Les droits humains à l'ère du numérique

WOMEN DELIVER

- Pré-test
- Introduction
- Que sont les droits numériques ?
- Comment protéger mes droits numériques ?
- Comment me protéger du cyberharcèlement et y réagir ?
- Conclusion
- Post-test

QUESTION BANKS

- Les droits humains à l'ère du numérique, évaluation avant/après

Pré-test

Avant de suivre ce nouveau cours de l'Université en ligne Women Deliver, nous allons faire une pause et réfléchir à ce que vous savez déjà sur ce sujet en faisant un petit pré-évaluation. Les questions de ce pré-évaluation seront toutes traitées dans le cours, donc ce n'est pas grave si vous ne connaissez pas encore toutes les réponses!

Question

01/01

---

7 questions drawn randomly from Les droits humains à l'ère du numérique, évaluation avant/après

Introduction

Nos vies et nos activités de plaidoyer dépendent de plus en plus de l'utilisation de technologies, notamment des réseaux sociaux. Or, la technologie peut être un outil précieux pour améliorer notre travail. Malheureusement, elle peut également nous exposer à des atteintes à la vie privée, à la discrimination et au harcèlement. En outre, les inégalités d'accès aux technologies numériques empêchent de nombreux individus d'exercer leurs droits.

« Numérique » désigne l'utilisation d'appareils électroniques qui stockent et traitent des données, tels que les téléphones mobiles et les ordinateurs, ainsi que les logiciels et les applications utilisés sur ces appareils, comme les e-mails et les réseaux sociaux. Dans l'espace numérique, vous avez les mêmes droits que dans le monde déconnecté ou physique, mais peu de gens savent comment reconnaître et protéger ces droits.

Ce module vous aidera à vous protéger et à protéger les autres, et vous montrera comment utiliser vos droits numériques de façon à augmenter votre impact.

À la fin de ce module, vous serez capable de :

1. Décrire ce que sont les droits numériques.
2. Comprendre comment protéger vos droits numériques et ceux des autres.
3. Prendre des mesures pour vous protéger du cyberharcèlement et savoir comment réagir lorsque d'autres personnes sont harcelées en ligne.

COMMENÇONS !

Que sont les droits numériques ?

Comprendre vos droits numériques est la première étape pour prendre le contrôle de votre présence en ligne. Même si vous utilisez peu les technologies, à l'ère d'Internet, les droits numériques sont un aspect essentiel des droits humains.

Que sont les droits numériques ?

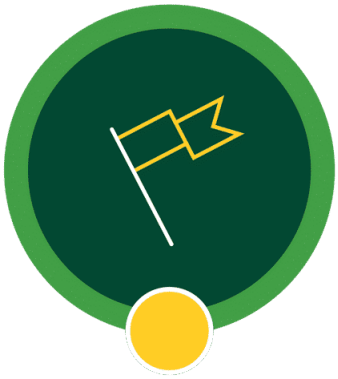
Le Conseil des droits humains de l'ONU affirme que tous les droits humains dont vous jouissez dans le monde physique (déconnecté) s'appliquent à votre identité numérique lorsque vous naviguez sur Internet, échangez sur les réseaux sociaux et utilisez des technologies comme votre téléphone/smartphone. Les droits numériques comprennent le droit à la vie privée, la liberté d'expression et le droit de vivre sans violence ni harcèlement.

Comment cela se traduit-il au niveau international et au niveau national ? Sélectionnez chaque élément pour en savoir plus.

International

National

International

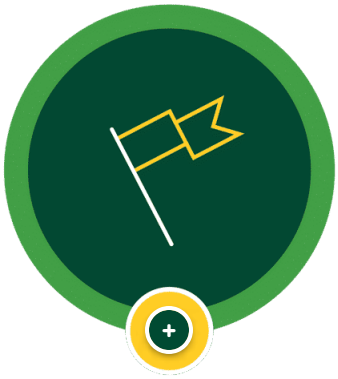


National

International

De nombre ux cadres internationaux pour les droits humains sur lesquels nous nous appuyons en tant que défenseur(e)s, tels que la Convention des droits de l'enfant (CIDE) ou la Convention sur l'élimination de toutes les formes de discrimination à l'égard des femmes (CEDEF)—ont été créés avant l'invention d'Internet et des technologies numériques grand public. Si ces conventions ont été modifiées à l'ère du numérique, il manque encore un cadre international sur les droits numériques.

International



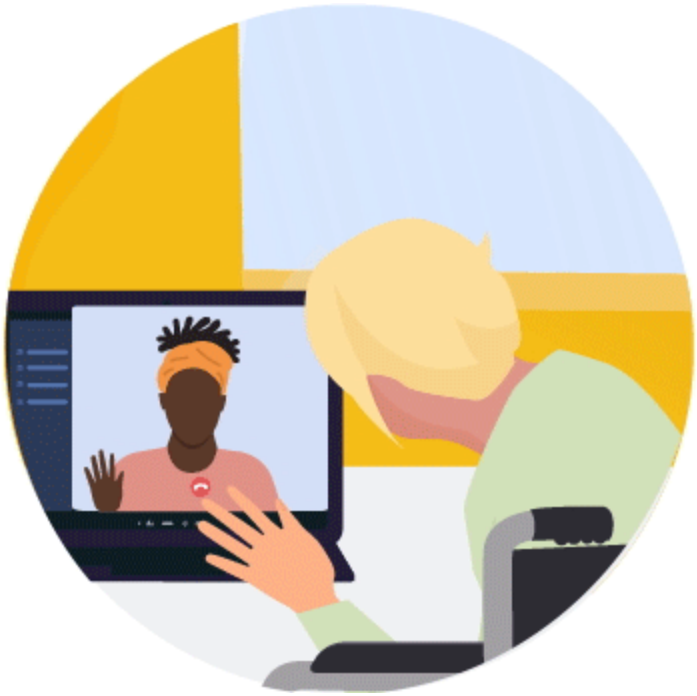
National

National

Au niveau national (du pays), les lois qui réglementent la navigation sur Internet se concentrent principalement sur les activités transactionnelles, financières et d'e-commerce. Elles ont tendance à délaisser la protection et l'application des droits numériques des citoyens. Quelques pays ont bien des lois qui traitent du harcèlement en ligne, mais celles-ci restent limitées et sont susceptibles de ne pas couvrir toutes les formes de cyberharcèlement que les citoyens, en particulier les personnes issues de populations sous-représentées, peuvent être amenés à rencontrer.

Pourquoi les droits numériques sont-ils si importants ?

Même avant la pandémie de Covid-19, de nombreux aspects de nos vies étaient déjà en ligne. Nous communiquons avec nos amis et notre famille, accédons aux informations et trouvons des ressources et des services importants sur Internet. Désormais, suite à la pandémie de Covid-19, nous sommes encore plus dépendants du numérique.



Jetons un œil à ces statistiques. Sélectionnez chaque élément pour en savoir plus.

4,57 milliards

d’internautes actifs en avril 2020.

59%

Pourcentage de la population mondiale ayant accès à Internet. 9 des 10 pays avec le plus faible accès à Internet sont en Afrique.

98%

Femmes/filles interrogées dans 22 pays qui utilisent les réseaux sociaux, les plateformes les plus utilisées étant Instagram, Facebook et WhatsApp.

Source: **Plan International**

En voyant à quel point nos vies et ces technologies sont entremêlées, il est important de comprendre qui gère les plateformes et les systèmes qui dictent une si grande partie de notre quotidien. Les espaces en ligne que nous fréquentons sont généralement contrôlés par des

entreprises privées motivées par le profit, comme Meta, Google, Alibaba, TenCent ou Apple. Les réglementations qui contraignent ces entreprises à protéger nos droits varient selon les pays et ne sont généralement pas très strictes.

Il existe de nombreuses violations possibles de nos droits en ligne, notamment le cyberharcèlement, le Data Mining (exploration de données) et la surveillance. Vous avez probablement vous-même déjà subi certaines de ces violations. Comme pour les droits humains, les droits numériques s'appliquent de manière disparate. Les populations qui rencontrent des discriminations dans le monde physique, comme les personnes autochtones, noires et de couleur (BIPOC), les personnes LGBTQIA+ et d'autres populations traditionnellement exclues, subissent souvent aussi davantage de discrimination et de marginalisation en ligne.

Qui est responsable de l'application et de la protection des droits numériques ?

Les États, les entreprises, les individus et les organisations de la société civile assument tous la responsabilité de la protection des droits numériques.

Sélectionnez chaque élément ci-dessous pour en savoir plus.

États

Comme pour vos droits fondamentaux, les **États** (ou gouvernements) assument la responsabilité de l'application et de la protection de vos droits numériques. Ceci est stipulé dans le Pacte international relatif aux droits civils et politiques, un traité mondial ratifié par 173 États membres de l'ONU. Les États ont l'obligation de s'abstenir d'enfreindre vos droits numériques (mesures « négatives ») ET de prendre des mesures pour protéger et garantir vos droits (mesures « positives »). Par exemple, les États ne peuvent pas vous surveiller sans suivre le processus défini par la loi dans leur pays (une mesure négative). Les États ont également l'obligation de réglementer les entreprises technologiques pour veiller à ce qu'elles n'extraient pas vos données pour les vendre sans votre consentement (mesure positive).

Entreprises

Même si les États sont les premiers responsables de la protection de vos droits, les **entreprises** ont l'obligation de respecter tous les droits humains, en plus de se conformer à toute législation nationale en vigueur. Ceci est énoncé dans les Principes directeurs des Nations Unies relatifs aux entreprises et aux droits humains, qui établit des normes mondiales de conduite attendue des entreprises. Les entreprises doivent examiner de manière proactive l'impact de leur modèle économique sur les droits humains et éviter de leur nuire à travers leurs activités, directement ou indirectement. Lorsqu'elles ont un impact négatif sur les droits humains, elles doivent prendre des mesures immédiates pour y remédier.

Organisations de la société civile

Les organisations de la société civile et les défenseur(e)s comme nous jouent un rôle important, car ils poussent les États et les entreprises à tenir leurs engagements. La défense des

droits numériques est un mouvement en plein essor aux échelons local, national, régional et mondial. Si vous souhaitez vous impliquer, lisez les questions sur la défense des droits numériques dans le rapport Free to Be Online, et renseignez-vous sur les organisations qui défendent les droits numériques à travers le monde.

- Global Network Initiative
- Privacy International
- Ranking Digital Rights
- Digital Rights Nepal
- Fundación Karisma
- IPANDETEC
- Digital Grassroots

Les organisations internationales, comme l'Organisation des Nations unies, contrôlent elles aussi les droits numériques et introduisent de nouvelles institutions et de nouveaux mécanismes. Citons par exemple le Rapporteur spécial sur le droit à la vie privée. récemment nommé.

Individus

Enfin, en tant qu'**individus**, nous avons une obligation de respect des droits numériques de nos pairs. Ceci implique de ne pas harceler les autres en ligne et de protéger toute information ou donnée personnelle partagée avec vous. Lisez la suite de ce module pour découvrir comment respecter et protéger les droits numériques de vos pairs, autres citoyen(ne)s et utilisateurs des technologies !

Envisagez le scénario suivant. Utilisez ce que vous avez appris sur les droits numériques jusqu'à présent pour répondre.

Vous organisez une campagne sur les réseaux sociaux pour un projet de défense à venir sur lequel vous travaillez. Quelles mesures pouvez-vous prendre pour vous assurer que les droits numériques seront pris en compte ?

Sélectionnez les meilleures réponses parmi les quatre options suivantes.

- [ ] Penser aux personnes qui auront accès aux réseaux sociaux pour participer à la campagne et à ce qui peut être fait pour garantir la participation de ceux qui n'y ont pas accès.
- [ ] Réfléchir à comment protéger ceux qui participent à votre campagne contre le cyberharcèlement.
- [ ] Veiller à ce que toute donnée recueillie soit utilisée aux fins prévues et stockée en lieu sûr.

- [ ] Passer en revue les préférences en matière de sécurité pour vos comptes de réseaux sociaux.

SUBMIT

À SUIVRE : COMMENT PROTÉGER MES DROITS NUMÉRIQUES ?

Comment protéger mes droits numériques ?

Maintenant que vous savez ce que sont les droits numériques, il est important de connaître leurs violations possibles afin de pouvoir prendre des précautions pour les éviter.

Qu'est-ce que la fracture numérique de genre ?

L'accès aux technologies numériques et à Internet est un droit fondamental. Pourtant, l'accès varie selon les communautés et les pays en fonction de l'endroit où vous vivez, votre revenu, votre genre, votre langue, ou encore votre origine ethnique. En tant que défenseurs de l'égalité de genre, il est important de savoir ce qu'est la fracture numérique de genre, c'est-à-dire l'inégalité d'accès aux technologies numériques selon le genre.

Regardez ces statistiques sur la fracture numérique de genre.

S'il n'y avait que 10 personnes dans le monde...

...5 n'auraient pas accès à Internet.

S'il n'y avait que 10 personnes en ligne...

...seule 1,5 disposerait d'une connexion Internet abordable et accessible.

S'il n'y avait que 10 personnes dans le monde, 4,9 seraient des femmes...

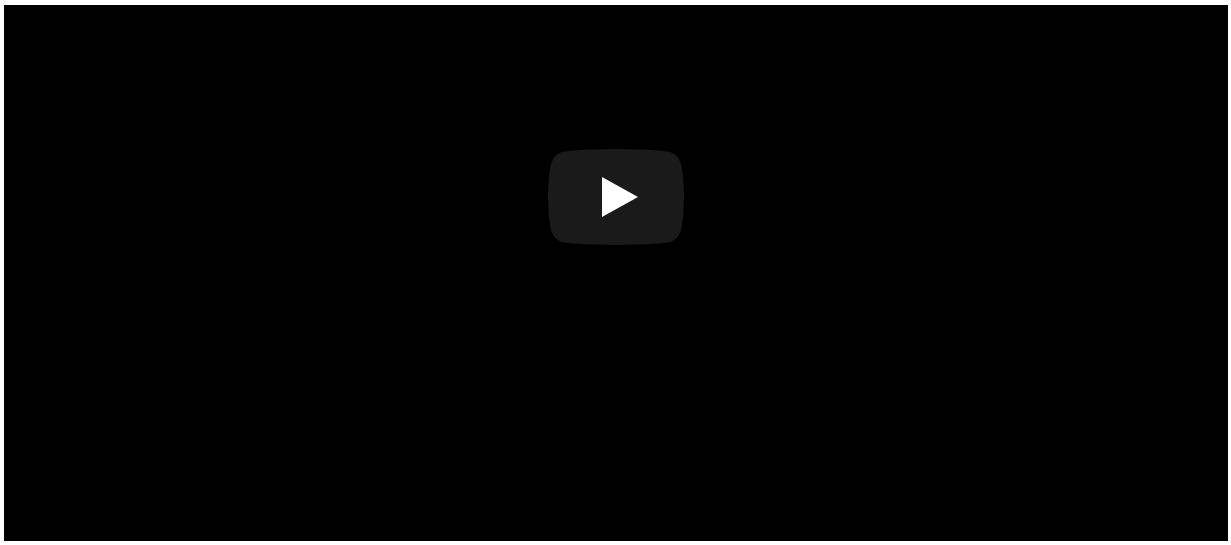
...et seules 2 d'entre elles auraient un accès mobile à Internet.

Source: **Association mondiale des guides et des éclaireuses**

Comment l’utilisation des données peut-elle être détournée ?

Les « Données » sont les faits ou informations bruts relatifs à votre identité (nom, date de naissance, adresse) et à votre comportement en ligne (sites consultés, termes de recherche utilisés). Ces données en disent beaucoup sur vous en tant que personne et sur ce qui compte pour vous. Lorsqu’elles sont compilées ensemble, on les appelle « empreinte numérique ». Votre empreinte numérique comprend tout ce qui vous concerne, des photos que vous aimez sur Facebook à la durée de visualisation d’une publicité sur Instagram.

Regardez cette vidéo pour savoir quand partager des données personnelles et privées (et quand s’abstenir !).



Analysons trois mauvais usage des données : l'utilisation d'algorithmes et l'exploitation de vos informations. Sélectionnez chaque élément pour en savoir plus.

Discrimination

Contrôle de l'information

Exploitation de vos données

Discrimination

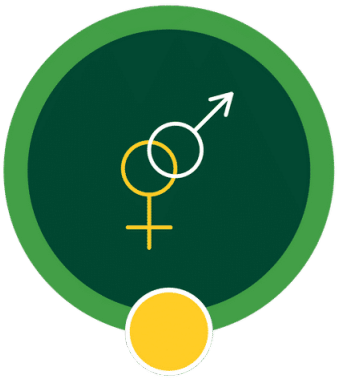
Contrôle de l’information

Exploitation de vos données

Discrimination

Parfois, notre empreinte numérique comprend des données qui ne reflètent pas forcément la complexité de notre identité, par exemple lorsque des sites web demandent aux utilisateurs de choisir entre des options binaires comme « homme » ou « femme ».

Dans ces cas-là, ces données peuvent être utilisées par la suite pour discriminer, car le ciblage de l’information (évoqué plus bas) utilise souvent les caractéristiques personnelles intégrées dans les données d’un utilisateur pour contrôler le type d’information que voit un utilisateur. Par exemple, des informations sur la contraception peuvent s’afficher uniquement pour les utilisateurs définis comme « femme » et « plus de 18 ans », alors que nous savons qu’en réalité, il est important que tout le monde ait un accès équitable à ces informations.



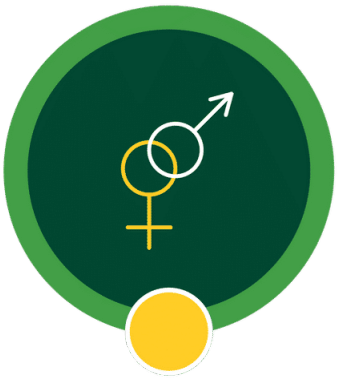
Discrimination

Contrôle de l’information

Exploitation de vos données

Contrôle de l’information

Vous avez un droit à l’information et le droit de vous exprimer librement en ligne. Cependant, les algorithmes et l’intelligence artificielle utilisés par de nombreuses entreprises de technologie pour améliorer les capacités de recherche perturbent l’échange libre et équitable d’informations et d’idées en ligne. Par exemple, de nombreux algorithmes font remonter du contenu erroné ou incorrect en fonction du nombre de vues. C’est pourquoi la désinformation et les rumeurs sensationnalistes, comme les mythes sur la Covid-19, peuvent se propager si rapidement sur Internet. Les algorithmes peuvent être très complexes. À partir des facteurs utilisés par l’algorithme, le concepteur de cet algorithme peut contrôler le type de contenu que voit un utilisateur sur un réseau social ou une plateforme de recherche. Par exemple, en fonction du contenu que vous voyez généralement en ligne (comme une source d’actualités spécifique ou un parti politique), un algorithme peut être programmé pour continuer à vous montrer du contenu similaire. Ceci peut vous empêcher de vous confronter à d’autres points de vue sur une question et contribuer à la propagation de la désinformation. Ce contrôle de l’information donne beaucoup de pouvoir aux entreprises de technologie, car elles peuvent décider des informations à amplifier. Les informations que nous consommons influencent grandement nos opinions et nos idées sur nos comportements personnels, nos convictions et notre vision du monde. Ainsi, elles peuvent entraver notre capacité à garder la tête froide et à poursuivre nos propres objectifs (liberté de penser). Être conscients de leur influence potentielle et rester vigilants à leur égard peut aider à briser leur emprise. Nombreux sont les défenseurs qui poussent pour une meilleure supervision et une réglementation de ces entreprises.



Discrimination

Contrôle de l'information

Exploitation de vos données

Exploitation de vos données

Une autre façon dont les entreprises technologiques qui recueillent des données à caractère personnel peuvent dévoyer l'utilisation des données consiste à partager ces informations avec d'autres entreprises, qui les utilisent pour cibler la publicité, ou avec des gouvernements, qui les utilisent pour censurer et contrôler leurs citoyens. De nombreuses entreprises technologiques fonctionnent avec un modèle économique (business model) qui dépend de l'extraction et/ou de la surveillance des données. Parfois, les gouvernements peuvent même exiger d'une entreprise qu'elle transmette les données ou dispose de sa propre technologie de surveillance. Les données peuvent également être volées par des cybercriminels au moyen du piratage et de cyberattaques, de plus en plus fréquents ces dernières années.

Réglementations en matière de protection des données

Heureusement, il existe des réglementations pour protéger vos données, telles que le Règlement général sur la protection des données (RGPD). Le RGPD est entré en vigueur dans l'Union européenne (UE) en 2018. Il régit les entreprises technologiques qui exercent leurs activités dans l'UE, y compris Meta et Google. Le RGPD exige que les entreprises qui recueillent des données à caractère personnel soient transparentes sur leur utilisation et obtiennent le consentement de l'utilisateur avant le recueil des données. Ces informations sont généralement communiquées à travers les Conditions générales, que les utilisateurs doivent lire et accepter avant d'utiliser une

plateforme. Cependant, les défenseurs soutiennent qu'au vu de la prédominance de certains géants du secteur dans nos vies quotidiennes, comme Meta, Apple et Google, les utilisateurs n'ont pas d'autre choix que d'accepter ces conditions. Par conséquent, le consentement accordé pour le recueil et l'utilisation de nos données n'est pas vraiment un consentement donné librement et pourrait être considéré comme un accord coercitif.

Comment me protéger en ligne ?

À présent, évoquons certaines mesures que vous pouvez prendre dès maintenant pour mieux vous protéger, ainsi que les organisations avec lesquelles vous travaillez. N'hésitez pas à interrompre le cours après chaque rubrique et à compléter certains de ces éléments d'action.

Sélectionnez chaque stratégie pour en savoir plus.

Utilisez des mots de passe forts

- Utilisez au moins 8 caractères dans votre mot de passe, y compris des chiffres, des symboles et des lettres en majuscules et en minuscules.
- Évitez les mots de passe répandus et les informations personnelles.
- Utilisez différents mots de passe pour vos différents comptes.
- Pensez à toujours vous déconnecter lorsque vous avez fini d'utiliser un site, quel que soit l'ordinateur ou l'appareil mobile utilisé.
- Utilisez une connexion avec une authentification à deux facteurs, ce qui signifie qu'en plus de votre mot de passe, vous devrez saisir un code que vous recevrez via une application sur votre appareil mobile.
- Si vous avez besoin d'enregistrer votre mot de passe, utilisez du papier ou un système de gestion de mots de passe chiffré et sécurisé. Ceci est particulièrement important si vous travaillez au sein d'une organisation où de nombreuses personnes doivent partager des mots de passe et peuvent accéder à des comptes sur différents appareils. Partagez les mots de passe uniquement avec vos collègues qui ont besoin d'accéder à ce site.

Vous ne savez toujours pas si votre mot de passe est fort ? Utilisez un outil comme The Password Meter pour vérifier.

Protégez votre empreinte numérique

Sécurisez vos informations personnelles en ligne et celles des autres en prenant les mesures suivantes :

- Ne partagez pas votre nom complet ou toute autre information permettant de vous identifier, telle que votre âge, votre localisation précise, votre numéro de téléphone, ou un nom d'école, sur les réseaux sociaux ou tout autre forum public.
- Contrôlez vos paramètres de confidentialité sur les réseaux sociaux pour vérifier que vous savez avec qui vous partagez des informations, telles qu'une photo, une mise à jour de statut ou votre localisation.
- N'oubliez pas qu'une fois qu'un contenu est en ligne, il est impossible de le supprimer totalement. Réfléchissez avant de publier ! Ceci vaut pour vos commentaires et réactions aux publications des autres, alors pensez à interagir avec vos pairs en ligne de la façon dont vous aimeriez qu'ils interagissent avec vous.
- Évaluez s'il est sûr de mentionner votre localisation, étant donné que les autres sauront où vous vous trouvez.
- Demandez toujours la permission avant de publier des photos, des vidéos ou du contenu concernant un tiers. Si vous gérez une organisation, ceci s'applique aussi à ses activités Internet : demandez toujours l'accord avant de publier ! Si quelqu'un publie quelque chose vous concernant et que cela vous déplaît, demandez-lui de le retirer.
- Si vous avez moins de 18 ans ou que vous travaillez vous-même avec des mineurs, sollicitez un adulte de confiance concernant la présence du mineur sur les réseaux sociaux.
- Si vous stockez des informations à caractère personnel ou des données sensibles concernant votre personnel, vos partenaires, vos électeurs ou vos participants, veillez à ce

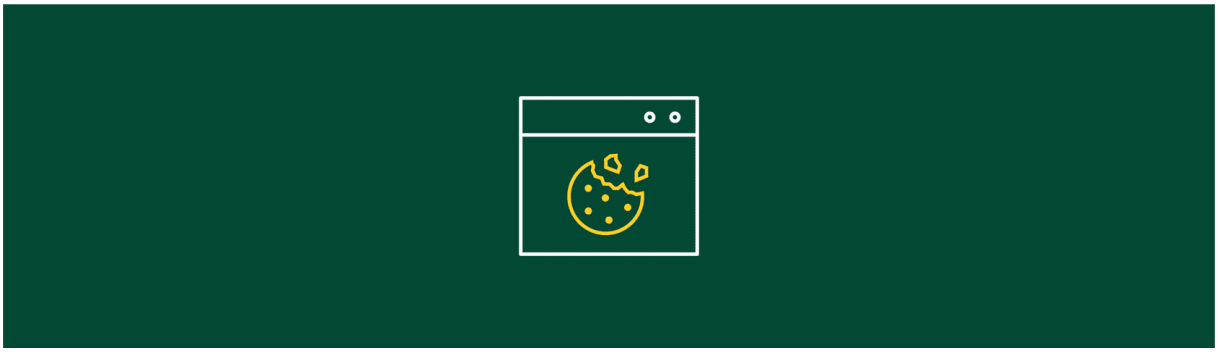
que ces informations soient conservées sur une plateforme protégée par un mot de passe, chiffrée ou sécurisée d'une façon ou d'une autre.

- Si vous travaillez au sein d'une organisation, pensez à demander une formation à la cybersécurité ou à l'offrir à vos collègues, si possible.

Soyez au fait des cookies

Les cookies ne sont pas seulement de délicieux biscuits ! Il s'agit également d'un moyen pour votre ordinateur de suivre votre activité sur le web, ce qui peut être utile pour enregistrer des données de connexion ou renseigner automatiquement votre nom et votre adresse lorsque vous effectuez des achats en ligne. Mais parfois, les cookies cachent également des problèmes de sécurité, alors veillez à vérifier régulièrement ce que stockent les cookies de votre navigateur web.

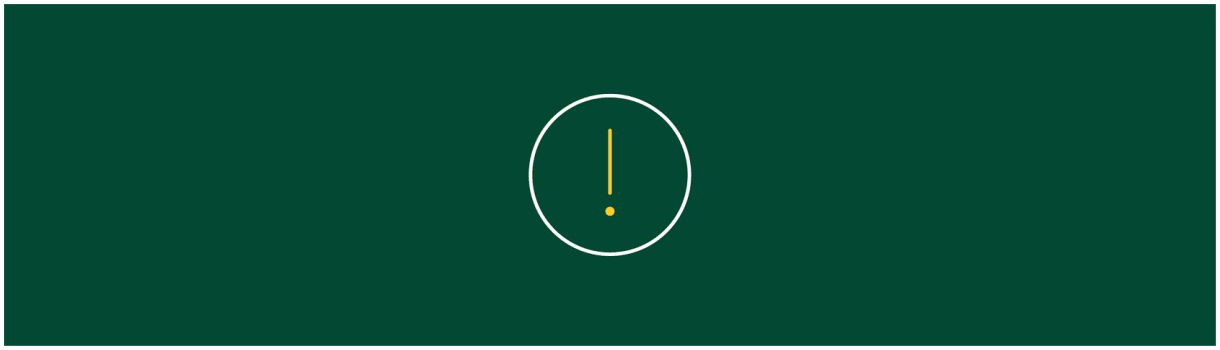
Pour plus de conseils, regardez la vidéo «Cookies and Your Online Privacy.» Vous pouvez également consulter l'article « How to delete Cookies?»



Faites attention à la désinformation

Il y a tellement d'informations en ligne. Comment savoir ce qui est vrai ? Voici quelques conseils pour distinguer le mythe de la réalité :

- Regardez la source d'origine de l'information. Que pouvez-vous trouver sur cette personne, cette organisation ou ce média qui pourrait vous aider à déterminer sa crédibilité ? Les médias fiables emploient des journalistes expérimentés et indépendants de tout gouvernement, entreprise ou organisation.
- Passez en revue les autres sources qui rapportent la même actualité afin de comprendre les différences de traitement. Cela permet de corriger tout biais qu'un média pourrait adopter.
- Analysez vos propres biais. Votre opinion obscurcit-elle votre jugement concernant la véracité de cette information ?
- Dans le doute, tournez-vous vers un expert reconnu dans ce domaine. Que dit cet expert de cette question ?



Réaction à la désinformation

Si vous avez connaissance d'une personne qui propage de fausses informations, comment réagir ?

Commencez par échanger respectueusement avec la personne dans un cadre privé et ne l'accusez de rien ; cela ne servirait qu'à la mettre sur la défensive. En utilisant les astuces que vous venez d'apprendre, expliquez-lui pourquoi vous ne pensez pas que l'information soit correcte (par exemple, elle ne provient pas d'une source fiable, d'autres agences de presse couvrent le sujet très différemment, un expert la contredit).

Vous pouvez partager d'autres informations issues d'autres sources avec la personne et lui poser des questions sur l'information qu'elle partage pour l'aider à comprendre d'elle-même si l'information est exacte ou non. Parfois, les personnes sont aveuglées par leur propre opinion et peuvent ne pas vouloir entendre ce que vous avez à dire. Si une conversation commence à s'échauffer ou que votre interlocuteur ne veut pas vous écouter, mettez un terme à la discussion.

Apprenez-en davantage en visionnant les deux vidéos suivantes :

- “Think before you share | UNICEF”
- “Helping Students Identify Fake News with the Five C’s of Critical Consuming” pour en savoir plus sur les moyens d’identifier des fausses informations.

En utilisant tout ce que vous avez appris, imaginez un autre scénario.

Vous menez une enquête en ligne pour étayer un policy brief destiné aux décideurs dans votre communauté. Cette enquête contient des

informations personnelles des sondés. Comment protéger au mieux ces informations ?

Sélectionnez les meilleures réponses parmi les cinq options suivantes.

- [ ] Vérifier que vos appareils et vos comptes en ligne où sont stockées les informations privées disposent de mots de passe forts.
- [ ] Laisser la feuille de calcul avec les données ouverte sur votre ordinateur. Tant que personne d'autre n'utilise votre téléphone ou votre ordinateur, les autres ne peuvent pas voir les informations.
- [ ] Vérifier vos paramètres de confidentialité et de sécurité.
- [ ] Utiliser les noms complets et des informations d'identification dans le rapport.
- [ ] Utiliser uniquement ces données aux fins de cette enquête, selon l'utilisation prévue, pour rédiger une politique.

SUBMIT

À SUIVRE : COMMENT ME PROTÉGER DU CYBERHARCÈLEMENT ET Y RÉAGIR ?

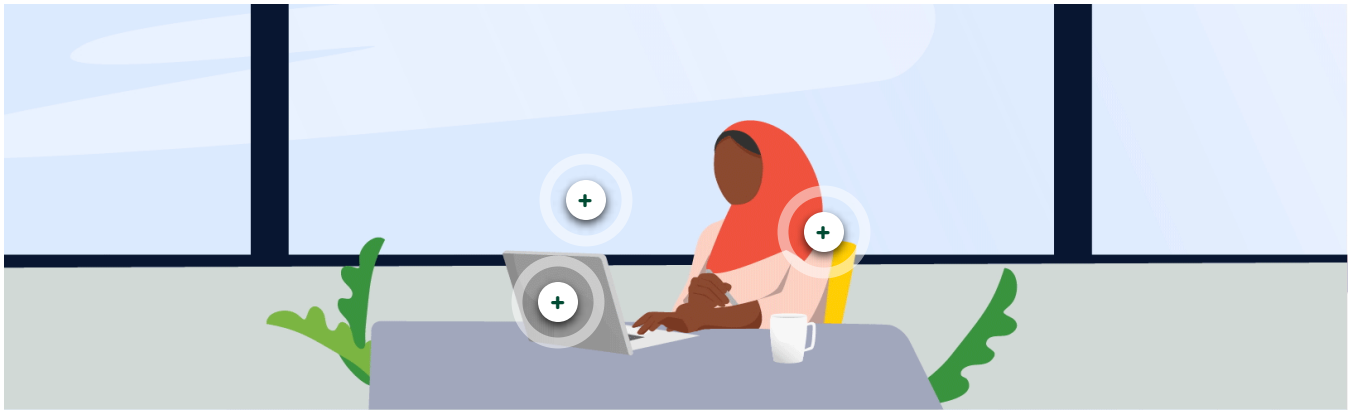
Comment me protéger du cyberharcèlement et y réagir ?

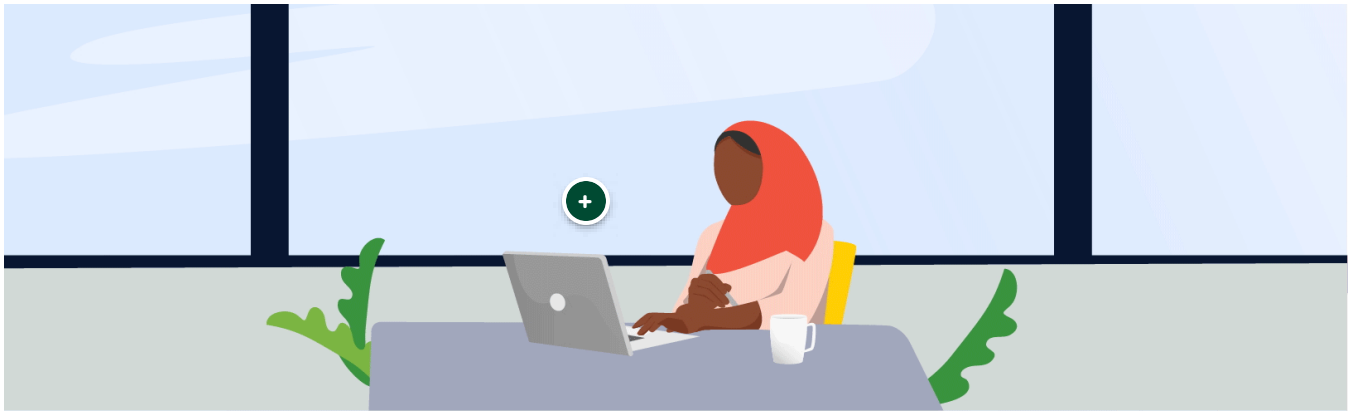
Selon une étude de 2020 de Plan International, 52% de jeunes filles ont déjà subi du harcèlement et de la maltraitance en ligne. Vous avez peut-être vous aussi déjà vécu des faits de cyberharcèlement, ou connaissez des personnes dans cette situation. Il s'agit d'un problème grave qui influence la santé et le bien-être des personnes où qu'elles se trouvent. Heureusement, il existe des moyens de l'arrêter et d'aider ceux qui en sont victimes.

Qu'est-ce que le cyberharcèlement ?

Le cyberharcèlement désigne une situation où une personne se montre intentionnellement et délibérément méchante ou cruelle envers une autre au moyen d'une technologie, par exemple sur les réseaux sociaux, par texto ou e-mail, ou dans une application mobile.

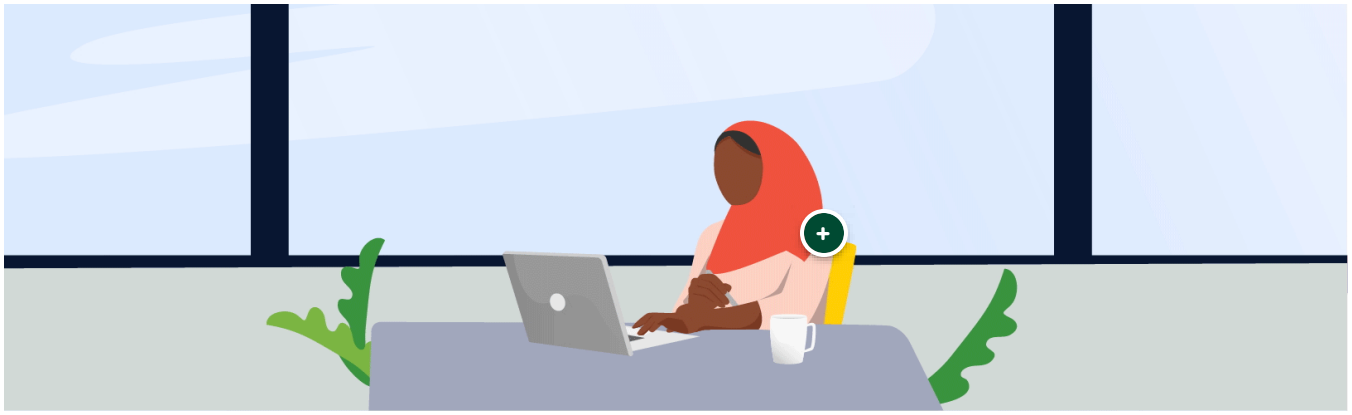
Pour apprendre les aspects Quoi, Où et Comment du cyberharcèlement, sélectionnez chaque élément.





Quoi

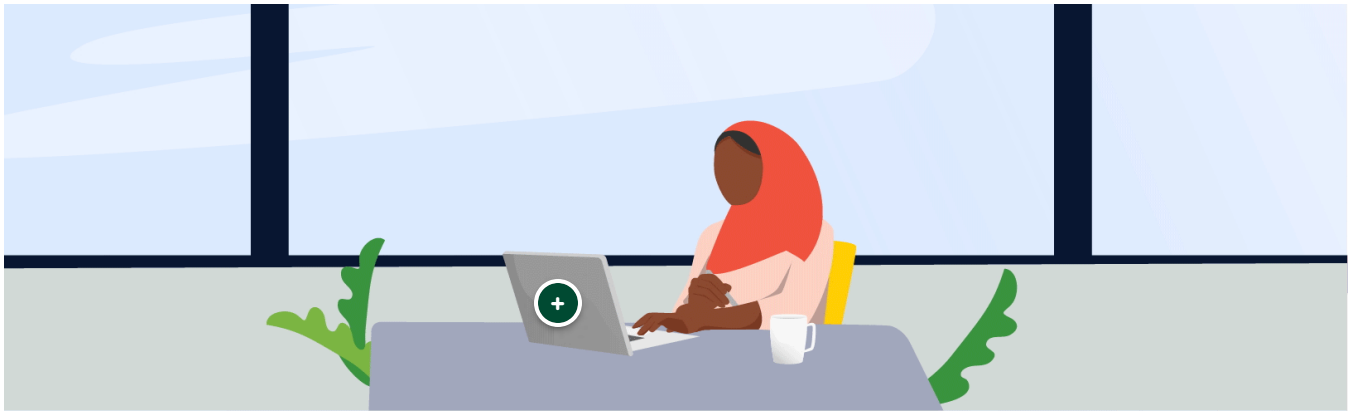
Le cyberharcèlement peut couvrir la publication, le sous-titrage ou la mention d'images de manière inappropriée, l'exclusion d'une personne de groupes ou de discussions en ligne, les commentaires irrespectueux sur le profil, les photos ou les mises à jour d'une personne, l'imitation ou l'irrespect envers des personnes à travers un statut ou du contenu en ligne, ou le partage d'informations personnelles sans le consentement de l'autre.



Qui

N’importe qui peut être victime de cyberharcèlement. Cependant, les personnes qui subissent la discrimination ou la marginalisation dans le monde physique à cause de leur identité (comme les filles et les femmes, les BIPOC, c’est-à-dire les personnes autochtones, noires et de couleur, les personnes LGBTQIA+, ou les personnes à l’intersection de ces identités, ainsi que d’autres populations traditionnellement exclues) sont souvent plus vulnérables face au cyberharcèlement.

Par exemple, le cyberharcèlement en raison du genre désigne le harcèlement d’une personne en raison de son orientation sexuelle ou de son identité de genre réelle ou perçue.



Où

Comme le cyberharcèlement se produit en ligne, il peut survenir à tout moment ou depuis n'importe quel endroit physique, mais il se déroule le plus souvent dans un espace numérique public. Contrairement au harcèlement classique, un cyber-harceleur peut se sentir anonyme et protégé car les faits se déroulent sur Internet, ce qui rend le contrôle plus difficile.

Parfois, le cyberharcèlement peut déborder et mener à du harcèlement en personne, surtout si les informations personnelles de la victime, telles que son nom et sa localisation, sont partagées en ligne. Selon le rapport de Plan International, une jeune fille sur quatre ayant subi du cyberharcèlement déclare se sentir physiquement en danger.

Découvrez les conclusions d'une étude de PLAN.


42%
14%
37%

42%

Le pourcentage de filles dans cette étude qui ont indiqué avoir été harcelées en raison de leur identité de LGBTIQ+ (sur le total des filles qui se considèrent comme LGBTIQ+ et ayant été victimes de harcèlement).

14%

Le pourcentage de filles dans cette étude qui ont indiqué avoir été harcelées en raison d'un handicap (sur le total des filles qui se considèrent comme étant en situation de handicap et ayant été victimes de harcèlement).

37%

Le pourcentage de filles dans cette étude qui ont indiqué avoir été harcelées en raison de leur appartenance à une minorité ethnique (sur le total des filles qui se considèrent comme étant issues d'une minorité ethnique et ayant été victimes de harcèlement).

Source: Plan International

Comme de nombreuses interactions sociales étaient limitées à l'espace en ligne pendant la pandémie de Covid-19, de nombreux jeunes ont signalé une augmentation du cyberharcèlement au cours de cette période.

En tant que défenseurs de certaines causes, nous avons souvent affiché nos points de vue et nos convictions, qui peuvent paraître de nature controversée ou même radicale au sein de nos communautés. Nous aussi pouvons faire l'objet de harcèlement en ligne en raison de nos convictions, de nos affiliations politiques et de nos opinions personnelles. Dans une étude de Plan International sur les jeunes défenseurs de l'égalité de genre, 47% ont déclaré avoir été attaqués en ligne pour leurs opinions. Le cyberharcèlement des défenseur(e)s peut être une tentative de réduire au silence ceux qui font avancer les problématiques de justice sociale ou d'égalité des genres.

Analysons comment réagir au cyberharcèlement.

Sélectionnez chaque élément pour en savoir plus.

Comment me protéger du cyberharcèlement ?

Les personnes qui se livrent au cyberharcèlement ne seront probablement pas ouvertes à la pensée rationnelle ou au raisonnement. Mieux vaut ne pas réagir ou répondre. S'engager dans une discussion risque d'aggraver les choses. Au lieu de cela, enregistrez des copies ou des captures d'écran du comportement de harcèlement, changez vos paramètres de confidentialité et bloquez la personne qui vous harcèle, si possible. Selon la plateforme numérique, il peut exister une option de signalement des abus. Gardez à l'esprit que dans bien des cas, une personne doit être signalée plusieurs fois avant d'être bloquée sur une plateforme. Aussi, le harceleur peut tenter de vous harceler à nouveau ou de harceler d'autres personnes par le biais d'un autre profil (non bloqué). Si vous connaissez personnellement l'individu à travers l'école ou votre lieu de travail, parlez avec un professeur ou un manager pour lui raconter les faits. Les responsables auront peut-être des moyens de vous aider. Dans certains cas, il existe des lois locales ou nationales de protection contre le cyberharcèlement.

En outre, tout comme le harcèlement ou les agressions dans le monde physique, le cyberharcèlement peut nuire à la santé mentale. Parlez de votre expérience à un ami de confiance, un conseiller, un parent ou un professionnel de la santé mentale, trouvez de l'aide auprès de votre communauté via Child Helpline International, ou recherchez des ressources en ligne.

Comment réagir au cyberharcèlement lorsque d'autres personnes sont victimes ?

Tout d'abord, faites attention à la façon dont vous traitez les autres en ligne pour vous assurer de ne pas contribuer vous-même au cyberharcèlement. Si vous êtes témoin de cyberharcèlement, parlez à la victime et offrez-lui toute l'aide possible, par exemple en l'écoutant ou en l'aidant à accéder à des ressources. N'interagissez pas directement avec le harceleur en ligne, car vous pourriez aussi vous mettre en danger.

Sensibiliser sur l'impact du cyberharcèlement peut aider les jeunes à comprendre les répercussions graves qu'il peut causer et ainsi contribuer à le prévenir avant qu'il ne se produise.

En outre, des programmes socio-émotionnels qui forment les jeunes sur les questions des relations saines et respectueuses peuvent non seulement leur apprendre à interagir avec bienveillance et compassion, mais aussi renforcer leur résilience, qui leur permettra de mieux gérer toute expérience de cyberharcèlement. À grande échelle, les campagnes de sensibilisation du public peuvent aider à transmettre le message et des lois peuvent tenir les harceleurs pour responsables. Certains défenseur(e)s tiennent également les entreprises de réseaux sociaux pour responsables en raison de l'impact de leurs plateformes sur les utilisateurs.

Étude de cas : Une jeune leader agit pour mettre fin au cyberharcèlement

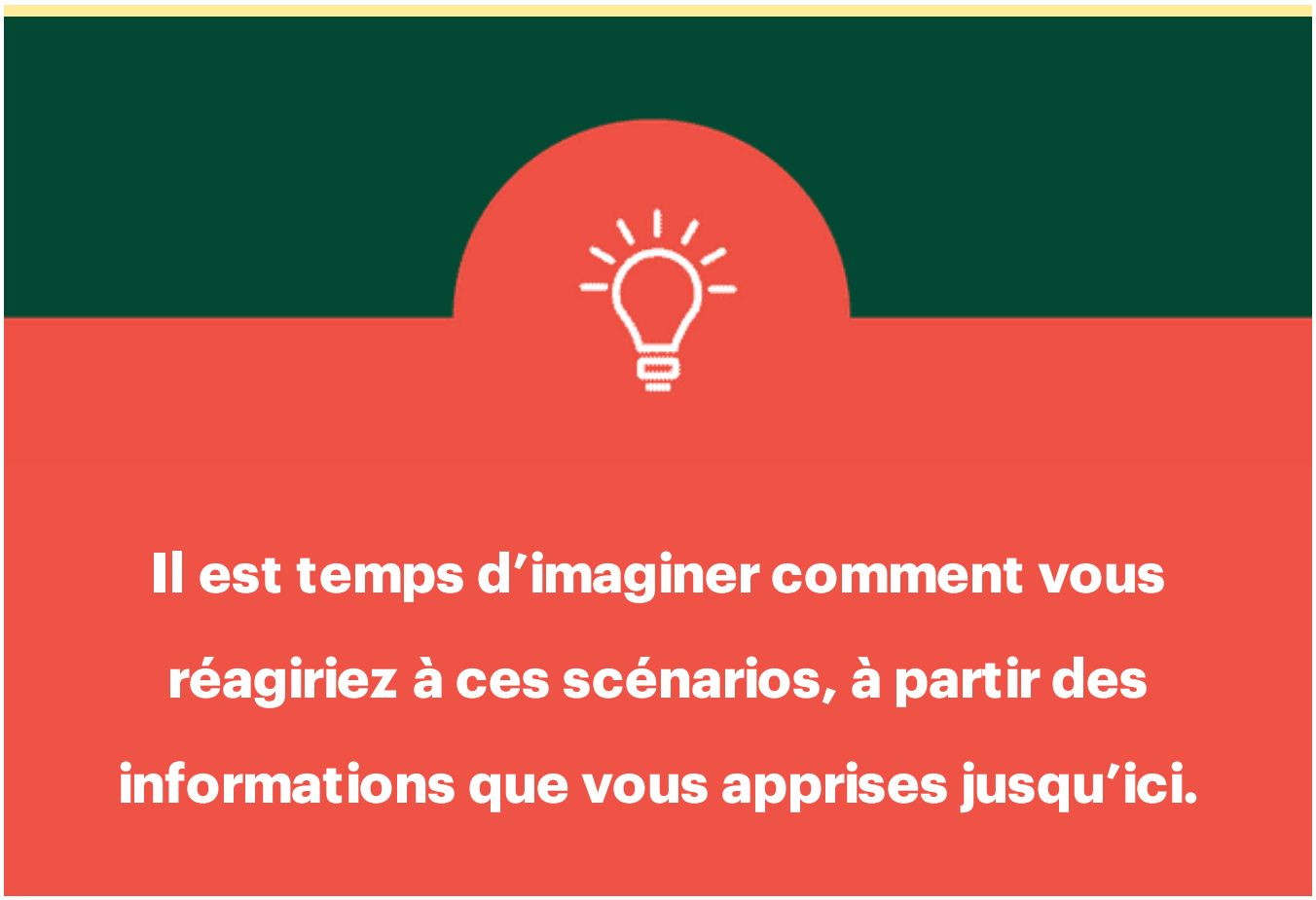
En plus des moyens permettant de nous soutenir mutuellement si nous sommes témoins de cyberharcèlement, de nombreux jeunes agissent pour éviter qu'il ne se produise et soutenir les victimes. Agita Pasaribu, Jeune leader Women Deliver, génération 2020, s'engage pour la cause ! Lorsque personne n'a pris au sérieux son propre signalement de harcèlement sexuel sur son lieu de travail, Agita, frustrée, a fondé Bullyid Indonesia. Bullyid dispense gratuitement un soutien juridique et une aide à la santé mentale en ligne pour les victimes de cyberharcèlement. En tant qu'association de défense, Bullyid a pour objectif de sensibiliser la population aux droits numériques, en particulier ceux en lien avec le cyberharcèlement, et d'augmenter l'auto-protection et la résilience des jeunes potentiellement victimes de harcèlement. Cette approche multiple traite à la fois les causes et les impacts du cyberharcèlement.

Un des types de cyberharcèlement est le *revenge porn*, ou porno-divulgation, c'est-à-dire une agression sexuelle basée sur les images. La porno-divulgation, également appelée vengeance pornographique, consiste à partager des images ou des vidéos intimes d'une personne sans son consentement, en ligne

ou hors ligne, dans le but de nuire. Depuis que la pandémie de Covid-19 a touché l'Indonésie, Bullyid a étendu ses services et son champ d'action pour inclure le Revenge Porn Help Centre.

Entre mars et mai 2020, les cas d'abus en ligne en Indonésie ont augmenté de plus de 300% par rapport aux statistiques de 2019, selon le Ministère de l'autonomisation des femmes et de la protection des enfants en Indonésie. De nombre uses affaires traitées par Bullyid entrent dans la catégorie de la diffamation en ligne et du *revenge porn*. Voyant cela, Bullyid a envoyé un courrier officiel à plusieurs entreprises de réseaux sociaux pour leur demander d'aider les victimes de *revenge porn* en retirant/supprimant rapidement ce contenu. À présent, le Revenge Porn Help Centre de Bullyid travaille en étroite collaboration avec le Public Policy Department de Facebook/Instagram et avec Twitter Indonésie pour supprimer plus rapidement tout contenu de porno-divulgation partagé sur leur plateforme.

Avec le soutien d'une bourse de Women Deliver, Bullyid a réussi à ajouter de nouvelles fonctionnalités à la plateforme. La plateforme de signalement de Bullyid, SHARE, est la première plateforme de signalement de harcèlement sécurisée et anonyme à destination des institutions qui permet à leurs employés et/ou étudiants de signaler tout harcèlement/cyberharcèlement ou comportement inapproprié. Elle intègre également une plateforme de gestion des incidents qui permet aux universités de réagir, de gérer et de fournir une assistance psychologique aux victimes. Depuis son lancement en mai 2021, la plateforme SHARE protège du cyberharcèlement quatorze entreprises, quatre universités et deux organisations, soit 27 780 employés et étudiants en Indonésie. En tant qu'association agréée de premier plan qui œuvre pour prévenir le cyberharcèlement et le harcèlement et pour aider les victimes, Bullyid a été citée par ou associée à 179 médias et organisations, y compris l'Organisation mondiale de la santé, l'UNICEF et One Young World. À ce jour, plus de 45 000 Indonésiens bénéficient de l'aide de Bullyid en ligne, et l'association continue de rechercher des partenariats et de défendre cette cause afin d'augmenter son impact et de sauver plus de vies.



Il est temps d’imaginer comment vous réagiriez à ces scénarios, à partir des informations que vous apprises jusqu’ici.

Une personne que vous avez rencontrée récemment lors d’un événement scolaire commence à vous envoyer des messages personnels sur Facebook. Alors qu’il s’agissait d’abord de compliments, les messages se transforment rapidement en des propositions insistantes de dîners et des demandes de numéro de téléphone et de photos personnelles.
Quelles mesures pouvez-vous prendre pour vous protéger ?
Sélectionnez les meilleures réponses parmi les six options suivantes.

- [ ] Ignorer la conversation et bloquer l'utilisateur pour qu'il ne puisse plus vous envoyer de messages.
- [ ] Enregistrer une copie des messages.
- [ ] Répondre aux messages directement et demander à la personne de vous laisser tranquille.
- [ ] Signaler la conversation à Facebook et à votre école.
- [ ] Publier publiquement le nom de la personne et ce qu'elle vous a dit sur votre statut pour l'humilier.
- [ ] Demander de l'aide à un membre de votre famille, un bon ami ou un professionnel de santé mentale pour digérer l'expérience.

SUBMIT

Une jeune maman publie sur Instagram une photo d'elle le premier jour de son retour à l'école après avoir accouché. Vous voyez une litanie de

réponses négatives, surtout d'hommes, la harcelant et lui disant qu'elle n'a rien à faire à l'école maintenant qu'elle est mère.

Comment pouvez-vous aider au mieux cette jeune femme ?

Sélectionnez la meilleure réponse parmi les trois options suivantes.

- [ ] Comme vous ne connaissez pas cette femme personnellement, vous ne devriez pas vous en mêler.
- [ ] Partager le post sur plusieurs pages de réseaux sociaux pour souligner l'injustice de la situation.
- [ ] La contacter, l'écouter et l'orienter vers des services qui pourront lui offrir un soutien supplémentaire, si besoin.

SUBMIT

À SUIVRE : CONCLUSION

Conclusion

Avec tout ce que vous avez appris sur vos droits numériques, comment les protéger et comment vous prémunir du cyberharcèlement, vous êtes prêt.e à utiliser vos connaissances dans le monde réel.

Nous vous recommandons d'appliquer les bonnes pratiques apprises dans ce cours, en particulier dans les scénarios. Restez à l'affût des problèmes et des situations survenant en ligne avec vos partenaires et vos allié(e)s, et aidez lorsque vous le pouvez. N'oubliez pas de contacter un membre de votre famille ou un ami de confiance lorsque vous avez besoin d'aide.

Étapes suivantes

Post-test

À présent, passez au test de fin pour vérifier vos connaissances une dernière fois.

Question

01/01

---

7 questions drawn randomly from Les droits humains à l'ère du numérique, évaluation avant/après

Les droits humains à l'ère du numérique, évaluation avant/après

Question

01/07

Vrai/Faux : Tous les droits humains dont vous jouissez dans le monde physique (hors ligne) s'appliquent à votre identité numérique lorsque vous êtes en ligne.

- ◯ Vrai
- ◯ Faux

Question

02/07

Vos droits numériques comprennent : (Sélectionnez toutes les bonnes réponses)

- [ ] Le droit à la vie privée
- [ ] La liberté d'expression
- [ ] Le droit de vivre sans violence ni harcèlement
- [ ] La liberté de faire ce que vous voulez

Question

03/07

Citez trois infractions à vos droits numériques. (Sélectionnez toutes les bonnes réponses)

- [ ] Cyberharcèlement
- [ ] Data Mining (exploration de données)
- [ ] Blogging
- [ ] Surveillance

Question

04/07

Qui est responsable de l’application et de la protection des droits numériques ? (Sélectionnez toutes les bonnes réponses)

- [ ] États
- [ ] Entreprises
- [ ] Individus
- [ ] Organisations de la société civile

Question

05/07

Que devez-vous faire lorsque vous êtes témoin de harcèlement en ligne à l'encontre d'un tiers ?

- Confronter le harceleur publiquement et critiquer son comportement pour que les autres tirent eux aussi des leçons de la situation.
- Envoyer un message privé au harceleur pour lui dire que son comportement est inapproprié et que vous avez alerté les autorités compétentes.
- Ne rien faire, car cela pourrait aggraver une situation déjà négative.
- Offrir votre soutien et écouter la victime.

Question

06/07

Vrai/Faux : 35% de jeunes filles ont signalé avoir déjà subi du harcèlement et des abus en ligne.

- ◯ Vrai
- ◯ Faux

Question

07/07

Par quels moyens pouvez-vous vous protéger et protéger vos données en ligne ?

(Sélectionnez toutes les bonnes réponses)

- [ ] Il n’existe aucun moyen de se protéger, sauf si on s’abstient totalement d’utiliser Internet.
- [ ] Utiliser des mots de passe forts.
- [ ] Vérifier vos paramètres de confidentialité sur tous les sites de réseaux sociaux.
- [ ] Accepter tous les cookies sur les sites que vous consultez.
- [ ] Identifier les fausses informations en vérifiant les sources et en effectuant des recherches supplémentaires.