BD Rencontres en ligne

Fiche pédagogique à l'intention des professionnel·le·s

Thème	**Les rencontres en ligne**
Public cible	**Enseignant·e·s, éducateur·ice·s, infirmier·ère·s, etc. ci-après désigné·e·s intervenant·e·s**
Degré(s)	**9e**
Durée	**45 à 90 minutes**

Lien PER

CT - La capacité à développer une démarche réflexive permet de prendre du recul sur les faits et les informations, tout autant que sur ses propres actions ; elle contribue au développement du sens critique.

PER EN 21 - Développer son esprit critique face aux médias
Sensibilisation à la notion de fiabilité de l'information.

PER EN 23 - Utiliser des outils numériques pour réaliser des projets
Application des règles de sécurité sur ses identifiants, ses mots de passe et ses données personnelles et respect de ceux de ses pairs.

Objectif principal et sous-objectifs

Cet atelier a pour but de permettre aux élèves de développer leurs compétences en lien avec les rencontres en ligne, et aussi:

- Sensibiliser les élèves au fait qu'il est difficile, voire impossible, de vérifier l'identité de quelqu'un·e sur Internet.
- Amener les élèves à développer de bons réflexes si elles et ils rencontrent un·e inconnu·e sur Internet.
- Protéger ses données personnelles sur Internet.

Matériel

- Ordinateur, beamer
- Fiche de l'élève - Rencontres en ligne (p.8)

Déroulement

L'activité se déroule en 4 étapes:

1. Pour démarrer l'activité, des groupes de 4-5 élèves sont formés et une lecture de la BD est faite avec l'ensemble des élèves.
2. La deuxième étape consiste à amener les élèves à discuter et réfléchir en groupes sur le thème abordé dans la BD. Il est attendu que les élèves se basent sur leur vécu et leurs expériences.
3. Lors de la troisième étape, toute la classe aborde différents concepts selon les sujets amenés par les élèves. Il s'agit d'un échange pour évoquer, voire débattre des éléments positifs et négatifs. Les élèves partagent avec les autres les comportements qu'ils pourraient changer et les implications que ces changements pourraient entraîner.
4. Au terme de l'activité, chaque groupe détermine un message à retenir.

Étape 1
Lecture de la BD

Projeter la BD et la lire avec l'ensemble de la classe. Préciser aux élèves qu'elles et ils en discuteront par la suite et les inviter à déjà réfléchir aux similitudes et différences avec leurs pratiques personnelles. Il s'agit de s'appuyer sur leurs expériences et la règle du non-jugement doit être rappelée.

Étape 2
Discussion en petits groupes

Par groupe de 4-5, les élèves reçoivent une planche BD et répondent aux questions ci-dessous :

1. Que pensez-vous de la situation ?
2. Quels sont les points positifs dans cette situation (pour soi, pour les autres, maintenant ou après) ?
3. Identifiez-vous des risques et si oui, lesquels (pour soi, pour les autres, maintenant ou après) ?
4. Que dit la loi ?
5. Quels conseils donneriez-vous à vos camarades ?

Demander aux élèves de résumer leur échange et de formuler un conseil qu'elles et ils aimeraient transmettre à leurs camarades.

Étape 3
Discussion générale

L'intervenant·e s'appuie sur les propos des élèves. Elle ou il rebondit dans le but de développer leurs compétences et connaissances, notamment sur les différents thèmes abordés dans le lexique (p.5).

L'intervenant·e aide les élèves à identifier les différents enjeux que représente la rencontre d'une personne inconnue sur Internet et les réseaux sociaux.

Questions de relance et de mise en débat :

Pourquoi rentrons-nous en contact avec des personnes inconnues via les réseaux sociaux ou des sites de rencontres anonymes ?

- Pour nous amuser
- Répondre à un défi de nos ami·e·s
- Nous faire de nouveaux ami·e·s
- Nous nous sentons seul·e·s.
- Poser des questions sur un sujet que nous n'oserions pas aborder avec nos ami·e·s
- Prendre un risque et voir jusqu'où la conversation peut aller
- Répondre à une personne inconnue qui nous a directement contacté·e·s sans que nous le souhaitions

Pourquoi devons-nous nous méfier des personnes inconnues sur Internet ?

- Il peut s'agir d'une arnaque.
- Il peut s'agir d'une personne qui souhaite nous pirater en nous demandant de cliquer sur des liens qu'elle partage avec nous.
- Il peut s'agir d'une personne malveillante avec des intentions à caractère sexuel (plus de détails dans le lexique p.5).

Avez-vous déjà entendu parler d'une pratique qui s'appelle le grooming (cf. lexique p.5) ?

Que pouvons-nous faire pour nous protéger des personnes inconnues sur les réseaux sociaux ?

- Éviter de parler à des inconnu·e·s
- Avoir un compte privé pour choisir qui aura accès à celui-ci
- Configurer les paramètres de confidentialité du réseau social que nous utilisons et bloquer les comptes qui nous posent problème
- Éviter de partager des informations personnelles qui pourraient permettre à quelqu'un·e de nous identifier
- Éviter de partager des contenus (photos et vidéos) sur lesquels nous sommes reconnaissables
- Éviter de partager des contenus intimes pour ne pas être victime de chantage (cf. lexique sous « Sextorsion »).

Comment pouvons-nous nous faire passer pour quelqu'un·e d'autre derrière un écran ?

- Lorsque nous créons un compte sur un réseau social, nous pouvons concevoir notre profil tel que nous le souhaitons car il n'y a pas de vérification d'identité.
- Nous pouvons utiliser des photos qui sont sur Internet ou sur d'autres comptes de réseaux sociaux.
- Il existe des logiciels de montage qui permettent de modifier son apparence. Même une vidéo peut être modifiée.

Est-t-il possible de faire des rencontres positives en ligne ?

- Nous pouvons rencontrer des personnes qui ont les mêmes passions et centres d'intérêts que nous.
- Même si cette rencontre est positive et que nous avons confiance, nous nous protégeons en évitant de transmettre des informations personnelles (nom, prénom, adresse, etc.) et nous ne partageons pas des contenus (images ou vidéos) qui pourraient ensuite être utilisés contre nous.

Quelles précautions devons-nous prendre si nous souhaitons rencontrer une personne que nous avons connue sur les réseaux sociaux ?

- Nous en parlons à nos parents ou à un·e adulte de confiance.
- Nous ne nous rendons pas seul·e·s au rendez-vous.
- Nous rencontrons la personne dans un lieu public.

Étape 4 Discussion et conclusion

Chaque groupe partage l'un après l'autre le message qu'il aimerait transmettre à ses camarades.

Messages à transmettre

- Nous ne savons jamais qui se cache derrière l'écran.
- Les personnes que nous rencontrons sur Internet peuvent mentir.
- Si nous rencontrons une personne sur Internet, nous protégeons nos données personnelles et notre intimité.
- Nous n'allons jamais seul·e·s à un rendez-vous avec une personne rencontrée sur Internet.
- Nous donnons rendez-vous dans un lieu public.

- Si une personne inconnue nous transmet des contenus inadaptés, nous pouvons bloquer son compte et en parler à un·e adulte de confiance.
- Les données personnelles que nous publions peuvent être utilisées contre nous.

Conseils pour se protéger d'une mauvaise rencontre

Lorsqu'une personne que nous ne connaissons pas souhaite s'abonner à notre compte de réseau social ou démarrer une discussion, il est important d'analyser son compte en vérifiant les éléments suivants :

La date de création du compte et le nombre de publications
S'il s'agit d'un compte qui vient d'être créé et qui ne possède aucune publication, nous devons nous méfier.

La photo de profil
Pour vérifier une photo de profil, il est possible d'utiliser Google Images. À l'adresse https://images.google.com, nous pouvons identifier le logo de l'appareil photo et cliquer sur « Rechercher par image ». Il nous suffit ensuite de copier l'adresse de la photo et de l'insérer dans le champ de recherche. Le moteur de recherche nous indiquera toutes les sources qui ont utilisé cette image. Cela nous permettra de déterminer si la photo de profil appartient, par exemple, à un·e mannequin ou à un, voire plusieurs compte·s existant·s. Il pourra alors s'agir d'une usurpation d'identité.

Il est possible dans les paramètres de confidentialité des réseaux sociaux ou des messageries de modifier les réglages pour empêcher les personnes qui ne font pas partie de nos contacts ou de nos abonné·e·s de nous contacter.

Il existe des sites Internet ou des réseaux sociaux qui permettent de faire des rencontres en ligne avec des personnes inconnues tout en allumant la caméra de son smartphone ou de son ordinateur. Les rencontres sont aléatoires. Nous pouvons alors nous retrouver face à des personnes de notre âge mais également des personnes plus âgées et malveillantes. Nous pouvons être confronté·e·s à des personnes qui sont nues voire, dans le pire des cas, être exposé·e·s à des actes sexuels en direct.

> **Il est important de sensibiliser les élèves au fait que sur les plateformes de rencontres aléatoires, il n'est pas possible de savoir sur quel profil nous allons tomber. Cela peut être très choquant et risqué.**

Lexique pour les intervenant·e·s

Grooming

Toute personne qui entre en contact avec des enfants et adolescent·e·s qui n'ont pas atteint la majorité sexuelle de 16 ans dans le but d'atteindre un plaisir sexuel ou d'avoir une relation à caractère sexuel.

Cette relation peut consister en :

- Un acte d'ordre sexuel physique entre l'auteur·ice et la victime
- Un acte d'ordre sexuel physique de l'auteur·ice sur lui-même ou elle-même ou un tiers, ou de la victime sur elle-même ou un tiers
- Un échange à caractère excitant sexuellement
  L'échange peut porter sur l'intimité de l'enfant au sujet de son développement sexuel, de l'arrivée des signes intimes de puberté, des relations de l'enfant, de ses désirs, des désirs ou des attributs de l'auteur·ice etc.

Le processus classique de grooming est le suivant :

- **Prise de contact**
  Dans la plupart des cas, un individu peut dans un premier temps essayer d'entrer en contact avec un·e enfant en utilisant un service en ligne.
- **Mise en confiance de la victime**
  L'individu peut tenter d'établir une relation de confiance avec l'enfant en lui posant des questions sur ses centres d'intérêts. Il peut demander progressivement à l'enfant comment elle ou il se sent, s'efforcer de savoir si elle ou il rencontre des difficultés dans ses amitiés ou sa relation avec ses parents. Si l'enfant est en difficulté, reconnaître son mal-être et se positionner comme un·e confident·e.
- **Questions intimes**
  Une fois la confiance instaurée et une relation amicale voire amoureuse établie, l'individu peut chercher à aborder des questions plus intimes.
- **Proposition d'une relation à caractère sexuel**
  La relation peut être prévue en ligne (par appel en visio ou par échange de contenu comme des photos ou des vidéos) ou dans un lieu donné (rencontre physique pour entretenir un ou plusieurs actes d'ordre sexuel définis spécifiquement ou non).
- **Préparation à la rencontre**
  Exemples : aller prendre le train ou la voiture, acheter des préservatifs sur la route, se rendre au lieu de rendez-vous
- **Rencontre à des fins sexuelles (physique ou virtuelle)**

Le grooming n'est pas inscrit en tant que tel dans le code pénal mais certains comportements constitutifs de grooming peuvent être poursuivis :

- Art.187 CP : Actes d'ordre sexuel avec des enfants
- Art.197 CP : Pornographie
- Art.180 CP : Menaces
- Art.181 CP : Contrainte
- Art.156 CP : Extorsion et chantage

Sources :
- www.actioninnocence.org/publication/dossier-thematique-grooming/
- www.actioninnocence.org/publication/depliant-professionnels-grooming/

Sextorsion

Cette pratique consiste à faire du chantage à une personne après avoir reçu de sa part un ou plusieurs fichiers de nu ou à caractère sexuel.

Cette pratique est illégale.

Elle peut être menée par
- des réseaux organisés qui utilisent de faux comptes sur les réseaux sociaux dans le but de demander de l'argent en échange
- une personne, connue ou inconnue, dont l'objectif n'est pas l'argent mais l'obtention de nouveaux fichiers de nu ou à caractère sexuel de l'enfant ou de l'adolescent·e (pédopornographie)
- la ou le partenaire de la victime, qui à la suite de l'envoi d'un « nude » (fichier à caractère sexuel) lui fait subir des pressions ou du chantage. Par exemple : « maintenant que j'ai ce fichier, tu feras tout ce que je veux sinon je le diffuse à tout le monde ».

Cette pratique n'est pas inscrite en tant que telle dans le code pénal mais des articles de loi y font référence :
- Art.156 CP : Extorsion et chantage
- Art.197 CP : Pornographie
- Art.174 CP : Calomnie
- Art.179 CP : Violation du domaine secret ou du domaine privé au moyen d'un appareil de prise de vues

Sources :
- www.skppsc.ch/fr/sujets/Internet/sextortion/
- www.ciao.ch/articles/sextorsion/

Âge d'inscription aux réseaux sociaux, que dit la loi ?

En Suisse, il n'existe pas de législation spécifique à l'âge requis pour s'inscrire sur les réseaux sociaux, sauf pour les sites de rencontres destinés aux adultes et ceux pour les jeux d'argent. L'âge d'inscription sur les réseaux sociaux dépend principalement de lois commerciales qui régissent ces plateformes et qui visent à les protéger.

Selon la loi américaine, les réseaux sociaux sont autorisés à collecter, stocker, analyser et vendre les données de leurs utilisateur·ice·s dès l'âge de 13 ans. C'est pourquoi YouTube, WhatsApp, Instagram, Snapchat et TikTok ont déterminé l'âge d'inscription à 13 ans.

Aux yeux de la loi suisse, seul le comportement des utilisateur·ice·s sur les réseaux sociaux peut faire l'objet de délits, les enfants étant pénalement responsables de leurs actes dès l'âge de 10 ans.

Mauvaises rencontres, différents profils

Les réseaux sociaux sont utilisés par des milliards de personnes dans le monde entier. Il est donc possible de rencontrer des personnes qui ont des bonnes intentions mais aussi des personnes malveillantes.

Ces dernières peuvent chercher à nous arnaquer en se faisant, par exemple, passer pour un·e youtubeur·se connu·e. Un faux compte envoie massivement des demandes d'ami·e·s sur les réseaux sociaux et nous transmet un message si nous acceptons la demande (technique de phishing). Le message nous explique que nous avons gagné un prix (par exemple un smartphone) et que pour le recevoir, nous devons cliquer sur un lien. Le lien nous amène vers un formulaire que nous devons remplir avec nos informations personnelles. Lorsque nous validons l'inscription, sans le savoir, nous souscrivons à un abonnement. Il peut aussi s'agir d'un appel à faire sur un numéro surtaxé.

Les comptes des personnalités publiques sur les réseaux sociaux sont accompagnés d'une pastille bleue à côté de leur nom. Cela signifie que ces personnalités sont « certifiées », leurs comptes sont confirmés comme authentique par le réseau social. Il s'agit bien de ces personnalités.

Une personne peut aussi vouloir nous pirater en nous envoyant, par exemple, un lien et en nous demandant de cliquer dessus. Il peut s'agir d'un moyen d'installer un logiciel malveillant sur notre téléphone ou ordinateur sans que nous nous en rendions compte. Notre appareil est ensuite bloqué et une demande de rançon est envoyée par l'escroc pour récupérer nos informations personnelles (rançongiciel). Le piratage peut prendre la forme de phishing, d'un rançongiciel, d'une clé USB piégée, d'un faux site Internet, d'un faux réseau wifi, etc.

Il peut également s'agir d'une personne pédophile qui se cache derrière un faux profil.

D'une manière générale, il est important de protéger nos informations personnelles et d'être prudent·e·s lorsque nous communiquons avec quelqu'un·e que nous ne connaissons pas.

Pour plus d'informations

Action Innocence
4 rue Viollier
CH - 1207 Genève
Tél. +41 (0)22 735 50 02
contact@actioninnocence.org
actioninnocence.org

Fiche de l'élève

BD Rencontres en ligne