



## Alerte internaute en danger

### Contexte

**21%**

des collégiennes déclarent avoir subi au moins une cyberviolence (comme des insultes, humiliations, moqueries en ligne), contre seulement 15% des garçons.

(Source : E-enfance, 2021)

### Objectifs pédagogiques

A l'issue de cette activité, les participant.es seront en capacité de :

- ✓ Développer une utilisation plus responsable des réseaux sociaux.
- ✓ Identifier les risques liés à l'exposition numérique (cyberharcèlement, arnaques, protection des données).
- ✓ Identifier les aspects genrés des interactions en ligne.



**Durée totale de la séance :**  
45 minutes



**Equipe :**  
≈ 20 participant.es  
2 à 4 animateur.rices



**Matériel nécessaire :**  
ballons, plots, coupelles, chasubles, etc.

### Déroulé

#### Introduction (5 minutes) :

Les participant.es sont recruté.es par une agence spéciale pour aider une jeune fille dont le comportement en ligne pose des questions.

Leur mission : analyser ses réseaux sociaux, des indices pour identifier les risques, déjouer des arnaques et l'aider à récupérer le contrôle de ses comptes avant qu'ils ne soient définitivement supprimés !

#### Installation du jeu (5 minutes) :

- 1 Faites des groupes équitables, en fonction du nombre de participant.es (3 minimum par équipe, 2 équipes minimum).
- 2 Préparez le terrain en installant cinq ateliers distincts, en disposition "tour du monde". Chaque équipe devra réaliser le défi technique associé, pour récolter les cinq missions à remplir pour sauver notre influenceuse en herbe, que vous trouverez en annexe de cette fiche (vous devez en imprimer autant que d'équipes). Par exemple, vous pouvez proposer :

- Un atelier jongles
- Un atelier crossbar
- Un atelier chamboule-tout/bowling
- Un atelier sensibilité/précision (ex : type "foot golf")
- Un atelier motricité (ex : relai en équipe)

Adaptez ces propositions au niveau de vos joueur.ses. Les ateliers doivent avoir une durée à peu près équivalente pour éviter les temps d'attente et laisser quelques minutes pour remplir la mission récoltée.

#### Déroulé (30 minutes) :

Chaque équipe passe sur chaque atelier, et vous rapporte la mission remplie pour accéder à l'atelier suivant. A la fin de chaque mission, les joueuses récupèrent un morceau du code final qui leur servira à remporter la partie, soit en le donnant à l'animateur.rice comme mot de passe, soit en ouvrant un cadenas, si vous pouvez fabriquer un "coffre-fort" (à remplir de bonbons ou toute autre récompense qui vous semble appropriée !)

#### Conclusion (5 minutes) :

Prenez le temps de revenir sur les notions abordées dans les missions : certaines étaient-elles difficiles à remplir ? Qu'ont appris les participant.es ? Comment se sont-ils/elles senti.es ?

#### Résumé des missions

##### Mission Selfie Sécurisé (Utiliser les réseaux de manière responsable)

Objectif : Repérer des mauvaises pratiques sur un faux profil Instagram et corriger le profil et savoir faire la différence entre informations privées et sensibles, et informations personnelles mais pas sensibles.

Les joueur.ses ont le fil d'actualité Instagram d'une internaute. Mais elle a laissé plein d'infos personnelles visibles.

Défi : À partir du profil public, les joueur.ses doivent retrouver 4 lieux où une personne mal attentionnée pourrait suivre l'internaute



**Solution :** Les lieux à retrouver sont :

- Le nom de son club de foot
- Son adresse
- Son lycée
- L'adresse de son école de musique

→ Les participant.es doivent entourer les erreurs sur l'impression papier, pour chacune évaluer le niveau de risque (faible / moyen / élevé) et proposer 1 action immédiate pour réduire le risque (ex. : rendre compte privé, supprimer la photo, flouter la façade...).

A la fin, ils/elles récupèrent le chiffre 6, pour le code final

##### Attape-Arnaques (Comprendre les risques - Arnaques et hameçonnage)

Objectif : Trouver le vrai mail parmi plusieurs fausses propositions (cadeaux gratuits, faux concours, messages suspects).



**Solution :**

→ Trouver que la 3e n'est pas une tentative d'arnaque.

→ Puis relier les mails avec un de ces mécanisme : Usurpation d'identité (mail 2) / Pièce jointe malveillante (mail 4) / Ingénierie sociale (mail 5) / Mail légitime (mail 3) / Phishing (1)

L'ordre des réponses de l'épreuve est 24531  
et le chiffre du code final à trouver ici est donc le 4.

##### Rakoles piégées (Risques - Cyberharcèlement)

Objectif : Lire des commentaires (fictifs) sous une vidéo de l'internaute, et repérer quand une interaction devient toxique puis l'associer avec un mécanisme de cyberharcèlement.



**Solution :**

→ Les participant.es doivent placer un "PAS OK" à l'écrit dès qu'un commentaire bascule dans le cyberharcèlement.

→ Ensuite, ils/elles doivent associer chaque mauvais commentaire avec un mécanisme de cyberharcèlement : Moquerie / Normalisation / Pression de groupe / Harcèlement / Rumeurs .

L'ordre des réponses est : 37546.

→ Ensuite, ils/elles doivent choisir une action : Bloquer ? Signaler ? Ignorer ? Répondre poliment ?

Et ils/elles récupèrent le chiffre du code final correspondant au 2e commentaire "pas ok", c'est-à-dire le 7.

#### Data Détectives (Protection des données personnelles)

Objectif : **Trouver un code secret en résolvant des énigmes sur les mots de passe forts, les infos à protéger, etc.**

→ Énigme finale : Créer le "mot de passe parfait".

i

**Solution :**

Chaque bonne réponse donne un bout du mot de passe (ex : "B4", "ll", "0n", "2025!").

#### 4 questions :

1. Lequel de ces éléments est à proscrire absolument dans la composition d'un mot de passe ?  
(Utiliser des informations personnelles (prénom, date de naissance...))
2. Tu reçois ce message : « Votre compte sera suspendu dans 24 h. Cliquez ici pour vérifier. » Quelle est la première action à faire ? (Chercher la même alerte directement dans l'application ou sur le site officiel (sans cliquer sur le lien))
3. Tu suspectes qu'un ami a été piraté et t'envoie des liens étranges. Que fais-tu ? (Lui demandes d'abord si elle a vraiment envoyé le message)
4. Quelle est la meilleure façon de gérer ses mots de passe au quotidien ? (Utiliser un gestionnaire de mots de passe sécurisé ou un mot de passe différent et complexe pour chaque compte)

**À la fin, ils/elles doivent assembler les morceaux**

**→ Mot de passe : "B4ll0n2025!", et ils/elles doivent vous le communiquer.**

**S'il est correct, il faut leur donner le 4e chiffre du code final : 1.**

#### A bas les stéréotypes

Objectif : **Reconnaître et nommer les biais genrés dans les médias. Comprendre leurs effets (sur la perception, la confiance, la légitimité).**

→ Énigme finale : Classer les articles du **plus stéréotypé au plus factuel**. Une fois positionnés, retourner les articles pour obtenir l'**échelle de couleur violet-rose-bleu-vert**. Ces couleurs correspondent par ailleurs aux autres missions (violet : selfie sécurisé, rose : attrape-arnaques, bleu : paroles piégées, vert : data détectives).

**Ainsi, les joueur.ses connaîtront l'ordre des chiffres pour former le code final : 6471.**

i

**Solution :**

Tweet de Craig Foster → le plus factuel, violet

Le petit Journal → un peu sexiste, rose

Article sur Clara Moretti → le 3e, bleu

La une de journal télévisé → la plus sexiste, vert

**Selon leur réponse, à la fin de chaque mission les joueur.ses vont récupérer les morceaux d'un code à 4 chiffre qu'ils/elles devront donner à l'organisatrice pour remporter la partie.**

**Le code final est : 6471.**

#### Résumé des missions

#### Mission Selfie Sécurisée (Utiliser les réseaux de manière responsable)

**Objectif :** Repérer des mauvaises pratiques sur un faux profil Instagram (géolocalisation activée, nom complet, adresse, etc.) et corriger le profil.

→ **Énigme finale :** Créer un post exemplaire sans infos sensibles.

L'internaute a posté un selfie sur Instagram. Mais elle a laissé plein d'infos personnelles visibles. Vite, il faut corriger ça !

**Défi :** Repérer au moins 5 erreurs sur un faux profil Instagram.



Sur le profil, on voit :

- Son vrai nom + prénom
- Son lycée mentionné en bio
- Sa date de naissance entière
- Une photo devant sa maison (adresse visible sur la façade)
- Sa localisation activée

→ Les participant.es doivent entourer les erreurs sur l'impression papier et proposer une bio sécurisée (ex : pas de nom complet, pas d'adresse, pas de localisation active).

#### Attrape-Arnaques (Comprendre les risques - Arnaques et hameçonnage)

**Objectif :** Trouver le vrai mail parmi plusieurs fausses propositions (cadeaux gratuits, faux concours, messages suspects).

→ **Énigme finale :** Proposer en quelques phrases une méthode pour reconnaître un piège en ligne.

L'internaute reçoit un message lui disant qu'elle a gagné un iPhone... mais est-ce un piège ?

**Défi :** Repérer les messages d'arnaques parmi des vrais et faux DM (messages privés).



**Enigme :** Tu reçois 4 messages :

- "Gagne un iPhone 15 Pro, clique vite ici !"
- "Ton ami Alex t'a identifié sur une photo"
- "Votre compte sera supprimé si vous ne cliquez pas là immédiatement"
- "Hey, tu viens à l'entraînement samedi ?"

→ Trouver que 1 et 3 sont des tentatives d'arnaque.

Ensuite, leur demander d'écrire leur(s) règle(s) d'or pour ne pas se faire avoir par une arnaque en ligne : par exemple, toujours vérifier l'expéditeur.ice, ne pas cliquer sur les liens, ne pas donner ses coordonnées sans accord parental, etc.

#### Rapôles piégées (Risques - Cyberharcèlement)

**Objectif :** Lire des conversations (fictives) et repérer quand une interaction devient toxique.

→ **Énigme finale :** Proposer une réaction adaptée face au cyberharcèlement (parler, signaler, bloquer).

Sur le compte TikTok de l'internaute, certains commentaires deviennent méchants... A partir de quand ça dépasse les limites ?

**Défi :** Analyser une discussion et dire à quel moment on doit agir.



**Enigme :** Discussion simulée

- "Stylé cet outfit !"
- "Wow, ton look est original"
- "T'es vraiment bizarre"
- "Tu fais pitié, arrête de poster"
- "Personne ne t'aime"

→ Les participant.es doivent placer un sticker "STOP" dès que ça bascule dans le cyberharcèlement (= à partir du "t'es vraiment bizarre").

Ensuite, ils/elles doivent choisir une action : Bloquer ? Signaler ? Ignorer ? Répondre poliment ? Et expliquer leur choix en quelques mots sur l'emplacement prévu à cet effet.

#### Data Détectives (Protection des données personnelles)

**Objectif :** Trouver un code secret en résolvant des énigmes sur les mots de passe forts, les infos à protéger, etc.

→ **Énigme finale :** Créer le "mot de passe parfait".

Pour protéger l'internaute, il faut retrouver son mot de passe... Mais il est super sécurisé !

**Défi :** Répondre à un quizz pour obtenir 4 morceaux d'un mot de passe.

i

**Enigme :** Chaque bonne réponse donne un bout du mot de passe (ex : "B4", "ll", "0n", "2025!").

4 questions :

- Quel est un bon conseil pour un mot de passe ? (Réponse : minimum 12 caractères, chiffres, majuscules, minuscules et symboles)
- Vrai ou faux ? "Utiliser son prénom + année de naissance est une bonne idée." (Faux)
- Pourquoi faut-il utiliser des majuscules, minuscules, chiffres et symboles dans un mot de passe ? (Réponse : pour que le mot de passe soit plus difficile à deviner)
- Quelle est une bonne habitude avec ses mots de passe ? (Réponse : les changer régulièrement et utiliser un mot de passe différent pour chaque compte)

À la fin, ils/elles doivent assembler les morceaux → **Mot de passe final : "B4ll0n2025!"**

#### Filles VS Stéréotypes (Aspects genrés des interactions en ligne)

**Objectif :** Trier des commentaires en ligne en "ok" ou "stéréotypés" (ex : "tu es jolie pour une fille qui joue au foot !")

→ **Énigme finale :** Imaginer une réponse qui déconstruit le stéréotype.

Sur ses tiktoks de foot, l'internaute reçoit des commentaires bizarres parce qu'elle est une fille.

Sauras-tu repérer les clichés ?

**Défi :** Classer des commentaires en deux catégories : OK (positif/normal) / Cliché/stéréotypé (sexiste, rabaissant)

i

**Enigme :** Commentaires à classer :

- "Tu es super forte, bravo pour ton match !"
- "Il te va bien ce short..."
- "Mais quel talent"
- "Pas mal pour une fille..."
- "T'es vraiment belle, tu veux sortir avec moi ?"
- "Continue à t'entraîner, tu vas tout déchirer !"

Ensuite, on leur demande d'écrire ou dire une réponse pour casser un stéréotype.

Exemple de réponse : "Être une fille n'empêche pas d'être une championne !"

