FRESQUE DES CYBERCITOYENS

GUIDE PEDAGOGIQUE

2025 I By aDvens
for People and Planet

Comment utiliser ce guide ?

Ce guide a été construit pour vous accompagner dans l'utilisation du jeu pédagogique « Fresque des cybercitoyens », tout au long de l'année scolaire.

Il contient toutes les informations nécessaires à l'animation. **Nous vous conseillons cependant de suivre une formation avec un référent académique de votre bassin ou alternativement en e-learning sur la plateforme magistère ou sur le site de la Fresque.**

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

1. INTRODUCTION

1.a Présentation générale du jeu

DEMAIN SPÉCIALISTE CYBER

2025 ANNÉE EUROPÉENNE DE L'ÉDUCATION À LA CITOYENNETÉ NUMÉRIQUE

Le jeu "Fresque des cybercitoyens" 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 le fonds de dotation 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.

Le jeu est actuellement déployé dans 24 académies de France. Il a obtenu une reconnaissance comme ressource pédagogique par le Conseil de l'Europe dans le cadre de l'Année européenne de l'éducation à la citoyenneté numérique et fait partie du catalogue « Demain spécialiste Cyber »

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 => **Quiz**
- La seconde permet la mise en pratique de celles-ci face à des scénarios d'attaque => **Cyberattaque**

Les thématiques abordées sont :

 Le Cyberharcèlement

 La Désinformation

 La Cyberdéfense

 Les Cyberattaques

 Les Mots de passe

 La Vie privée

1.a Présentation générale du jeu

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.

Il aborde ainsi de nombreuses compétences du Cadre de référence des compétences numériques (CRCN), certifiable avec PIX (v. slide 13), et s'insère dans la stratégie d'intégration des enjeux de cybersécurité dans les programmes scolaire.

1.b Objectifs pédagogiques

Les objectifs pédagogiques du jeu Fresque des cybercitoyens et citoyennes peuvent être classés en trois catégories principales : connaissances, 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 : cybercriminel, cyberprédateur ou harceleur ou influenceur.

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.

1.b Objectifs pédagogiques

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

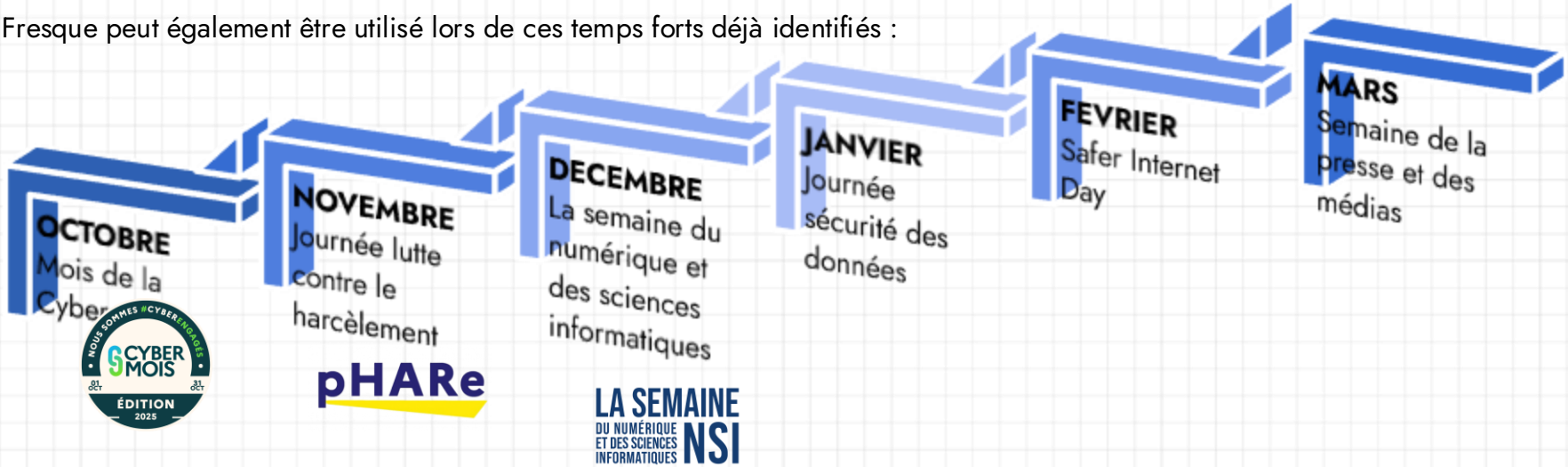
Les joueurs tireront parti des connaissances et des perspectives diverses de leurs coéquipiers pour enrichir leur compréhension globale de la citoyenneté numérique.

1.c Temps forts de l'année scolaire

Le jeu est conçu pour être utilisé plusieurs fois et tout au long de l'année, grâce à la sélection de thématiques et de niveaux de difficultés.

En 2025, aura lieu un défi collectif de sensibilisation cyber en classe du cycle 3 à la terminale autour de jeux, ainsi qu'un grand concours organisé par l'équipe de la Fresque à l'occasion du Cybermois. Plus d'infos comment déclarer votre participation sur la slide conclure un atelier.

La Fresque peut également être utilisé lors de ces temps forts déjà identifiés :



1.d Cadre de référence des compétences numériques (CRCN) et Parcours PIX

La Fresque des Cybercitoyens a été conçue avec l'académie de Paris et révisée depuis sont premier déploiement en 2023 grâce au soutien et retours de nombreux enseignants et aussi experts en cybersécurité ou désinformation. Ainsi, elle s'inscrit au plus proche des usages et réalités des jeunes, mais aussi du programme scolaire, niveaux de compétences attendues et évaluation de celles-ci notamment via PIX.

Une matrice de correspondance est disponible dans les ressources complémentaires au jeu (dans le parcours magistère et sur le site de la Fresque), afin d'identifier les parcours, compétences et acquis à cibler qui peuvent être introduits et révisés grâce au jeu. Voir également exemple d'une séquence pédagogique « PIX »

Attestation de sensibilisation au numérique 6e (obligatoire)			Protection et Sécurité	Initiation aux compétences numériques				
						FRESQUE CYBERCITOYENS		
Temporalité	PARCOURS PIX - 6èn	Domaine de compétences	Compétences	Sujets	Acquis	Thématiques QUIZ	Acquis abordé	Scénario de C
Trimestre 1	Protection et sécurité	2. Communication et collaboration	2.4 S'insérer dans le monde numérique	Présence en ligne	Identité numérique + choix identifiant	Vie Privée	Pseudonyme	Tous
Trimestre 1	Protection et sécurité	4. Protection et sécurité	4.1 Sécuriser l'environnement numérique	Comportement de prudence	Connaître les recommandations pour le choix d'un mot de passe robuste	Mots de passe	Toutes les cartes Quiz de la thématique	Cybercriminel
Trimestre 1	Protection et sécurité	4. Protection et sécurité	4.1 Sécuriser l'environnement numérique	Comportement de prudence	Identifier des situations d'arnaque par manipulation psychologique (hameçonnage, usurpation d'identité, faux support informatique)	Cyberattaque	Phishing, Usurpation d'identité	Cybercriminel

1.d Education à la citoyenneté numérique

La Fresque des Cybercitoyens est labélisée comme ressource pédagogique par **le Conseil de l'Europe** dans le cadre de l'**année européenne de l'éducation à la citoyenneté numérique**

Un cadre de référence qui définit 10 thèmes et des compétences rattachées

1. Accès et inclusion
2. Apprentissage et créativité
3. Éducation aux médias et à l'information
4. Éthique et empathie
5. Santé et bien-être
6. Présence et communication en ligne
7. Participation active
8. Droits et responsabilités
9. Vie privée et sécurité
10. Sensibilisation des consommateurs

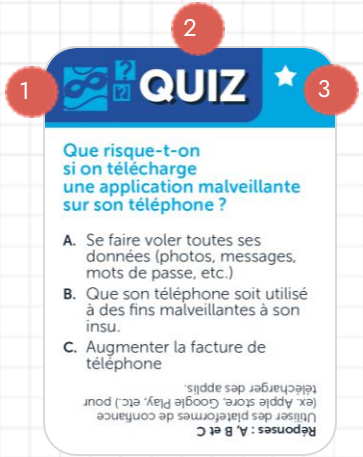
2025 ANNÉE EUROPÉENNE DE L'ÉDUCATION À LA CITOYENNETÉ NUMÉRIQUE

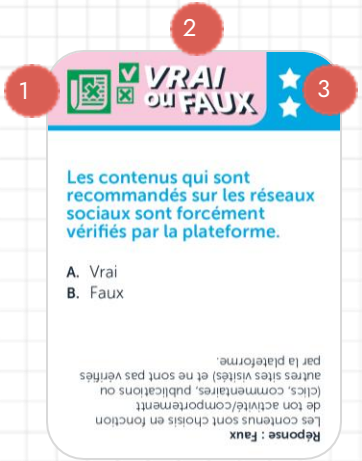
Plus d'infos et ressources à destination notamment des enseignants et parents sur le site du Conseil de l'Europe

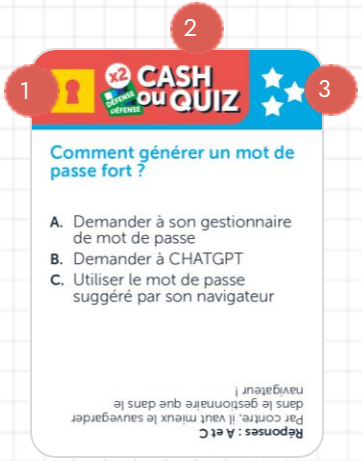
Dans la **matrice de correspondance** disponible dans les ressources complémentaires au jeu, sont répertoriés les liens entre le jeu et les compétences rattachées à l'éducation à la citoyenneté numérique (DCE Planner).

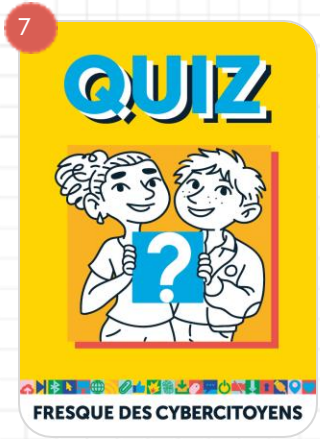
2. CONTENU DU JEU

2.a 94 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 complet des cartes disponible sur le site fresquedescybercitoyens.fr/ressources

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

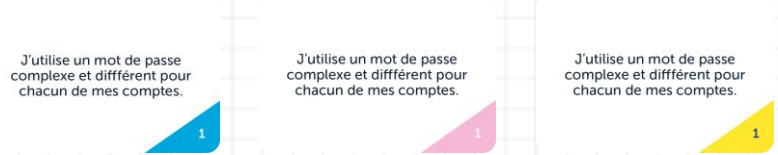
Les cartes « Défense » et les cartes « Cyberattaque » sont composées de trois lots de cartes identiques :

- 15 cartes « Défense » et 20 cartes « Cyberattaque » pour l'équipe bleue / rose / jaune

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

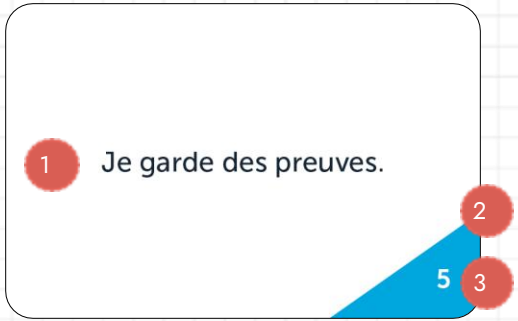
Par ailleurs, ces cartes présentent un numéro inscrit en bas à droit de la carte.

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.



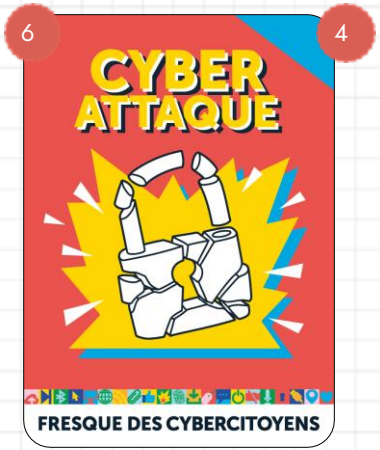
Exemple de cartes « Défense »

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



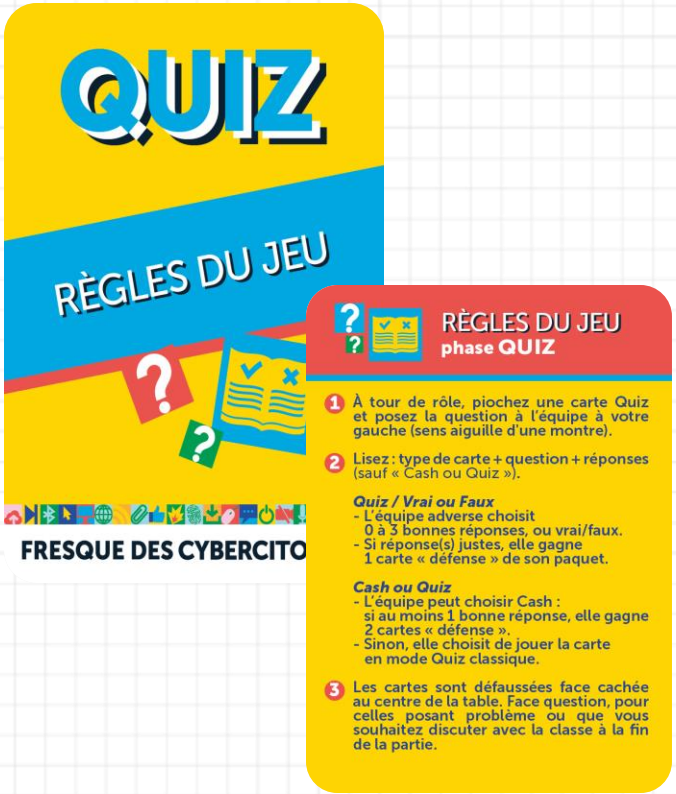
1. Intitulé de la carte « Défense »
2. Couleur de l’équipe : rose, jaune ou bleu
3. Numéro de la carte
4. Dos de la carte : identique pour toutes les cartes « Défense », modulo la couleur de l’équipe
5. Indication de la valeur de la carte = 1 point

2.d 20 cartes “Cyberattaque” par équipe (60 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

2.e Cartes Règles du jeu

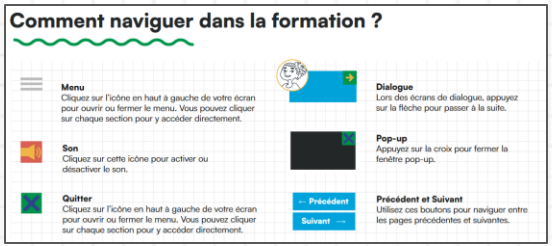


2.d Ressources autour du jeu

Les supports de formation

- Un MOOC de 30 min disponible sur la plateforme Magistère pour former les animateurs

Parcours : Animer le jeu pédagogique La Fresque des cybercitoyens



Magistère

Les guides pour l'animateur

Lien dans le parcours magistère ou sur notre site

- Un **tuto express** reprenant les éléments essentiels pour animer une Fresque (à imprimer)
- Un **guide complet des cartes**, avec des explications et ressources complémentaires par thématique. Pratique pour projeter en cas de questions des élèves.
- Un **support d'explication** des règles qui peut être projeté en classe
- Un **lexique de la cybersécurité**
- Une **matrice de correspondance avec les parcours pix et le référentiel européen DCE**
- Un **guide pédagogique** (celui-ci)

Le site web

Dans l'espace animateur, il y a :

- Une FAQ alimentée au fur et à mesure des animations et de vos feedbacks
- Toutes les versions des guides
- Questionnaire déclaration atelier
- Des extensions, des jeux concours, et d'autres surprises au fur et à mesure.

https://www.fresquedescybercitoyens.fr

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.

3.a Les règles du jeu

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

- Répartissez les joueurs 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 environ 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. Les cartes difficiles ou qui posent problème peuvent être laissées face ouverte pour en discuter à la fin de la séance.

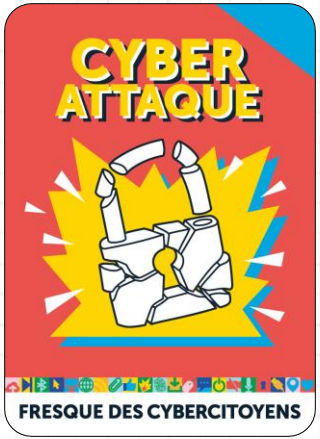
>> L'équipe qui pose la question doit lire le type de carte, la question et les propositions de réponse (sauf pour les cartes « Cash ou Quiz »). Après concertation, l'équipe adverse répond à la question posée en choisissant aucune, une, deux ou trois bonnes réponses. L'équipe qui a posé la question doit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



- Invitez ensuite chaque équipe à disposer toutes les cartes « Défense » devant elles (15 cartes en tout), même celles qui n'ont pas été gagnées lors de la précédente phase.
- Disposez une séquence d'attaque identique devant chacune des équipes (vous pouvez vous aider des exemples de Scénarios d'attaque). Pour cette partie, les cartes ne sont qu'un squelette du scénario ; il est essentiel, pour la bonne compréhension, de l'insérer dans un contexte, des faits récents ou qui parlent plus personnellement à la classe.
- 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 les pages dédiées.
- Additionnez éventuellement les points des deux phases de jeu :

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

2.b Préparer un atelier

Préparer 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, les temps forts de l'année scolaire (cybermois, journée de lutte contre le harcèlement,...) ou programme scolaire (certifications pix, compétences à aquérir en cybersécurité, heures dédiées audispositif phare).

3. Vérifiez que vous disposez du matériel nécessaire :
   - Jeu de la fresque (1 boite de jeu pour 12 élèves au maximum) ;
   - Le présent « Tuto express » et la « Présentation des règles en classe » pour projection
   - Un papier et un stylo pour faire le compte des points, alternativement au tableau ;
   - En option : Un chrono (montre, sablier, téléphone) pour chronométrer et dynamiser le jeu.

2.b Déroulement d'une session

Introduction [-> 10 min]

- Constitution des équipes et choix du nom
- Présentation de l'atelier (objectifs, thématique abordées, phases de jeux, etc...)

Explication des règles [-> 5 min]

- Projeter les règles du jeu au tableau avec la présentation disponible dans les ressources Explication des règles aux participants

Phase de jeu [20 – 35 min]

- Quiz
- Cyberattaque
- Les deux

Fin de l'activité [10 – 15 min]

- Annonce de l'équipe vainqueur
- Tour de table pour avoir des retours sur l'atelier
- Remplir le questionnaire

Après l'atelier [5min]

- Tri des cartes et rangement du jeu
- Rangement de l'espace de jeu

**Des cartes par phase (Quiz/Cyberattaque) récapitulant les règles du jeu sont également disponibles dans la boite.*

2.b. Conclure un atelier

Mise en commun après la phase Quiz :

- Aborder les éventuelles cartes qui ont fait débat ou posent problèmes (identifiables face ouverte à côté de la défausse)
- Utiliser le guide complet des cartes pour s'appuyer sur les informations complémentaires

Correction des scénarios d'attaque :

- Faire une correction individuelle par équipe ou en commun avec la classe
- Les cartes « Défense » choisies sont présentées de manière argumentée en quoi elles permettent de prévenir ou réagir face au scénario
- Possibilité de projeter les cartes du scénario et les cartes « défense »

Conclure l'atelier :

- Demander le tri et le rangement des cartes par couleur, c'est-à-dire par équipe ;
- Faire l'annonce de l'équipe vainqueur et la féliciter ;
- Faire un tour de table pour recueillir les impressions (exemple : Chaque participant dit une notion qu'il a apprise, une notion qu'il connaissait déjà, un élément du jeu qu'il a aimé et un élément qu'il a moins aimé.)
- Remplir le questionnaire

2.b. Conclure un atelier

- **Déclarer la session de jeu**

Après chaque atelier, l'animateur est invité à scanner le QR Code qui se trouve sur le dos de la boite de jeu ou ci-contre pour déclarer la session. Cela est essentiel pour que nous puissions continuer d'améliorer le jeu. Merci !

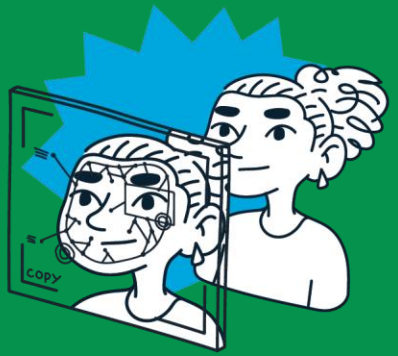
• Challenge Cybermois : Participez à notre jeu concours !

Du 1er octobre au 14 novembre se tiendra un grand challenge inter-collèges ! Déclarez le plus de sessions de jeu pour avoir une chance de gagner de nombreuses récompenses. Vous pouvez choisir le questionnaire spécifique « DECLARATION FRESQUE CYBERMOIS » en scannant le QR code ci-contre.

• Défi Cyber de la DGESCO dans le cadre de « Demain Spécialiste Cyber »

Durant le cybermois et tout au long de l'année, la DGESCO propose un défi collectif de sensibilisation cyber en classe du cycle 3 à la terminale tout au long de l'année autour de jeux de sensibilisation avec le kit CyberEnJeux ou des ressources de sensibilisation au choix (L'Odysée du numérique, la Fresque des cybercitoyens...). Participez et répondez au questionnaire ici : Actions_cyber_jeunes.

DEMAIN SPÉCIALISTE CYBER



4. SÉQUENCES PÉDAGOGIQUES

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 94 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 abordées 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) et concernant les scénarios sur le nombre de cartes « Défense » qui s'appliquent (plus il y a de bonnes pratiques, plus le niveau est facile).

4. Construire une séquence pédagogique « PIX »

Exemple d'une séquence pédagogique « PIX »

Classe	Parcours PIX	Thématiques abordées	Sélection de 30 cartes Quiz	Scénario d'attaque
6e	**Attestation de sensibilisation: Protection & Sécurité**	Cyberharcèlement & mots de passe	Cartes de niveau 1 ou 2 sur les thématiques	Attaquant: cyberharceleur, scénario 3 ou 4
6e	**Attestation de sensibilisation: Initiation aux compétences numériques**	Désinformation	Cartes de niveau 1 ou 2 sur la thématique (notamment wikipedia, vérification information)	Attaquant: influenceur, scénario 1 ou 2
3e	**Cyberattaque & mot de passe**	Cyberattaque & mots de passe	Cartes de niveau 3 sur les thématiques abordées	

4. Construire une séquence pédagogique lutte contre le harcèlement

Exemple d'une séquence pédagogique, journée lutte contre le harcèlement/dispositif phare

Classe	Thématiques abordées	Sélection de 30 cartes Quiz	Scénario d'attaque
6e	Cyberharcèlement & vie privée	Sélection de cartes de niveau 1 et éventuellement 2	Attaquant: cyberharceleur, scénario n° 1 et 2
6e	Cyberharcèlement & mots de passe	Cyberharcèlement: Cartes de niveau 1 & 2 Mots de passe: cartes de niveau 1	Attaquant: cyberharceleur, scénario n° 3 et nr4
5e	Cyberharcèlement & Désinformation	Cyberharcèlement : cartes de niveau 1 ou 2 Désinformation: cartes concernant la e-réputation, vérification des sources, origine des images	Attaquant: cyberharceleur ou éventuellement cyberprédateur

4. Construire une séquence pédagogique « EMI »

Exemple d'une séquence pédagogique EMI, Semaine de la presse et des médias

Classe	Thématiques abordées	Sélection de 30 cartes Quiz	Scénario d'attaque
6e-3ème	Désinformation & Cyberattaque	Désinformation : sélection avec niveau de difficulté adapté aux participants Cyberattaque: ingénierie sociale, attaque réseaux sociaux, typosquatting	Attaquant: cybercriminel, scénario n° 4 ou influenceur 2 et 4
6e-3ème	Désinformation & vie privée	Sélection avec niveau de difficulté adapté aux participants	Attaquant: influenceur scénatio n°1 ou à inventer avec cyberharceleur+fake news

5.
ANIMER UNE FRESQUE

5.a 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.

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 lexique ou du guide complet des cartes;
- 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 informations 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 boite 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.dou

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 et la carte récapitulative des règles du jeu :
   - Cartes dans le même ordre pour chaque table et avec le bon équilibre et enchainement pour donner à chaque équipe la chance de répondre à des cartes Cash ou Quiz et Vrai ou Faux.
   - 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.

5.d Pendant l'atelier

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 le cas échéant).
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, même celles qui n'ont pas été gagnées durant la phase « Quiz » (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 Fin de 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.

Ce questionnaire ne prend que **5 minutes** ; il contient des questions pour les élèves (auquel l'animateur répondra pour le collectif) et pour les animateurs.

Pour que ce jeu **continue d'exister et afin de nous aider à l'améliorer**, il est essentiel que vous nous fassiez des retours sur votre expérience et sur celle des participants. 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.

Par exemple, en 2025 nous avons modifié les cartes en intégrant plus d'IA, de « Cash ou Quiz » et un de nouveaux scénarios d'attaque suite aux retours que nous avons eu via le questionnaire.

6. SCÉNARIOS CYBERATTAQUE

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 ».

A noter : certains scénarios possèdent plus de cinq bonnes réponses. Ces scénarios sont ainsi plus facile, car ils laissent plus de possibilités aux élèves d'obtenir des points.

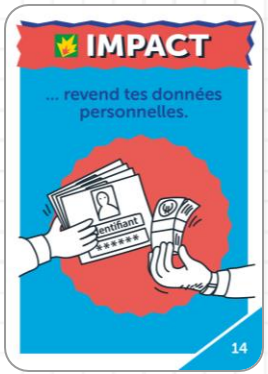
6.1. Cybercriminel.le

Numéro	Scénario	Cartes « Cyberattaque »	Cartes « Défense »
n° 1	Une cybercriminelle 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 -> 7 -> 14	1 - 2 - 7 - 8 - 15
n° 2	Un cybercriminel 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 -> 7 -> 14	1 - 7 - 8 - 14 - 15
n°3	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 -> 7 -> 17	1 - 5 - 8 - 14 - 15

6.1. Cybercriminel.le

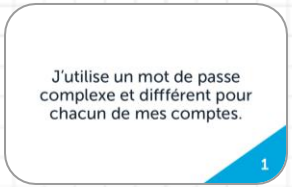
Scénario Cybercriminel.le n°1 : 1 -> 9 -> 7 -> 14

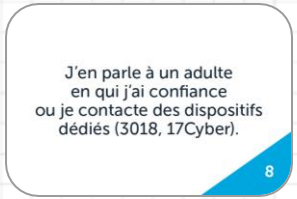
Une cybercriminelle propage un virus sur ton téléphone ou ton ordinateur qui lui permet d'avoir accès à tes comptes et elle revend tes données sur le dark web.



Contexte : Selon une étude de 2023, près de 50 % des attaques par malware ont pour objectif le vol de données personnelles.

Défense : 1 - 2 - 7 - 8 - 15





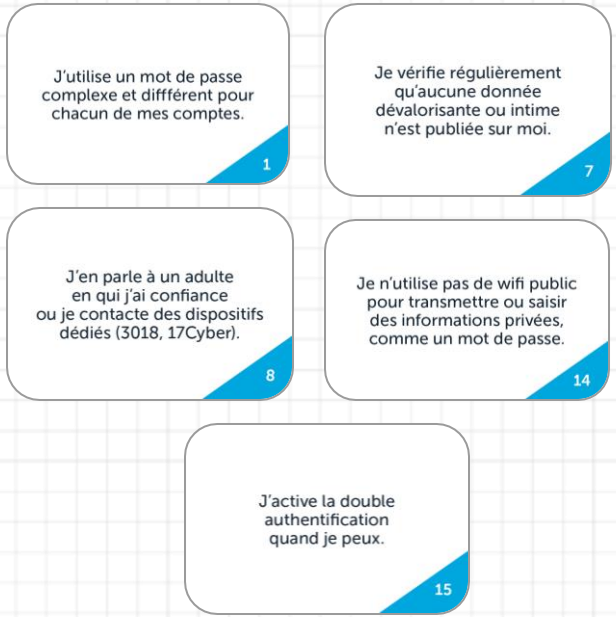
6.1. Cybercriminel.le

Scénario Cybercriminel.le n° 2 : 1 -> 10 -> 7 -> 14

Un cybercriminel 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.

Contexte : Par exemple, un attaquant Man-in-the-Middle pourrait intercepter les communications sur un réseau Wi-Fi public non sécurisé. En surveillant le trafic, il peut facilement capturer des informations sensibles comme des mots de passe et les revendre sur le dark web.

Défense : 1 - 7 - 8 - 14 - 15



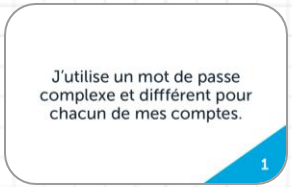
6.1. Cybercriminel.le

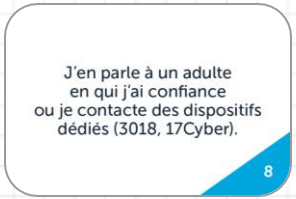
Scénario Cybercriminel.le n° 3 : 1 -> 10 -> 7 -> 17

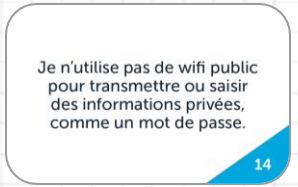
Un cybercriminel pirate un réseau wifi public. Comme il voit tout ce qui transite sur le réseau, il capte ton mot de passe et vole l'accès à tes comptes. Alors, il décide de de te faire chanter : par exemple, il te demande de l'argent pour te rendre tes accès à tes comptes sur les réseaux sociaux.

Contexte : En 2021, environ 20 % des attaques par piratage ont été suivies de tentatives de chantage, souvent via l'exploitation de données volées.

Défense : 1 - 5 - 8 - 14 - 15







6.2.Cybercriminel.le

Numéro	Scénario	Cartes « Cyberattaque »	Cartes « Défense »
n° 4	Un cybercriminel se renseigne sur toi sur internet. Comme il voit tout ce que tu as publié, il devine ton mot de passe faible. Avec celui-ci, il récupère tes accès à tes comptes et usurpe ton identité (= il se fait passer pour toi).	1 -> 6 -> 7 -> 15	1 - 7 - 8 - 9 - 10 - 15
n° 5	Une cybercriminelle 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 -> 16	2 - 4 - 5 - 8 - 12
n°6	Une cybercriminelle 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 -> 14	1 - 2 - 4 - 7 - 8 - 15

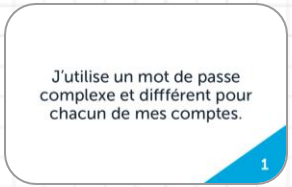
6..1 Cybercriminel.le

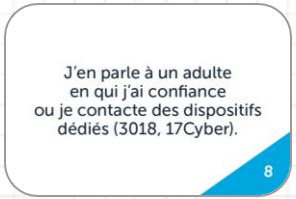
Scénario Cybercriminel.le n° 4 : 1 -> 6 -> 7 -> 15

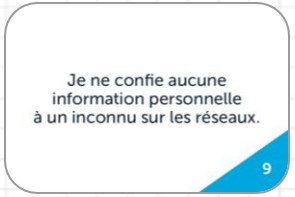
Un cybercriminel se renseigne sur toi sur internet. Comme il voit tout ce que tu as publié, il devine ton mot de passe faible. Avec celui-ci, il récupère tes accès à tes comptes et usurpe ton identité (= il se fait passer pour toi).

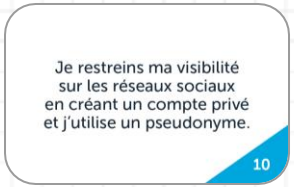
Contexte : Selon une étude, 30 % des personnes utilisent des mots de passe basés sur des informations personnelles, rendant leurs comptes vulnérables aux attaques.

Défense : 1 – 7 – 8 – 9 – 10 - 15









6..1 Cybercriminel.le

Scénario Cybercriminel.le n° 5 : 1 -> 5 -> 9 -> 16

Une cybercriminelle 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.

Contexte : En 2021, environ 20 % des attaques par piratage ont été suivies de tentatives de chantage, souvent via l'exploitation de données volées.

Défense : 2 – 4 – 5 – 8 – 12

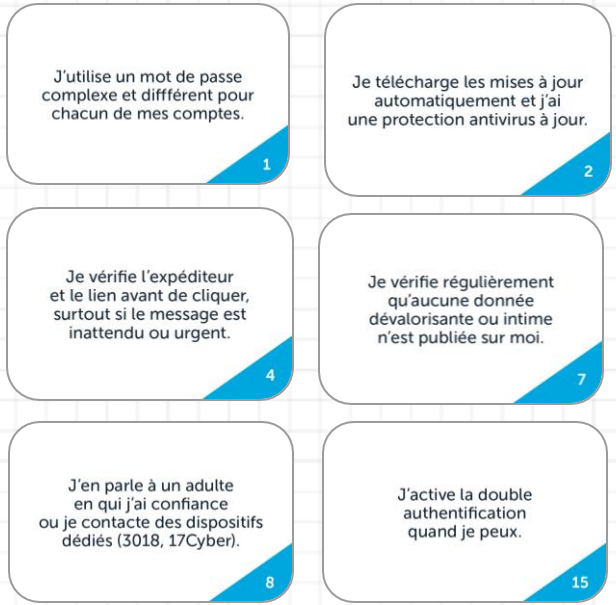
6..1 Cybercriminel.le

Scénario Cybercriminel.le n° 6 : 1 -> 5 ->9 -> 14

Une cybercriminelle 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.

Contexte : Selon une étude de 2023, près de 50 % des attaques par malware ont pour objectif le vol de données personnelles.

Défense : 1 – 2 – 4 – 7 – 8 – 15



6.2. Cyberprédateur.trice ou Cyberharceleur.se

Comme vous pourrez le constater, les attaques des cyberharceleurs et cyberprédateurs sont quasiment similaires. Cependant, les deux ont des objectifs bien différents :

Cyberharceleurs : Ce sont des personnes qui utilisent Internet pour harceler, insulter ou menacer d'autres personnes. Ils peuvent envoyer des messages méchants ou publier des informations privées pour faire du mal, de manière répétée.

Cyberprédateurs : Ce sont des personnes qui cherchent à manipuler et exploiter d'autres en ligne, dans un but malveillant et majoritairement à caractère sexuel. Ils sont dans une logique de construction d'une relation de confiance, pour obtenir des informations personnelles ou des photos intimes.

Précision à faire avec les élèves : La différence principale réside ainsi dans les intentions et la nature de la relation entre l'attaquant et la victime. Le cyberharceleur veut nuire ou blesser la victime par des actes répétés, tandis que le cyberprédateur essaie d'établir une relation intime et privilégiée afin d'obtenir quelque chose d'intime et manipuler la victime. Le prédateur peut devenir harceleur.

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

6.2. Cyberprédateur.trice

Numéro	Scénario	Cartes « Cyberattaque »	Cartes « Défense »
n° 1	Un cyberprédateur se renseigne sur toi, par exemple sur les réseaux sociaux, et te harcèle par messages ou à l'école.	2 -> 8 -> 18	5 - 6 - 7 - 8 - 10 - 13
n° 2	Un cyberprédateur se renseigne sur toi, t'envoie des messages dégradants et te menace.	2 -> 6 -> 8 -> 17	5 - 8 - 9 - 10 - 13
n°3	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 -> 15	1 - 7 - 8 - 9 - 10 - 13 - 15

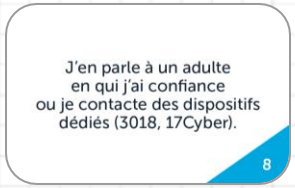
6. 2. Scénarios Cyberprédateur.trice

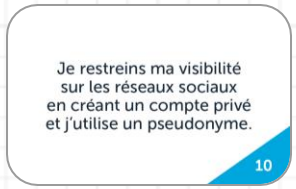
Scénario Cyberprédateur.trice n° 1 : 2 -> 6 -> 18

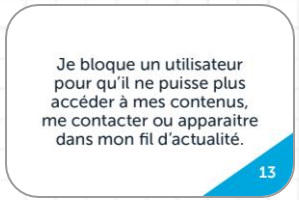
Un cyberprédateur se renseigne sur toi, par exemple sur les réseaux sociaux, et te harcèle par messages ou à l'école.

Contexte : 1 enfant sur 5 aurait déjà reçu des propositions en ligne dans le monde, selon France TV.

Défense : 5 - 6 - 7 - 8 - 10 - 13







6. 2. Scénarios Cyberprédateur.trice

Scénario Cyberprédateur.trice n°2 : 2 -> 6 -> 8 -> 17

Un cyberprédateur se renseigne sur toi, t'envoie des messages dégradants et te menace.

Contexte : 750.000 cyberprédateurs sont en permanence en ligne à travers le monde, selon France TV.

Défense : 5 - 8 - 9 - 10 - 13

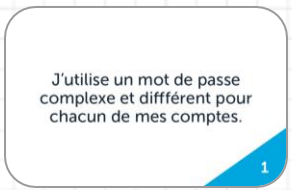
6. 2. Scénarios Cyberprédateur.trice

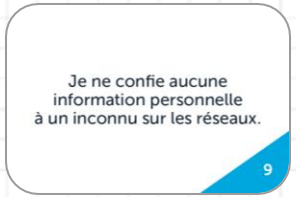
Scénario Cyberprédateur.trice n° 3 : 2 -> 6 -> 7 -> 15

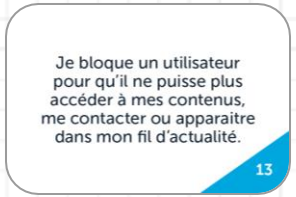
Une cyberprédatrice se renseigne sur toi et avec les informations qu'elle a obtenues, elle trouve ton mot de passe et usurpe ton identité. Elle contacte tes amis et tente d'obtenir des photos intimes.

Contexte : 750.000 cyberprédateurs sont en permanence en ligne à travers le monde, selon France TV.

Défense : 1 - 7 - 8 - 9 - 10 - 13 - 15







4.b Cyberprédateur.trice

Numéro	Scénario	Cartes « Cyberattaque »	Cartes « Défense »
n° 4	Un cyberprédateur se renseigne sur toi, par exemple sur les réseaux sociaux, utilise les informations pour te manipuler psychologiquement et t'incite à partager des contenus privés ou adopter des comportements risqués.	2 -> 6 -> 11 -> 19	5 - 6 - 7 - 8 - 9 - 10 - 13
n° 5	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 -> 13 -> 17	5 - 6 - 7 - 8 - 9 - 10
n°6	Un cyberprédateur crée des deepfakes de lui avec de l'IA pour se présenter comme quelqu'un d'autre. Il te manipule psychologiquement pour t'inciter à partager d'autres photos intimes de toi.	2 -> 13 -> 11 -> 19	5 - 7 - 8 - 9 - 10 - 13

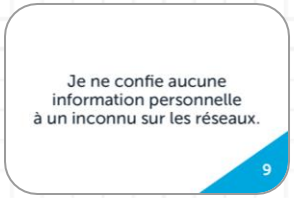
6. 2. Scénarios Cyberprédateur.trice

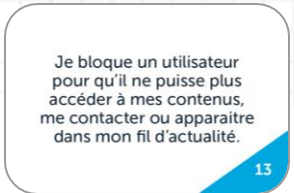
Scénario Cyberprédateur.trice n° 4 : 2 -> 6 -> 11 -> 19

Un cyberprédateur se renseigne sur toi, par exemple sur les réseaux sociaux, utilise les informations pour te manipuler psychologiquement et t'incite à partager des contenus privés ou adopter des comportements risqués.

Contexte : 750.000 cyberprédateurs sont en permanence en ligne à travers le monde, selon France TV.

Défense : 5 - 6 - 7 - 8 - 9 - 10 - 13



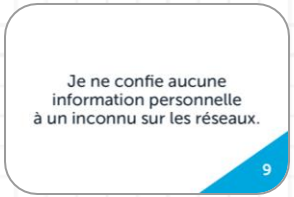


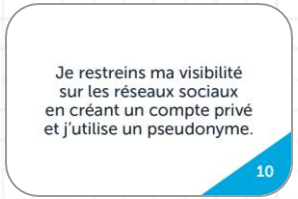
6. 2. Scénarios Cyberprédateur.trice

Scénario Cyberprédateur.trice n°5 : 2 -> 6 -> 13 -> 17

Une cyberprédatrice se renseigne sur toi et avec les informations ou images qu'elle a obtenues, elle crée des deepfakes de toi avec de l'IA pour te faire du chantage.

Défense : 5 - 6 - 7 - 8 - 9 - 10





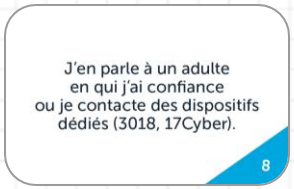
6. 2. Scénarios Cyberprédateur.trice

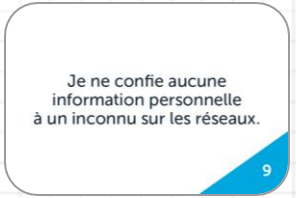
Scénario Cyberprédateur.trice n° 6 : 2 -> 13 -> 11 -> 19

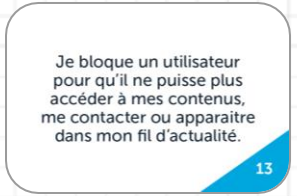
Un cyberprédateur crée des deepfakes de lui avec de l'IA pour se présenter comme quelqu'un d'autre. Il te manipule psychologiquement pour t'inciter à partager des photos intimes de toi.

Contexte : 750.000 cyberprédateurs sont en permanence en ligne à travers le monde, selon France TV.

Défense : 5 - 7 - 8 - 9 - 10 - 13







6.3. Harceleur.se

Numéro	Scénario	Cartes « Cyberattaque »	Cartes « Défense »
n° 1	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 -> 17	5 - 7 - 8 - 9 - 10 - 13
n° 2	Une cyberharceleuse te trouve sur les réseaux sociaux et t'envoie des messages injurieux	3 -> 8 -> 18	5 - 6 - 7 - 8 - 13
n°3	Un cyberharceleur devine ton mot de passe et se fait passer pour toi sur les réseaux sociaux ou sur l'ENT.	3 -> 7 -> 15	1 - 5 - 7 - 8 - 15
n°4	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 -> 17	1 - 5 - 7 - 8 - 9 - 10 - 15

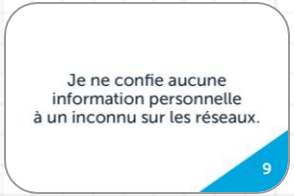
6. 3. Scénarios Harceleur.se

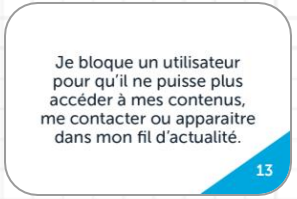
Scénario Harceleur.se n° 1 : 3 -> 6 -> 17

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.

Contexte : 1 enfant sur 4 était victime de cyberharcèlement en 2023.

Défense : 5 - 7 - 8 - 9 - 10 - 13





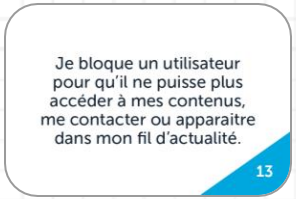
6. 3. Scénarios Harceleur.se

Scénario Harceleur.se n° 2 : 3 -> 8 -> 17

Une cyberharceleuse te trouve sur les réseaux sociaux et t'envoie des messages injurieux.

Contexte : 1 enfant sur 4 était victime de cyberharcèlement en 2023.

Défense : 5 - 6 - 7 - 8 - 13



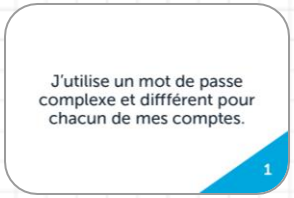
6. 3. Scénarios Harceleur.se

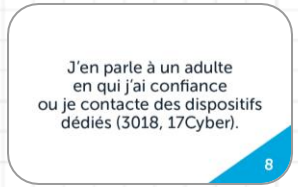
Scénario Harceleur.se n° 3 : 3 -> 7 -> 15

Un cyberharceleur devine ton mot de passe et se fait passer pour toi sur les réseaux sociaux ou sur l'ENT.

Contexte : 1 enfant sur 4 était victime de cyberharcèlement en 2023.

Défense : 1 - 5 - 7 - 8 - 15



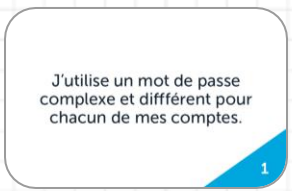


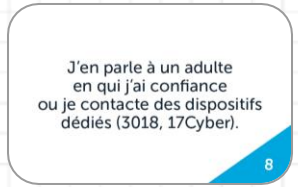
Scénario Harceleur.se n° 4 : 3 -> 6 -> 7 -> 17

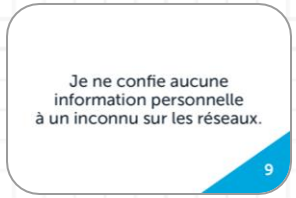
Une cyberharceleuse se renseigne sur toi, trouve ton mot de passe et te fait du chantage ou te menace de diffuser des infos persos sur toi.

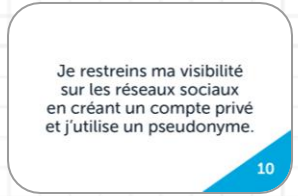
Contexte : 1 enfant sur 4 était victime de cyberharcèlement en 2023.

Défense : 1 - 5 - 7 - 8 - 9 - 10 - 15









4.d Influenceur.se

Numéro	Scénario	Cartes « Cyberattaque »	Cartes « Défense »
n° 1	Un influenceur propage de fausses informations pour te manipuler – par exemple, que les femmes ne sont pas biologiquement faites pour travailler. Cela t'amène à changer d'opinion et de comportement, par exemple à présenter des comportements sexistes et misogynes.	4 -> 12 -> 11 -> 20	3 - 6 - 8 - 11 - 13
n° 2	Une influenceuse crée des deepfakes avec de l'IA – par exemple une vidéo d'un OVNI – et t'amène à croire à des théories du complot.	4 -> 13 -> 20	3 - 6 - 8 - 11 - 13
n°3	Un influenceur crée un deepfake par l'IA d'une célébrité adoptant un comportement risqué en incitant à faire de même. Cela t'amène à te mettre en danger.	4 -> 13 -> 11 -> 19	3 - 6 - 8 - 11 - 13
n°4	Une influenceuse propage de fausses informations sur un évènement dans ta ville. Cela t'incite à vouloir te rendre sur les lieux et te mettre en danger.	4 -> 12 -> 19	3 - 6 - 8 - 11 - 13

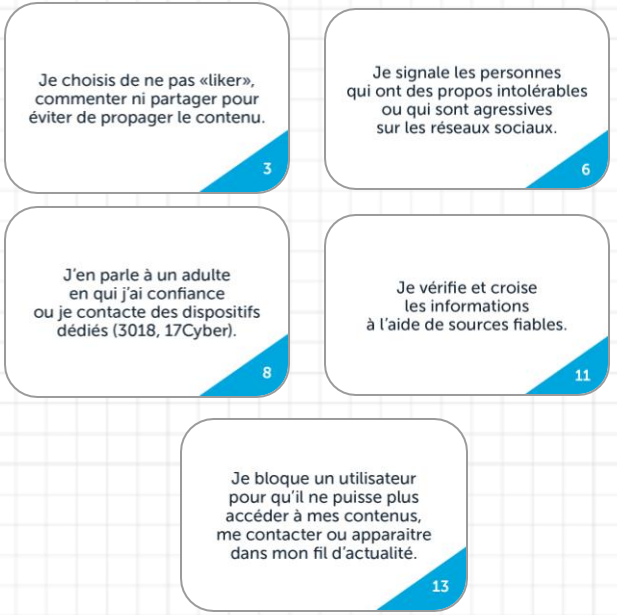
6.4 . Scénarios Influenceur.se

Scénario Influenceur.se n° 1 : 4 -> 12 -> 11 ->20

Un influenceur propage de fausses informations pour te manipuler – par exemple, que les femmes ne sont pas biologiquement faites pour travailler. Cela t'amène à changer d'opinion et de comportement, par exemple à présenter des comportements sexistes et misogynes.

Contexte : Selon le Baromètre 2023 du CLEMI & Junior Connect' (Ipsos, 2023-2024), 29% des jeunes ne se sentent pas capables de différencier une vraie et une fausse information.

Défense : 3 - 6 - 8 - 11 - 13



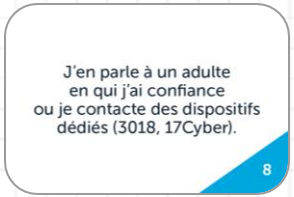
6.4 . Scénarios Influenceur.se

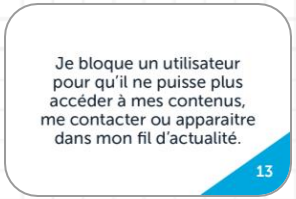
Scénario Influenceur.se 2 : 4 -> 13 -> 20

Une influenceuse crée des deepfakes avec de l'IA – par exemple une vidéo d'un OVNI – et t'amène à croire à des théories du complot.

Contexte : Selon le Baromètre 2023 du CLEMI & Junior Connect' (Ipsos, 2023-2024), 44% des jeunes déclarent avoir déjà cru à une info qui s'est révélée fausse.

Défense : 3 - 6 - 8 - 11 - 13





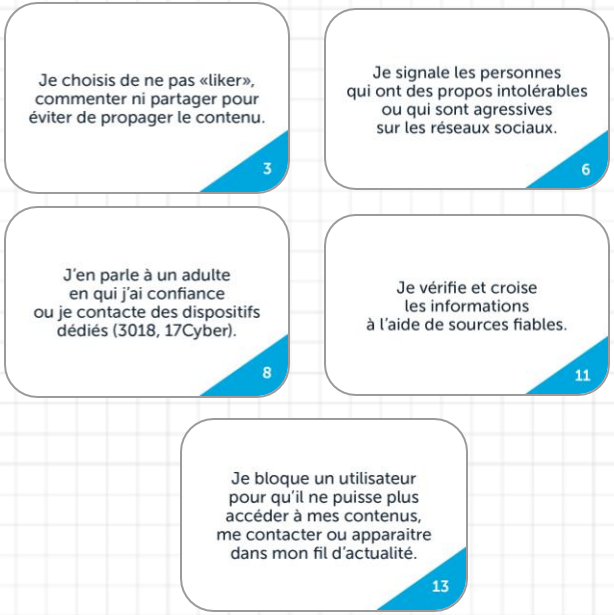
6.4 . Scénarios Influenceur.se

Scénario Influenceur.se n° 3 : 4 -> 13 -> 11 -> 19

Un influenceur crée un deepfake par l'IA d'une célébrité adoptant un comportement risqué en incitant à faire de même. Cela t'amène à te mettre en danger.

Contexte : Selon l'étude "Jeunes, médias, réseaux sociaux et fake news" (Médiamétrie, 2023), près de 57% des adolescents français déclarent voir "régulièrement" des fake news sur les réseaux sociaux.

Défense : 3 - 6 - 8 - 11 - 13



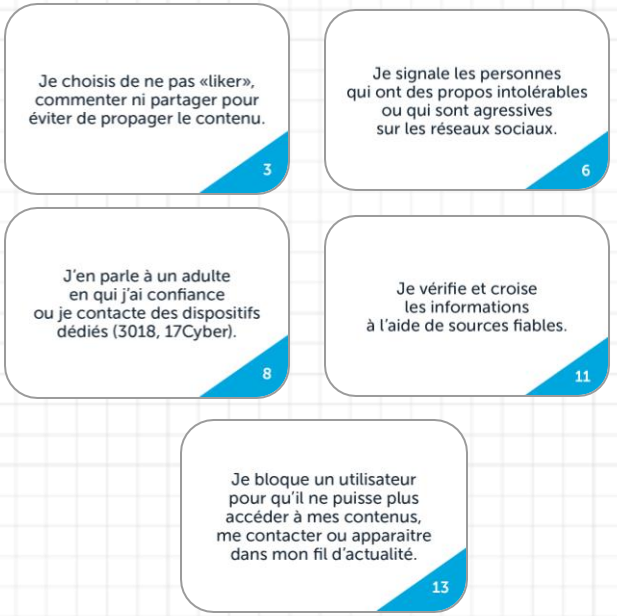
6.4 . Scénarios Influenceur.se

Scénario Influenceur.se n° 4 : 4 -> 12 -> 11 -> 19

Une influenceuse propage de fausses informations sur un évènement dans ta ville. Cela t'incite à vouloir te rendre sur les lieux et te mettre en danger.

Contexte : Selon l'étude "Jeunes, médias, réseaux sociaux et fake news" (Médiamétrie, 2023), 38% des jeunes interrogés se disent inquiets face à la circulation de fake news.

Défense : 3 - 6 - 8 - 11 - 13



7.
FOIRE AUX QUESTIONS

8. FAQ

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.

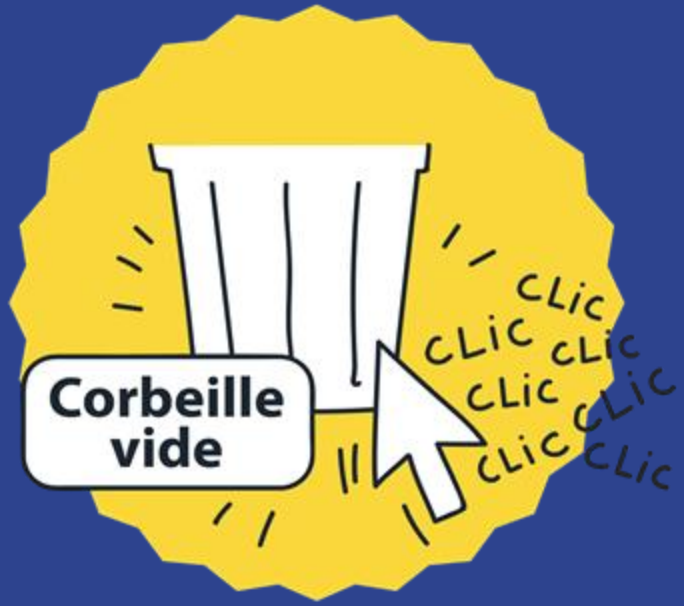
Enfin, en admettant humblement votre propre « non-expertise » dans ce domaine, vous pouvez créer un environnement propice à l'apprentissage collaboratif. Encouragez la réflexion critique, favorisez les discussions et fournissez des ressources (définitions, scénario...) pour aider les participants à se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

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.
Astroturfing	Une opération qui crée artificiellement une apparence de soutien populaire ou d'opinion spontanée sur un sujet, souvent à des fins de manipulation.
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.

8. Glossaire

Mot	Définition
Chiffrer	Protéger des données en les transformant en un code illisible sans la clé de déchiffrement correspondante.
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

Deep fake	Une vidéo ou un audio truqués par intelligence artificielle pour imiter de façon réaliste l'apparence ou la voix de quelqu'un.
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.
Désinformation	Information fausse ou manipulée créée et diffusée intentionnellement pour tromper, manipuler ou nuire.
Données	Informations stockées, traitées et utilisées par des systèmes informatiques.

8. Glossaire

Double authentification	Un mécanisme de sécurité exigeant deux formes d'identification différentes pour accéder à un compte ou un système.
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

Historique	La liste des sites web visités et des actions effectuées sur un navigateur web.
Intégrité	Qualité qui garantit que les données ou les informations n'ont pas été modifiées ou altérées, volontairement ou non.
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.
Malinformation	Information exacte ou basée sur des faits réels, diffusée dans un but de nuire ou de manipuler.

8. Glossaire

Man in the middle	Une attaque où un attaquant intercepte et éventuellement modifie les communications entre deux parties sans leur consentement.
Mésinformation	Information erronée diffusée sans intention de tromper ou de nuire.
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.

8. Glossaire

Navigation privée	Un mode de navigation sur Internet qui ne stocke pas l'historique de navigation ni les cookies.
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

Quishing	Une escroquerie utilisant des QR codes pour rediriger les victimes vers des sites malveillants ou voler des informations.
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

Typosquatting	Une technique qui consiste à enregistrer des noms de domaine ressemblant à des sites légitimes pour piéger les utilisateurs qui font des fautes de frappe.
URL	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.

Pour toute remarque ou suggestion, contactez l'équipe de la Fresque des Cybercitoyens:

fresquedescybercitoyens@advens.fr