fr pour que nous puissions intégrer la réponse dans le guide.

Comment réagir si un jeune vient se confier concernant une situation de harcèlement ? (1/2)

Le contexte du jeu peut amener certains jeunes à venir se confier à vous concernant des situations de harcèlement dont ils ont été ou sont toujours victimes ou témoins. D'ailleurs, nous insistons beaucoup dans le jeu pour rappeler qu'il faut en parler à un adulte de confiance.

Il est difficile d'établir une recommandation globale, mais voici quelques conseils de la fondation de France : https://www.fondation-enfance.org/jai-besoin-daide/je-suis-adulte/mon-enfant-est-temoin/suis-enseignant-directeur-decole-chef-detablissement/

Il est essentiel dans tous les cas de :

- Faire attention à ne pas minimiser la situation ou son impact sur le jeune ;
- Recueillir la parole de la personne qui se confie ;

…

Comment réagir si un jeune vient se confier concernant une situation de harcèlement ? (2/2)

Il est essentiel dans tous les cas de :

- Réagir proportionnellement à la situation décrite, mais réagir dans tous les cas ;
- S'informer : il n'est pas toujours facile d'identifier une victime de harcèlement, mais certains indices peuvent mettre sur la voie (isolement, décrochage scolaire...) ;
- Vous pouvez également appeler le numéro suivant pour obtenir des conseils :
    - 3018 (Accessible par Whatsapp, Messenger, Appel, Mail) : le numéro national pour les jeunes victimes de violences numériques et toutes les questions liées aux usages numériques. Retrouvez les infos sur https://e-enfance.org/numero-3018/besoin-daide/

Je ne suis pas un expert de la cybersécurité, comment vais-je faire pour animer ? (1/2)

Premièrement, ce n'est pas à vous qu'il incombe la charge d'apporter les connaissances sur la cybersécurité : le jeu et le guide ont été réalisés par des professionnels du domaine. Nous avons tenté de le rendre le plus « clé en main » possible pour qu'une personne sans connaissance préalable puisse l'animer après une rapide formation et la lecture de ce guide.

De plus, le jeu est quasiment autoporteur. Vous pouvez donc animer des ateliers, même sans compétence technique préalable.

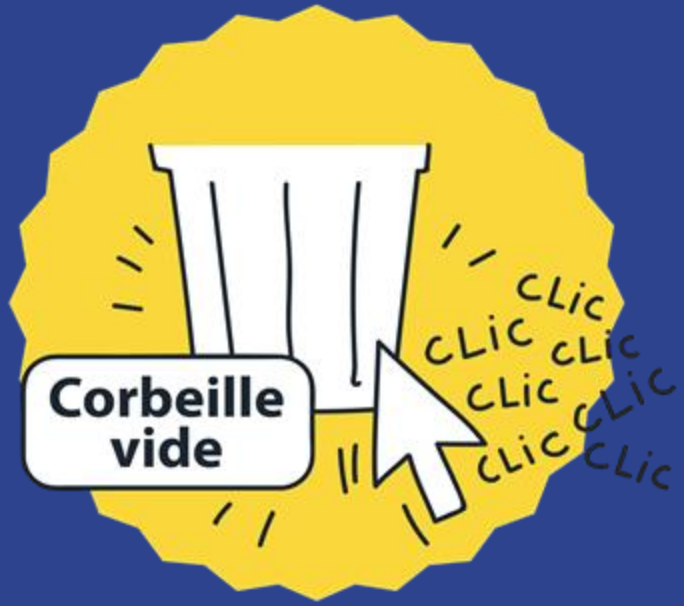
Enfin, en admettant humblement votre propre « non-expertise » dans ce domaine, vous pouvez créer un environnement propice à l'apprentissage collaboratif. Encouragez la réflexion critique, favorisez les discussions et fournissez des ressources (définitions, scénario…) pour aider les participants à se former à être des cybercitoyens et cybercitoyennes responsables.

8. FAQ

Je ne suis pas d'accord avec une carte, que puis-je faire ?

Il est difficile parfois de trouver l'équilibre entre être exhaustif tout en restant dans la pédagogie : des choix ont donc été faits lors de la création de ce jeu. N'hésitez donc pas à vous approprier le jeu si vous pensez que cela peut permettre de renforcer les compétences des participants. N'hésitez pas à nous envoyer toutes vos suggestions d'amélioration afin que nous puissions enrichir le jeu à l'adresse suivante : fresquedescybercitoyens@advens.fr

Retrouvez le reste de la FAQ sur le site web « www.fresquedescybercitoyens.fr »



8. GLOSSAIRE

8. Glossaire

Mot	Définition
Antivirus	Un logiciel conçu pour détecter, prévenir et éliminer les logiciels malveillants de votre système informatique.
Application	Un programme informatique conçu pour effectuer des tâches spécifiques sur un dispositif électronique, comme un smartphone ou un ordinateur.
Brute force	Une méthode d'attaque informatique où toutes les combinaisons possibles sont essayées pour trouver un mot de passe ou une clé de chiffrement.
Chiffrer	Protéger des données en les transformant en un code illisible sans la clé de déchiffrement correspondante.

8. Glossaire

Mot	Définition
ChatGPT	Un modèle de langage développé par OpenAI, capable de comprendre et de générer du texte en langage naturel.
Cloud	Un service de stockage en ligne permettant d'accéder aux données via Internet plutôt que depuis un disque dur local.
Code PIN	Un numéro confidentiel utilisé pour authentifier un utilisateur, souvent associé à des cartes bancaires ou des appareils électroniques.
Compte	Un ensemble d'informations personnelles et d'autorisations associées à un utilisateur dans un système informatique.

8. Glossaire

Mot	Définition
Cookies	De petits fichiers texte stockés sur un ordinateur par un navigateur web, contenant des informations sur les habitudes de navigation de l'utilisateur.
Cyberharcèlement	L'utilisation d'Internet et des technologies pour harceler, menacer ou intimider une personne
Cyberprédateur	Une personne utilisant Internet pour cibler et exploiter des individus vulnérables, en particulier des mineurs.
Dark web	Une partie d'Internet inaccessible aux moteurs de recherche conventionnels, souvent associée à des activités illégales.

8. Glossaire

Mot	Définition
Défaçage	Modifier le contenu d'un site web, souvent dans un but malveillant, pour afficher un message ou une image indésirable.
Déni de service	Une attaque visant à rendre un service indisponible en submergeant le serveur de requêtes.
Données	Informations stockées, traitées et utilisées par des systèmes informatiques.
Double authentification	Un mécanisme de sécurité exigeant deux formes d'identification différentes pour accéder à un compte ou un système.

8. Glossaire

Mot	Définition
Fake news	Informations fausses ou trompeuses présentées comme des faits réels, généralement diffusées sur Internet.
Faire chanter	Menacer de divulguer des informations compromettantes pour obtenir un avantage, souvent sous la forme d'argent.
Gestionnaire de mots de passe	Un outil facilitant la gestion et la sécurisation des mots de passe en les stockant de manière chiffrée.
Hackeur	Une personne utilisant ses compétences techniques pour accéder à des systèmes informatiques de manière non autorisée. Il existe cependant des hackeurs éthiques qui agissent légalement pour trouver des failles dans des systèmes d'information.

8. Glossaire

Mot	Définition
Historique	La liste des sites web visités et des actions effectuées sur un navigateur web.
Intelligence artificielle	Des systèmes informatiques conçus pour effectuer des tâches nécessitant une intelligence humaine, comme l'apprentissage et la résolution de problèmes.
Logiciel malveillant	Un programme informatique conçu pour causer des dommages, collecter des informations ou compromettre la sécurité d'un système.
Man in the middle	Une attaque où un attaquant intercepte et éventuellement modifie les communications entre deux parties sans leur consentement.

8. Glossaire

Mot	Définition
Métadonnées	Des données décrivant d'autres données, fournissant des informations contextuelles sur l'origine, le contenu, le format, etc.
Mot de passe	Une séquence de caractères utilisée pour vérifier l'identité d'un utilisateur et accéder à un compte ou un système.
Mot de passe complexe	Un mot de passe avec une combinaison de lettres, chiffres et caractères spéciaux, renforçant sa sécurité.
Navigation privée	Un mode de navigation sur Internet qui ne stocke pas l'historique de navigation ni les cookies.

8. Glossaire

Mot	Définition
Pirater	Accéder à un système informatique de manière non autorisée.
Phishing	Une technique d'escroquerie en ligne visant à tromper les gens pour obtenir leurs informations personnelles, comme les mots de passe.
Profil (réseau social)	Une page personnelle ou professionnelle créée par un utilisateur sur une plateforme de médias sociaux.
Pseudonyme	Un nom fictif utilisé pour protéger l'identité réelle d'une personne en ligne.

8. Glossaire

Mot	Définition
Rançongiciel / Ransomware	Un type de logiciel malveillant qui chiffre les données d'un utilisateur et demande une rançon en échange de leur libération.
Risque	La probabilité de subir des dommages ou des pertes liés à des menaces informatiques.
Sauvegarde	Une copie de données importantes effectuée pour prévenir la perte en cas de défaillance du système.
Source	L'origine ou la provenance d'une information, d'un fichier ou d'un programme.

8. Glossaire

Mot	Définition
Rançongiciel / Ransomware	Uniform Resource Locator, l'adresse spécifique qui identifie une ressource sur Internet.
Usurper l'identité	Faire semblant d'être quelqu'un d'autre en ligne, généralement dans le but de tromper ou de nuire.
Virus	Un programme informatique malveillant capable de se reproduire et d'infecter d'autres programmes ou fichiers.
VPN	Virtual Private Network, un réseau privé virtuel permettant de sécuriser et d'anonymiser la connexion à Internet.

8. Glossaire

Mot	Définition
Wifi public	Un réseau sans fil accessible au public, souvent disponible dans des lieux publics tels que les cafés, les aéroports, etc.